



# ATTACHMENT A: PROPOSAL REQUIREMENTS & SPECIFICATIONS EQUALIS GROUP: RECORDS MANAGEMENT, SHREDDING, STORAGE & DESTRUCTION WITH RELATED SERVICES & SOLUTIONS PROGRAM

## Table of Contents

Section 1.	General Guidelines.....	1
1.1.	Instructions for Completing Attachment A.....	1
1.2.	Trade Secrets.....	1
1.3.	Attachments.....	1
Section 2.	Initial Qualifying Criteria.....	2
2.1.	Completing & Submitting Initial Qualifying Criteria Documentation.....	2
Section 3.	Bidder Overview & Qualifications.....	3
3.1.	Company Information.....	3
3.2.	Financial Strength & Legal Considerations.....	3
3.3.	Industry Qualifications.....	5
3.4.	Public Sector Focus.....	5
3.5.	Customer References.....	6
3.6.	Insurance Coverage.....	6
Section 4.	Products and Services.....	8
4.1.	Products & Services.....	8
4.2.	Additional Features.....	10
4.3.	Additional Offerings.....	10
4.4.	Warranty.....	10
Section 5.	Business Operations.....	12
5.1.	Logistics.....	12
5.2.	Customer Service.....	12
5.3.	Order & Invoice Processing; Payment.....	13
5.4.	Members Contracting for Services.....	13
5.5.	Sustainability, Reclamation, and Recycling Initiatives.....	14
Section 6.	Go-To-Market Strategy.....	15
6.1.	Bidder Organizational Structure & Staffing of Relationship.....	15
6.2.	Contract Implementation Strategy & Expectations.....	15
6.3.	Administrative Fee & Reporting.....	17

## Section 1. General Guidelines

### 1.1. Instructions for Completing Attachment A

The specific requirements and proposal specifications for this Program are detailed in this [Attachment A – Technical Proposal Requirements & Proposal Specifications](#). Attachment A is provided to Bidders in an editable Microsoft Word form so that it can easily serve as the base document for a Bidder's Technical Proposal. Bidders should incorporate their Technical Proposal responses directly into this document and include referenced attachments separately.

Use the following electronic file naming convention for naming your Technical Proposal prior to uploading your completed Technical Proposal to Bonfire: *Technical Proposal – Bidder Name.docx*.

For sections of Attachment A structured like the example below, simply click in the green cell on the “Click here to enter response” text and either type in or paste (using the *Paste Special > Merge Formatting* function in Microsoft Word) your response.

1.1.1.	<b>Formation.</b> In what year was the company formed? For how long has your company been operating under its present business name? If your company has changed its business name, include the most recent prior business name and the year of the name change.
This is a sample question. Please do not respond.	

For sections of Attachment A structured like the example below, click on the “Yes” checkbox if your solution **fully provides** the defined requirement. Click on the “No” checkbox if your solution does not provide or only provides part of the defined requirement. The green cell is included for Bidders to provide any additional information or capabilities relating to that defined requirement. For example, if your solution i) provides more capabilities around that requirement, ii) meets some, but not all of that requirement, or iii) does not meet the defined requirement, but provides an alternative solution for the Proposal Review Team’s (“PRT’s”) consideration, click in the green cell on the “Click here to provide additional commentary, if necessary.” text and either type in or paste (using the *Paste Special > Merge Formatting* function in Microsoft Word) clarifying or additional information as appropriate.

1.1.2.	<b>NAID Certification.</b> Do your facilities meet NAID AAA certifications?	<input type="checkbox"/> Yes <input type="checkbox"/> No
This is a sample question. Please do not respond.		

### 1.2. Trade Secrets

Bidders are encouraged to review [RFP Section 3.4 – Trade Secrets Prohibition; Public Information Disclaimer](#) in conjunction with developing their responses to this RFP. Any information provided by a Bidder in its proposal that is not marked as trade secret information shall be deemed to be public records in accordance with Ohio law.

### 1.3. Attachments

Bidders may incorporate additional documents by reference as part of their response to [Attachment A – Technical Proposal Requirements & Proposal Specifications](#). For example, you may want to include brochures, charts, or graphs in response to specific questions included in this Attachment A. Bidders should clearly state in their response to questions in Attachment A whether any specific documents are incorporated in their proposal by reference. In the event the attached documents are not references or referenced correctly, the PRT may exclude those attachments from consideration when scoring proposals.

The file names of such referenced documents that are included in a Bidder's electronic Technical Proposal submissions and uploaded to Bonfire should include, in the following order: i) Technical Proposal, ii) Bidder's name, iii) the Section number of the question for which the file is included as part of the response, and iv) a brief description of what is included in the electronic file. For example, if a Bidder references an attachment that includes financial statements in response to [Section 3.2.1.](#), the following electronic file name would be appropriate: *Technical Proposal – Bidder Name – Section 3.2.1. – Financial Statements.pdf*.

## Section 2. Initial Qualifying Criteria

### 2.1. Completing & Submitting Initial Qualifying Criteria Documentation

As described in **RFP Section 5 – Criteria for Proposal Evaluation & Selection**, Bidders must complete and provide executed originals of the following documents as part of the proposal Bidders submit. Equalis Group will not consider a Bidder's Technical and Cost Proposals unless these forms are properly completed and submitted as part of the Bidder's proposal.

2.1.1.	<b>Attachment C – Required Bidder Information &amp; Certifications.</b> This document includes information about the Bidder, key points of contact for proposal and legal questions that may arise during Equalis Group's review of the response, minority business enterprise and certifications, required affirmations subject to Ohio Revised Code guidelines, equal employment opportunity questions, questions regarding the subcontracting of certain elements of a Bidder's service delivery to Members, and confirmation that Bidder has reviewed and annotated, if applicable, the Equalis Group model i) Master Agreement, and ii) Administration Agreement entered into with Winning Suppliers.
This is complete and included in the ZipFile provided.	
2.1.2.	<b>Attachment D – W-9.</b> Bidders must complete the W-9 form and include the completed W-9 form in their response.
This is complete and included in the ZipFile provided.	
2.1.3.	Does your proposal include the properly completed and executed <b>Attachment C</b> and <b>Attachment D</b> ? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Click here to provide additional commentary, if necessary.	

## Section 3. Bidder Overview & Qualifications

### 3.1. Company Information

3.1.1.	<b>Company Name &amp; Address.</b>	
Company Name:	Stericycle, Inc.	
Headquarters Street Address:	2355 Waukegan Rd	
City, State & Zip Code:	Bannockburn, IL, 60015	
Main Telephone Number:	866-783-7422	
Website:	<a href="https://www.stericycle.com/">https://www.stericycle.com/</a>	
3.1.2.	<b>Formation.</b> In what year was the company formed? For how long has your company been operating under its present business name? If your company has changed its business name, include the most recent prior business name and the year of the name change.	
1989, Shred-It is a wholly-owned subsidiary of Stericycle, Inc. Financial information can be found on Stericycle's website, <a href="http://investors.stericycle.com/">http://investors.stericycle.com/</a> .		
3.1.3.	<b>Legal Structure.</b> Check the box next to the option that best describes the company's legal structure. Include requested narrative in the space provided.	
&	Corporation – provide the State of incorporation and the company ownership structure.	Stericycle is a publicly held company traded on the Nasdaq (SRCL).
&	Partnership – provide the State of registration and the names of all partners.	<a href="#">Click here to enter response.</a>
&	Sole Proprietorship – provide the State of registration and the name and title of the principal.	<a href="#">Click here to enter response.</a>
&	Joint Venture – provide the State of registration and the names and titles of all principals.	<a href="#">Click here to enter response.</a>
&	Other – provide detailed description of corporate structure and ownership.	<a href="#">Click here to enter response.</a>

### 3.2. Financial Strength & Legal Considerations

3.2.1.	<b>Financial Strength.</b> Provide three (3) years of company and any parent company financial statements or other documents that speak to the financial strength of the company, such as the most recent Annual Report to Shareholders and 10K Report (if applicable) or audited financial statements, including income statement and balance sheet. <i>Note: you may mark this information as a "Trade Secret" per the terms of <a href="#">RFP Section 3.4 – Trade Secrets Prohibition; Public Information Disclaimer</a> and provide your response to this question in a separate electronic file that includes a "Trade Secret" watermark. Any company financial information provided should be included as part of the Technical Proposal. The proposal scoring of this <a href="#">Section 3.2.1.</a> for Bidders that do not provide any financial information will be zero/fails to meet.</i>	
--------	--	--

Shred-it is a wholly-owned subsidiary of Stericycle, Inc. Financial information can be found on Stericycle's website, <http://investors.stericycle.com/>.

**3.2.2.** **Bankruptcy & Insolvency.** Describe any bankruptcy or insolvency for your organization (or its predecessors, if any) or any principal of the firm in the last three (3) years.

N/A

**3.2.3.** **Litigation.** Describe any litigation in which your company has been involved in the last three (3) years and the status of that litigation.

Stericycle, Inc. operates in a highly regulated industry and must deal with legal actions and regulatory inquiries or investigations from time to time that may be instituted for a variety of reasons and may eventually result in a fine or other resolution. Information concerning these issues can be found in our quarterly reports which are available on [www.stericycle.com](http://www.stericycle.com).

**3.2.4.** **Mandatory Contract Performance Disclosure.** Pursuant to **RFP Section 3.13**, disclose whether the your company's performance and/or the performance of any of the proposed subcontractor(s) under contracts for the provision of services that are the same or similar to those to be provided for the Program which is the subject of this RFP has resulted in any "formal claims" for breach of those contracts. For purposes of this disclosure, "formal claims" means any claims for breach that have been filed as a lawsuit in any court, submitted for arbitration (whether voluntary or involuntary, binding or not), or assigned to mediation. For any such claims disclosed, fully explain the details of those claims, including the allegations regarding all alleged breaches, any written or legal action resulting from those allegations, and the results of any litigation, arbitration, or mediation regarding those claims, including terms of any settlement. While disclosure of any formal claims will not automatically disqualify a Bidder from consideration, at the sole discretion of Equalis Group, such claims and a review of the background details may result in a rejection of a Bidder's proposal. Equalis Group will make this decision based on the Proposal Review Team's determination of the seriousness of the claims, the potential impact that the behavior that led to the claims could have on the Bidder's performance of the work, and the best interests of Members.

Stericycle, Inc. operates in a highly regulated industry and must deal with legal actions and regulatory inquiries or investigations from time to time that may be instituted for a variety of reasons and may eventually result in a fine or other resolution. Information concerning these issues can be found in our quarterly reports which are available on [www.stericycle.com](http://www.stericycle.com).

**3.2.5.** **Mandatory Disclosure of Governmental Investigations.** Pursuant to **RFP Section 3.14**, indicate whether your company and/or any of the proposed subcontractor(s) has been the subject of any adverse regulatory or adverse administrative governmental action (federal, state, or local) with respect to your company's performance of services similar to those described in this RFP. If any such instances are disclosed, Bidders must fully explain, in detail, the nature of the governmental action, the allegations that led to the governmental action, and the results of the governmental action including any legal action that was taken against the Bidder by the governmental agency. While disclosure of any governmental action will not automatically disqualify a Bidder from consideration, such governmental action and a review of the background details may result in a rejection of the Bidder's proposal at Group's sole discretion. Equalis Group will make this decision based on the Proposal Review Team's determination of the seriousness of the claims, the potential impact that the behavior that led to the claims could have on the Bidder's performance of the work, and the best interests of Members.

Stericycle, Inc. operates in a highly regulated industry and must deal with legal actions and regulatory inquiries or investigations from time to time that may be instituted for a variety of reasons and may eventually result in a fine or other resolution. Information concerning these issues can be found in our quarterly reports which are available on [www.stericycle.com](http://www.stericycle.com).

### 3.3. Industry Qualifications

3.3.1.	<b>Company Identification.</b> How is your organization best identified? Is it a manufacturer, distributor/dealer/reseller, or service provider? Based on your answer, please provide a response to question 3.3.1.1.
Stericycle is a publicly held company traded on the Nasdaq (SRCL). Stericycle is primarily a service provider.	
3.3.1.1.	<b>Authorization.</b> If your company is best described as a distributor/dealer/reseller (or similar entity), please provide your written authorization to act as a distributor/dealer/reseller for the manufacturer of the products proposed in this RFP. If applicable, is your dealer network independent or company owned?
Stericycle is a publicly held company traded on the Nasdaq (SRCL).	
3.3.2.	<b>Industry Experience.</b> For how long has your company been in the records management, shredding, storage, destruction and/or related products and services industry? What percentage of your company's revenue in each of the last three (3) full calendar years was generated from the provision of records management, shredding, storage, destruction and/or related products and services?
Shred-it is a wholly-owned subsidiary of Stericycle, Inc. Financial information can be found on Stericycle's website, <a href="http://investors.stericycle.com/">http://investors.stericycle.com/</a> . Shred-it does not operate in the storage category.	
3.3.3.	<b>Geographic Reach.</b> Describe your company's service area in the United States (e.g., nationwide, the continental United States, or specific states or regions). If your company does not currently provide services nationwide, describe your plans/timeframes to achieve nationwide service provision, if applicable.
Stericycle is a global company and has the largest footprint of any other service provider of information destruction services throughout the United States and Canada.	
3.3.4.	<b>Certifications and Licenses.</b> Provide a detailed explanation outlining the licenses and certifications that are i) required to be held, and ii) actually held by your organization (including third parties and subcontractors that you use). Has your company maintained these certifications on an ongoing basis? If not, when, and why did your company lose any referenced certifications?
Stericycle operates in a highly regulated industry. Stericycle is a business to business service provider in secure data destruction. All services are NAID compliant under a multi facility certification. This certification ensures our customers fulfill their regulatory requirement of due diligence. Stericycle it will verify and monitor regulatory compliance as well as security best practices of secure data destruction to fulfill the customer's regulatory obligation, including HIPAA, FACTA, and IRS Regulations.	

### 3.4. Public Sector Focus

3.4.1.	<b>Public Sector Contract Vehicles.</b> What Public Sector contract vehicles (e.g., state term contracts, General Services Administration schedules, group purchasing organization contracts, etc.) does your company have in place to provide records management, shredding, storage, destruction and/or related products and services to public sector entities under an exemption from the standard public sector bid/RFP process? For each contract vehicle, when was the contract established, what is the expiration date, and is the award sole source or multi-source (i.e., is your company the only supplier for the spending category or are multiple competing suppliers included in the contract vehicle), and how much annual revenue your company generated through the contract(s) in each of the last three (3) calendar years?
--------	--

As it relates to information destruction services only, Stericycle has a cooperative purchasing agreement in place with Omnia Partners/US Communities. To our knowledge and to date, Stericycle is listed as the only provider of services within this category, again, specific to information destruction services.

**3.4.2.** *Education Success.* What is the i) total dollar amount, and ii) percentage of your company's total annual revenue generated by sales to educational institutions (i.e., K-12 schools & school districts and high education)?

Shred-it is a wholly-owned subsidiary of Stericycle, Inc. Financial information can be found on Stericycle's website, <http://investors.stericycle.com/>.

**3.4.3.** *Government Success.* What is the i) total dollar amount, and ii) percentage of your company's total annual revenue generated by sales to local governments (i.e., municipalities, counties, special districts, and state agencies)?

Shred-it is a wholly-owned subsidiary of Stericycle, Inc. Financial information can be found on Stericycle's website, <http://investors.stericycle.com/>.

**3.4.4.** *Public Sector Strategic Growth Plan.* Describe your company's three to five-year local government, K-12, and higher education sales objectives and the key elements of your strategic plan to achieve those objectives. What is the total annual dollar value of your company's revenue generated by sales to local governments and educational institutions in each of the last three (3) calendar years? What percentage of your company's total annual revenue is generated by sales to local governments and educational institutions?

Shred-it is a wholly-owned subsidiary of Stericycle, Inc. Financial information can be found on Stericycle's website, <http://investors.stericycle.com/>.

### 3.5. Customer References

**3.5.1.** Provide references of at least five (5) local government or educational institution customers for which your company has provided products and services similar in nature and scope to those defined in this RFP in the last three (3) years. Your references should include a mix of types and sizes of public sector entities such as municipalities, K-12 schools or schools districts, and colleges and universities. Each reference should include:

- Customer name and location;
- Customer contact person and their title, telephone number, and email address;
- A brief description of the products and services provided by your company;
- Customer relationship starting and ending dates; and,
- Notes or other pertinent information relating to the customer and/or the products and services your company provided.

We are working on providing references in accordance with the requirements.

### 3.6. Insurance Coverage

**3.6.1.** *General Liability, Property & Automobile Insurance.* If your company is selected as the Winning Supplier, during the term of any agreements between your company and Equalis Group, and for two (2) years following expiration or termination of such agreements, your company, at its own expense, will maintain and will require that its agents, subcontractors, or suppliers engaged in your company's

Yes  No

	<p>performance of its duties under such agreements, maintain general liability insurance, property insurance, and automobile insurance (at a minimum, in the amount of \$1,000,000 per occurrence/\$5,000,000 annual aggregate) applicable to any claims, liabilities, damages, costs, or expenses arising out of its performance under such agreements. Confirm that your company either a) has, or b) will purchase insurance coverage as described herein.</p>	
<p><a href="#">Click here to provide additional commentary, if necessary.</a></p>		
<p>3.6.2.</p>	<p><b>Employee Dishonesty – Members.</b> The Winning Supplier shall be held fully liable for any and all dishonest acts of its employees and/or its subcontractor’s employees. Coverage must be provided for Third Party Employee Dishonesty, covering all employees and all officers of your company and any subcontractors, in an amount not less than \$100,000 per occurrence. Confirm that your company either a) has, or b) will purchase insurance coverage as described above covering all employees and all officers of your company, in an amount not less than \$100,000 per occurrence for each Equalis Group Member utilizing the Program.</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p><a href="#">Click here to provide additional commentary, if necessary.</a></p>		
<p>3.6.3.</p>	<p><b>Third Party Employment Practice Liability – Members.</b> The Winning Supplier shall be held fully liable for any and all employment practice acts of its employees and/or its subcontractor’s employees, such as, but not limited to, sexual harassment and discrimination. Coverage must be provided for employment practice liability, covering all employees and all officers of your company and any subcontractors, in an amount not less than \$1,000,000 per occurrence. Confirm that your company either a) has, or b) will purchase insurance coverage as described above covering all employees and all officers of your company, in an amount not less than \$1,000,000 per occurrence for each Equalis Group Member utilizing the Program.</p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p><a href="#">Click here to provide additional commentary, if necessary.</a></p>		



## Section 4. Products and Services

### 4.1. Products & Services

4.1.1.	<b>Products &amp; Services Description(s).</b> Identify and provide a detailed description of the products and services you are offering as a part of your proposal.
<p><b>Regularly Scheduled Document Destruction Service</b>          Shred-it's regularly scheduled service provides an always-on solution that protects everyday workplace document. This program ensures strict chain of custody procedures are followed from the moment the customer's documents are placed in the Shred-it secure consoles and totes until they are shredded at the customer location or at a Shred-it secure branch facility.</p> <p>Service features:</p> <ul style="list-style-type: none"> <li>• Secure, locked consoles in your office</li> <li>• Complimentary Workplace Privacy Policies</li> <li>• Regularly scheduled pick-ups at the workplace</li> <li>• A Certificate of Destruction after every service</li> <li>• All shredded paper is 100% securely recycled</li> </ul> <p><b>One Time Document Destruction Service</b>          Shred-it's one-time service provides secure destruction of an accumulated volume of confidential documents. Documents are scheduled for pick up at a time and day convenient to the customer and then destroyed either on the customer's premises or at a Shred-it secure branch facility following strict chain of custody procedures.</p> <p>Service features:</p> <ul style="list-style-type: none"> <li>• Schedule your service at your convenience</li> <li>• Large or small volume of paper documents, hard drives, or other media</li> <li>• A Certificate of Destruction after every service</li> <li>• All shredded paper is 100% securely recycled</li> </ul> <p><b>Hard Drive and e-Media Destruction Service</b>          Shred-it applies the same proven, state-of-the-art, chain of custody protocols for hard drive destruction and e-media as we do for document destruction, ensuring safe, secure destruction of your media.</p> <p>Service features:</p> <ul style="list-style-type: none"> <li>• Regularly-scheduled or one-time destruction</li> <li>• Magnetic backup tapes, Floppy Disks, CD-ROMs, DVDs, all hard drives and USBs</li> </ul> <p>A Certificate of Destruction after every service</p>	
4.1.2.	<b>Open Market Products.</b> Provide a detailed description of your ability to accommodate requests for Open Market Products. Open Market Products is a category of products that cannot be found in your standard catalog offering or non-inventoried products.
N/A-This does not pertain to the solutions/services offered under this RFP related to Information Destruction Services/Shredding	
4.1.3.	<b>Differentiators.</b> Describe what differentiates your company's products and services from your competitors.
<b>The Shred-it Advantage</b>	

Protecting organizations' information for their people, customers and brands. Shred-it information security solutions help organizations prevent, protect, and recover from data exposure risks.

**Security Expertise**

- Largest information security provider in North America with a singular focus on document destruction
- Shred-it has more NAID AAA Certified facilities, which means less transfer points and places where data breaches could occur
- Proprietary secure chain of custody with barcode scanning at every touch point
- Secure, tamper-proof consoles
- GPS-tracked and alarmed trucking fleet
- Secure shredding facilities with 3rd party security monitoring, video cameras, key card access, no cell phones on premises
- Trained expertise in a wide range of information security laws and legislation

**Service Reliability**

- Offer accessible and convenient local, regional and national service
- The largest number of shredding plants in the industry means we can handle any shred volume
- Advanced route management technology means you can rely on us to be on time

**Customer Service**

- Proactive account management with local, regional, and national offices, staffed with security experts ready to answer your questions
- A customer portal for managing your information security program; from scheduling services, adding services to managing your account and paying bills quickly and easily

**4.1.4.** | **Data and Information Security.** Describe your organizations data and information security practices.

Please see attached Security Policies & Procedures Summary

**4.1.5.** | **Reporting.** Describe your reporting capabilities. For destruction related services, do you provide of Certificate of Destruction.

Shred-it uses an integrated SAP ERP (Enterprise Resource Planning) platform to track interactions with clients. This technology also enables Shred-it to create a wide range of custom reports for clients including:

- Certificate of Destruction report by location
- Invoice report by business group/building
- Monthly expenditures
- Quarterly volume destruction
- Location vs. volume
- Trees saved/environmental impact
- Top billing locations
- Service optimization / recommendations report

**4.1.6.** | **NAID Certification.** Do your facilities meet NAID AAA certifications?  Yes  No

Shred it is a business to business service provider in secure data destruction. All services are NAID compliant under a multi facility certification. This certification ensures our customers fulfill their regulatory requirement of due diligence. Shred it will verify and monitor

regulatory compliance as well as security best practices of secure data destruction to fulfill the customer's regulatory obligation, including HIPAA, FACTA, and IRS Regulations.

## 4.2. Additional Features

4.2.1.	<b>Value Add.</b> Describe any other features or capabilities relating to records management, shredding, storage, and destruction that would improve or enhance the Program. Your response may include, but is not limited to, ecommerce capabilities, marketing capabilities, green initiatives, and technological advancements.
--------	---

**Customized planning expertise:** Our dedicated team of information security specialists will design a service plan to address the specific needs of your organization and ensure privacy law compliance

**Centralized support:** Access to a dedicated account team through a single point of contact. This team can also add and remove locations or change service levels immediately if ever your service requirements change.

**Management reports:** We provide you with your document and hard drive destruction data so that you can monitor and manage your service, including cost analysis by location or department.

**Consistent service:** We have the geographic reach to support your organization with consistent, high-quality chain-of-custody service.

**Consolidated billing:** Simplified invoicing provides a single, easy-to-read report of your service that can be customized to show the details you want to see, saving you unnecessary reconciliation time.

**Cost savings:** By managing a single information security contract that supports all of your locations with multiple security products and services, you will save time and money.

**Customer Portal:** A customer portal for managing your information security program; from scheduling services, adding services to managing your account and paying bills quickly and easily

## 4.3. Additional Offerings

4.3.1.	<b>Other Capabilities.</b> Identify and describe any other products and/or services your company offers outside the primary scope of this RFP that can be made available to Equalis Group Members. Include proposed pricing for any additional products or services your company offers in <b>Attachment B – Cost Proposal</b> in accordance with the directions provide in <b>RFP Section 2.3 Cost Proposal &amp; Acceptable Pricing Formats</b> .
--------	---

N/A

## 4.4. Warranty

4.4.1.	<b>Warranty.</b> Provide a copy of the manufacturer's warranty. If required, please attach the warranty as an attachment as instructed in <b>Section 2.3</b> of this document. Describe notable features and/or characteristics of the warranty that a public sector customer would find interesting or appealing. How long is the warranty? Please indicate, and describe if applicable, if there are any optional extended warranty coverage available to Members. How does your warranty coverage compare to that of your competitors? Pricing related to the any extended warranty options must be included in <b>Attachment B – Cost Proposal</b> .
--------	--

A Certificate of Destruction (COD) is administered upon the completion of services rendered to substantiate the work performed. The COD is provided electronically in PDF format via email and can be administered upon completion of each service, monthly, or on demand. Each end user may specify the manner in which they prefer to receive the COD.

Each COD details such information as the date of service, address, container bar code scans, quantities of containers serviced, time stamps on scan of containers and trucks, next service date, etc.

Stericycle is NAID AAA and PCI-DSS compliant.

<b>4.4.2.</b>	<i>Claims.</i> Describe your warranty claims process.
---------------	---

N/A
-----

## Section 5. Business Operations

### 5.1. Logistics

5.1.1.	<b>Storage Capabilities.</b> Describe your document organizations storage capabilities including, but not limited to, the number size and location of facilities.
N/A- We are not participating in a Storage proposal	
5.1.2.	<b>Supply Chain.</b> Identify all other companies that will be involved in processing, handling, or shipping the products or services to the Equalis Group Member.
<p>Stericycle self performs information destruction services for better than 98% of its customer base throughout the United States. Upon destruction of materials beyond recognition or replication, materials are baled and securely transported to strategic paper mill partners throughout the United States, namely GP Harmon. In the event that Stericycle is unable to self perform services for specific customer locations, an approved subcontractor may perform services on the behalf of Stericycle. Customer sites serviced by way of subcontractor are notified in advance prior to services being rendered.</p>	
5.1.3.	<b>Expedited Service Request.</b> Describe your approach to handling emergency orders and/or service. Your description may include, but is not limited to, response time, breadth of service coverage, and service level.
<p>Shred-it assigns a dedicated support team for the management and service of each customer account. A top-line overview of job titles and responsibilities is documented below. Upon acceptance of Shred-it's proposal, Shred-it will issue a communication plan that details the account management and servicing approach, and will provide the customer with the names of those Team Members responsible for keeping them and their information secure. All assigned personnel have senior-level experience to manage the account.</p> <p>Customer Security Representative (CSR) – Shred-it Team Members responsible for performing the daily operational responsibilities of driving the vehicles, securely collecting customers' information and operating Shred-it equipment to perform the strict chain of custody in securing and destroying customers' information.</p> <p>Service Managers – Supervisors who perform routing of vehicles, management of CSR teams and many other operational functions related to maintaining and improving efficiencies in Shred-it's business resulting in better customer service.</p> <p>District Operations Managers – Managers responsible for overseeing regional branch operations.</p> <p>National Account Customer Experience (CE) Representative – Responsible for handling daily service requests that get dispatched to the branch operations through Shred-it's internal Client Interaction Center software.</p> <p>Billing Associate - Responsible for creating consolidated invoices by pulling transactional data monthly and performing pre-audit for any discrepancies, cancelling and re-billing invoices where issues occur, sending invoices based on a defined billing cycle, following up with customer inquiries about billing issues, and working in partnership with the AR team to help resolve outstanding payment issues.</p> <p>National Account Manager – This position is responsible for the overall success of the customer program, for integrating new initiatives and quarterly business reviews.</p>	

### 5.2. Customer Service

5.2.1.	<b>Customer Service Department.</b> Describe your company's customer service department & operations. Your description may include, but is not limited to, hours of operation, number and location of service centers, parts outlets, number of customer service representatives. Clarify if the service centers are owned by your company or if they are a network of subcontractors.
--------	--

Please reference Structure outlined 5.1.3.	
5.2.2.	<b>Complaint Resolution.</b> Describe your customer complaint resolution process. Describe how unresolved complaints are handled.
Customer complaints are taken very seriously and handled on a 1 off basis outlined in the Structure referenced in section 5.1.3.	

### 5.3. Order & Invoice Processing; Payment

5.3.1.	<b>Purchasing Options.</b> Describe the different channels in which this contract will be made available to Equalis Group Members. Your response should include, but is not limited to, whether your organization will serve as the single point of contact or if the contract will be made available to your dealers and reseller to serve as the single point of contact.
Please reference Structure outlined 5.1.3.	
5.3.2.	<b>Order Process.</b> Describe your company's proposal development and order submission process.
Please reference Structure outlined 5.1.3.	
5.3.3.	<b>Invoice Process.</b> Describe your company's invoicing process.
Please reference Structure outlined 5.1.3.	
5.3.4.	<b>Payment.</b> What is your standard payment terms? What methods of payment do your company accept?
Standard payment terms are NET 30, however, in many cases, payment terms are negotiated at the local end user agreement level.	
5.3.5.	<b>Financing.</b> Does your company offer any financing options or programs? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
N/A	

### 5.4. Members Contracting for Services

5.4.1.	<b>Customer Set Up.</b> Once an Equalis Group Member decides to accept your company's proposal for services as described in this RFP, what is the process for the Member to become a customer?
The Equalis Group Member (EQM) will work with the designated local/national account representative in the respective regions/markets to understand the needs as it relates to information destruction services. Should the EQM decide to move forward with the contracting of services, an End User Agreement will be mutually accepted by both parties outlining the terms and conditions of the services to be rendered. We will work with each EQM to install the appropriate equipment and service frequency specific to the needs of the customer. An account will be created in our system to manage the service detail. In addition to the reporting requirements set forth by Equalis as part of this RFP and subsequent Agreement between Stericycle, Inc. and Equalis, any invoicing and reporting requirements will be outlined in the aforementioned End User Agreement.	
5.4.2.	<b>Customer Agreements.</b> Does your company have standard customer agreements? If yes, please provide copies of any standard customer agreements and provide a response to question 6.3.3. <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

Please Reference Attached End User Agreement	
5.4.3.	<b>Contracting.</b> What is the process for reviewing, negotiating, and finalizing any customer-specific contract terms or requirements? Approximately how long does the contracting process take to complete (i.e., secure a fully executed contract document)? What is the typical term length of your customer agreements?
<p>In addition to the response in Section 5.4.1, the contracting process varies from customer to customer. This depends on how long it takes for each party to agree to terms and conditions. Once the contracting process has been finalized, the end user can expect a turnaround time between 4-8 weeks to have equipment installed and begin receiving services; the turnaround time will depend on the size of the opportunity. While 4-8 weeks can be expected, expedited turnaround time may be possible, again depending on the size of the opportunity. Typical term length of customer agreements range from 36 to 60 months.</p>	

**5.5. Sustainability, Reclamation, and Recycling Initiatives**

5.5.1.	<b>Sustainable Company Initiatives.</b> Describe the ways in which your company is addressing the issue of recycling & sustainability.
<p>Stericycle is actively collecting energy and emission data now with the intent of filing its first CDP Climate Change survey in 2021 (with 2020 data). This survey will enable us to report environmental sustainability data in future years.</p>	

## Section 6. Go-To-Market Strategy

### 6.1. Bidder Organizational Structure & Staffing of Relationship

6.1.1.	<p><b>Primary Point of Contact for Equalis Group.</b> Who is the individual that will serve as Equalis Group's primary point of contact for developing and implementing a go-to-market strategy to increase Program participation by local governments and educational institutions across the country? Include the individual's name, title, a description of their role, and a resume or biography.</p>
<p>Please see attached document referencing Key Program Personnel; the list of key contacts can change throughout the managed relationship with Equalis</p>	
6.1.2.	<p><b>Key Staff.</b> Provide the names, roles, and tenure with the company of other key staff members who will be working with Equalis Group in such areas as sales management, field sales, marketing, collateral development and approval, accounting, and reporting.</p>
<p>Please see attached document referencing Key Program Personnel; the list of key contacts can change throughout the managed relationship with Equalis</p>	
6.1.3.	<p><b>Sales Organization.</b> Provide a description of your sales organization, including key staff members, the size of the organization, in-house vs. third-party sales resources, geographic territories, vertical market segmentation, segmentation by account size, inside sales, field sales, and how sales representatives are compensated (e.g., on gross revenue, profitability, or some other formula).</p>
<p>Shred-it assigns a dedicated support team for the management and service of each customer account. A top-line overview of job titles and responsibilities is documented below. Upon acceptance of Shred-it's proposal, Shred-it will issue a communication plan that details the account management and servicing approach, and will provide the customer with the names of those Team Members responsible for keeping them and their information secure. All assigned personnel have senior-level experience to manage the account.</p> <p>Customer Security Representative (CSR) – Shred-it Team Members responsible for performing the daily operational responsibilities of driving the vehicles, securely collecting customers' information and operating Shred-it equipment to perform the strict chain of custody in securing and destroying customers' information.</p> <p>Service Managers – Supervisors who perform routing of vehicles, management of CSR teams and many other operational functions related to maintaining and improving efficiencies in Shred-it's business resulting in better customer service.</p> <p>District Operations Managers – Managers responsible for overseeing regional branch operations.</p> <p>National Account Customer Experience (CE) Representative – Responsible for handling daily service requests that get dispatched to the branch operations through Shred-it's internal Client Interaction Center software.</p> <p>Billing Associate - Responsible for creating consolidated invoices by pulling transactional data monthly and performing pre-audit for any discrepancies, cancelling and re-billing invoices where issues occur, sending invoices based on a defined billing cycle, following up with customer inquiries about billing issues, and working in partnership with the AR team to help resolve outstanding payment issues.</p> <p>National Account Manager – This position is responsible for the overall success of the customer program, for integrating new initiatives and quarterly business reviews.</p>	

### 6.2. Contract Implementation Strategy & Expectations

6.2.1.	<p><b>Five (5) Year Sales Vision &amp; Strategy.</b> Describe your company's vision and strategy to leverage a piggybackable Master Agreement with Equalis Group to win and retain local government and educational institution business over the next five (5) years. Your response may include, but is not limited to; the geographic or public sector vertical markets being targeted;</p>
--------	---



	your strategy for acquiring new business and retaining existing business; how the contract will be deployed with your sales team; and the time frames in which this strategy will be implemented.
--	---

Upon completion of this agreement and mutual execution by both parties, Shred-it shall assign Equalis a “National Account Code” which shall be used to imbed in all signed agreements with Agencies fostered or brought forth by the relationship of the parties. All those accounts shall then be “linked” to the Equalis National Account program for the purposes of creating a Parent/Child Hierarchy and appropriate archiving and recording of individual Child relationship agreements and the revenues generated between the Agencies and Shred-it.

Shred-it will work with Equalis to “roll out” the plan to our joint Sales Organizations and train both on the inter-relationship of the program as it is defined or as it may evolve and encourage and sponsor related activities to encourage ongoing Prospecting and Engagement using:

- Available Marketing Listings of Membership provided by Equalis
- Generally available Agency Listings that Equalis may make available to Shred-it defining preferred target agencies
- NOTE: Shred-it reserves the right to consider only Net New Agency relationships or to disqualify Agencies that may be under an existing and legally binding Agreement with Shred-it through another Competitive program engaged with Shred-it.

Shred-it’s overarching business assumption is that Equalis will make every effort to aggregate the purchasing power of combined population of existing and future public agency population nationwide by offering net new Participating Public Agencies the ability to make purchases through existing, competitively solicited contracts between a supplier and a lead public agency. We would anticipate that effort to include the entire geographic contiguous United States (with non-Continental US States, Regions or Territories being subject to inclusion or exception based upon mutual agreement) and which may include but not be limited to:

We understand that it takes some time to build our program up to what we all would expect to be fruitful. We are relying on Equalis and its lead agency partners to satisfy bidding requirements on behalf of public agencies removing barriers to our products and services. Having the largest sales force in the industry, we are looking for a partner that will reciprocate the efforts involved in gaining new business while continuing to build on our existing partnerships. Lets combine our efforts to bring the best in class solutions to our public agencies. We have the infrastructure like no other company within this category to execute shared business strategies that build value based programs. From agencies with few employees to thousands, our solutions stretch from coast to coast and north and south covering 98%+ of the United States.

Help us bring opportunities to light leveraging our “piggyback” and we will work with each individual public agency to put a unique program in place that satisfies the requirements of the agency while remaining compliant. Our field sales organization, through the use of our robust Salesforce platform/cloud, will proactively engage agencies to ensure our services/solutions put us within their facilities “just in time”. Agencies will have their own Customer Service Agreement under the Equalis family contract (think parent/child relationship as it relates to account setup) defining specific terms and conditions relevant to the respective agency. Time frames are dependent upon the complexity of each opportunity.

A full suite of reporting capabilities help us to provide valuable metrics, feedback and perform service optimizations saving time and money.

Lastly, what are exceptional solutions without world class Customer Service. Our Customer Support Team stands ready to assist customers of all size to manage simple day to day interactions and changes with service to contract renewals and more. Our People Drive our Value!

<b>6.2.2.</b>	<b>Sales Team Incentives.</b> Will your sales team be equally incentivized to leverage the Equalis Group Master Agreement as compared to any other traditional sales process or cooperative contract?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
---------------	---	---

Our sales teams would be equally incentivized to use the Equalis Group MSA compared to other cooperative contracts. What will set the Equalis Group MSA apart from other relationships will be the intercompany interaction and collaboration of new strategies aimed at meeting and exceeding goals set forth by both organizations. Consistent business reviews shall be established to determine what is working and where they may be potential room for improvement. Our field sales organization, including hundreds of local and national reps across the US and Canada, is unrivaled in the industry.

**6.2.3.** *Revenue Objectives.* What are your revenue objectives in each of the five (5) years of the piggybackable Master Agreement?

While all new and emerging programs have projections for potential growth, it is unreasonable to presume any element of forecast accuracy inherent in a “Net New” and untested program. Based upon other models employing a similar Lead Agency Piggy-Back Strategy, it could be reasonable to presume that

1. The initial or “gestation” year will have results that may be initially weak or even disappointing depending upon “roll out” opportunities or willingness of Agencies to embrace the acceptable concept with a new entity but
2. Year TWO is very likely to see a growth of between 80 and 100% and
3. Years THREE and Beyond may see average annual growth of between 2% and 12% again dependent upon the qualification of the Agency size and opportunity (with the understanding that these opportunities are individually self-qualifying as “as small as a three Deputy County Sheriff’s Department” to as potentially “as large as a multiple city campus structure of a State University”.

Our goal will be to grow this contract to \$2M+ of annual revenue.

### 6.3. Administrative Fee & Reporting

<b>6.3.1.</b>	<p><i>Administrative Fee.</i> Equalis Group generates revenue as a percentage of the Winning Supplier’s revenue from local government and educational institutions purchasing products and services from Winning Supplier through the piggybackable Master Agreement between the Winning Supplier and Equalis Group. The Administrative Fee is designed to align the interests of the Winning Supplier and Equalis Group – Equalis Group only generates revenue when the Winning Supplier generates revenue based on Program utilization by current and future Members. The Administrative Fee for this Program is two percent (2%) of the Winning Supplier’s Program revenue, payable upon invoice issued by the Winning Supplier to participating Equalis Group Members. Confirm that, if selected as the Winning Supplier of this RFP process, Bidder agrees to this Administrative Fee structure.</p>	<input checked="" type="checkbox"/> Agree <input type="checkbox"/> Negotiate
---------------	---	---

Stericycle will agree to the 2% Administrative Fee and is willing to have further discussions to increase the amount of the Fee to reward achieved revenue thresholds. It may be necessary to revise the amount of the Administrative Fee from time to time depending on situational circumstances per opportunity.

<b>6.3.2.</b>	<p><i>Sales &amp; Administrative Fee Reporting.</i> Equalis Group requires monthly reports detailing sales invoiced the prior month and associated Administrative Fees earned by the 15<sup>th</sup> of each month and reports detailing the prior calendar year’s sales invoiced and Administrative Fees earned within thirty (30) days following the end of the calendar year. Confirm that your company will meet or exceed this reporting requirement. If your company cannot meet this reporting requirements schedule, explain why, and propose an alternative time schedule for providing these reports to Equalis Group.</p>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
---------------	--	---

Shred-it will be able to satisfy this requirement, however, we prefer to have a discussion about the frequency of the payout. Our preference is to provide this Admin Fee payout quarterly.

# Stericycle Shred-it Key Contacts



**Customer Care Team – National Accounts**  
Hours of Operation 8:00 am - 8:00 pm EST

National Acct #: XXXXXXXXX  
National Account Code: NXXXX

Customer Care	Responsibilities	Phone	Email
<b>Service Request Email Address</b>	Primary email for all Service Requests of any type, new location, change/add/modify service, and all billing related inquiries.	US: 800-69-shred or 800-697-4733	<a href="mailto:ShreditNationalSupport@STERICYCLE.com">ShreditNationalSupport@STERICYCLE.com</a> Account #'s: TBD
<b>Supervisor, National Accounts Customer Care</b> Candise Bennett	Utilize for escalation	US: 800-697-4733 or 905-491-2379	<a href="mailto:Candise.Bennett@stericycle.com">Candise.Bennett@stericycle.com</a>
<b>Supervisor, National Accounts Customer Care</b> Anthony Riedi	Utilize for escalation	US: 800-697-4733	<a href="mailto:Anthony.Riedi@stericycle.com">Anthony.Riedi@stericycle.com</a>
<b>National Account Management Team</b>			
<b>National Program Manager – Enterprise Sales</b> Andy Allu	Use for contractual questions or issues, pricing, special projects, escalations, account relationship.	M: 917-528-7940	<a href="mailto:Andrew.Allu@stericycle.com">Andrew.Allu@stericycle.com</a>
<b>National Account Executive - Commercial/Healthcare</b> Peter Sansone	Escalation of issues, management escalations, account relationship.	M: 636-856-7558	<a href="mailto:Peter.Sansone@stericycle.com">Peter.Sansone@stericycle.com</a>

## Andy Allu



Andy has been a National Account Manager/Client Care Executive operating out of the Northeast for Shred-it since 2013. During that time, he has been responsible for account management of national Fortune 2000 companies (with specific emphasis on the Commercial and Financial verticals) and a key contributor who has opened up new opportunities for customers in Corporate Document Security, Secure Document Destruction, Hard Drive and eMedia Destruction. During his time with us, he has managed over 150 diverse National Accounts, 30 General Purchasing Organizations (GPOs) and six significant Facility Management Partnership Relationships. Prior to joining Shred-it, Andy was Vice President of Federal Law Enforcement Tactical Vehicle Sales for Odyssey Automotive, National Sales Manager for Pattern Systems International and spent over 20 years in Procurement and Materials Management for Commercial Prime Vendors of the Department of Defense.

## Andy

### Andrew Allu

National Account Manager

Stericycle Ethics Champion

M: 917.528.7940 | [andrew.allu@stericycle.com](mailto:andrew.allu@stericycle.com)

[Stericycle.com](http://Stericycle.com) | [Shred-it.com](http://Shred-it.com)

205 Winchester Dr. E. Stroudsburg PA 18301



## Pete Sansone



Pete's roots to Stericycle go back to 2004 when Pete began working at Cintas. From 2004 to 2009, Pete sold van-delivered First Aid & Safety solutions as well as Uniform Rental programs in his local market of St. Louis. During his time at Cintas, Pete garnered several awards highlighted by his 2006 First Aid & Safety Central Region Rep of the Year and President's Club. Pete also achieved 13 consecutive Achiever's Clubs, spanning First Aid & Safety and Uniform Rental, for his sales achievements quarterly. Pete was named to Cintas' Captain's Club in 2008.

In 2009, Pete left Cintas to work for Ferno-Washington, Inc., a patient handling and medical device manufacturing company. Pete was responsible for the sale of Ferno's capital equipment and other patient handling products to Fire/EMS Agencies over a three-state region of MO, KS, and NE. After earning Regional Sales Manager of the Year and President's Club in 2013, Pete was promoted to Key Account Specialist responsible for working with the largest Fire/EMS agencies over half of North America. Pete also was awarded the Suzie Xavier Award given to one Ferno employee annually that demonstrates Outstanding Customer Service.

In April of 2015, Pete joined Shred-it as a National Account Executive responsible for providing information destruction solutions for public agencies throughout North America. Pete worked extensively with the National Joint Powers Alliance (now Sourcewell) to grow Shred-it's portfolio by more than 4X annually in two years. In 2017, Pete began providing enterprise category solutions to commercial/healthcare companies. Pete has produced over \$1M in New Business Revenue for consecutive years achieving President's Club in 2017, 2018, and 2019.

Outside of work, Pete enjoys spending time with his wife of 15 years and 6 beautiful children (3 boys and 3 girls). Pete loves coaching Little League baseball for two of his boys, watching his girls play volleyball and gymnastics, and enjoys fishing and playing golf.

### **Pete Sansone**

National Account Executive – Commercial/Healthcare

M: +1 636-856-7558 | [stericycle.com](http://stericycle.com) | [shredit.com](http://shredit.com)



December 10, 2020

To Whom It May Concern,

Please see the references below regarding information destruction services performed by Stericycle Shred-it Inc.

1. Indiana University  
Tresa Fredericks  
[trfreder@iu.edu](mailto:trfreder@iu.edu)  
Phone: 812-855-9952
2. Wisconsin Department of Corrections  
Edward Bradley  
[edward.bradley@wisconsin.gov](mailto:edward.bradley@wisconsin.gov)  
Phone: 608-240-5572
3. County of Henrico, VA  
Leisel Collins  
[col119@henrico.us](mailto:col119@henrico.us)  
Phone: 804-501-5687
4. University of Florida  
Steve Neal  
[sneal@ufl.edu](mailto:sneal@ufl.edu)  
Phone: 352-294-1157
5. Wyoming Department of Transportation  
Cori Schrinardot  
[procurement-services@wyo.gov](mailto:procurement-services@wyo.gov)  
Phone: 307-777-4111

Please let me know if you have any questions.

Thank you!

Pete Sansone  
Sr. National Account Executive  
[Peter.Sansone@Stericycle.com](mailto:Peter.Sansone@Stericycle.com)  
636-856-7558

# Business Continuity Plan

Shred-it Service Operations



## Executive Summary

The Shred-it Business Continuity Plan outlines the procedures and key measures required to maintain continuity of service operations in defined crisis situations. The primary elements of the Shred-it Business Continuity Plan focus on post-interruption actions and decision-making as well as Shred-it's response to any critical disruption or extended interruption of normal service operations.

This plan serves as the primary and governing document for the Business Continuity component of Shred-it's overall Risk Management Policy and Oversight Framework. The Information Security component is governed by Shred-it's Corporate Information Security Policy and Strategy document. The Operational Compliance component is governed by several core documents that relate to internal operational compliance, including Human Resource policies.

The Shred-it Business Continuity Plan is structured around a multi-level activation, notification, and subsequent reaction process. Activation type is determined by level of emergency. However, any action initializes immediate business control measures. The institution of a field level business resumption management structure occurs for site level reaction and a corporate level support structure is instituted for information processing, resource procurement, and overall regional emergency operations control. Each structure is tasked with the functional objective of service resumption within six hours all resource deployment and emergency system setup surrounds specific procedures and protocols. Activation of key management structures is contingent upon service vulnerability recognition associated with any given plausible emergency. The Emergency Operations Center procedures and protocols illustrate support structure assurance associated with the general Business Continuity Plan activation. This structure assists in the execution of high-level tasks and is the foremost platform for information sharing and senior management action associated with vulnerability mitigation.

The Emergency Operations Plan created as a sub-section to the Business Continuity Plan serves as the primary resource for the Emergency Site Operations Team (herein: ESOT). The plan outlines primary tasks associated with ESOT roles and identifies procedures to ensure continued service and operations effectiveness during an emergency re-location or primary facility operations interruption. The plan focuses primarily on critical process coordination and specific service resumption management control, reporting, and information networking with Emergency Operations Center personnel.

Supporting both the Emergency Operations Center and the ESOT is the Shred-it Crisis Communication Plan. As part of the greater organizational communications structure, this plan supports media information control and information distribution to local and major account customers of any affected Shred-it location.

The coordination and control of business resumption activities is facilitated by key process resumption protocols. ESOT and support level functions are determined by priority tasks situated around process recovery time variables and acceptable downtime allowances. Each department



or section identified pursuant to the emergency impact assessment thus has outlined a primary set of procedures to ensure maximum recovery efficiency.

The Shred-it Business Continuity Program illustrates the company's continued commitment operations effectiveness and reliable, *secure* service provision to customers. As the program continues to develop, so too will efforts surrounding risk mitigation and overall process resiliency.

The Shred-it Business Continuity Program is authorized as follows:

1. Oversight, governance and approval:

**Shred-it Compliance and Executive Management Team**

2. Primary authority for implementation and operational accountability:

**Rich Moore**  
**Senior Vice President – Operations**

## **Introduction**

This Shred-it Business Continuity Plan contains the procedures and key measures required to maintain continuity of service operations in defined crisis situations. The primary elements of this document focus on post-interruption decision-making and Shred-it's response to any disruptive or extended interruption of normal operations.

This plan represents Shred-it's commitment to continued efforts to develop effective response, recovery, and restoration planning protocols and procedures. As such, each individual responsible for information or materials in this document have committed to ensuring the maintenance of its contents.

The Shred-it Business Continuity Plan was developed with the intent to provide a decision-making framework for field office business resumption while ensuring the safety and security of customers, team members, and vendors.

Although this plan provides guidance and documentation upon which to base emergency response, resumption, and recovery planning efforts, it is not intended as a substitute for informed decision-making. Individual management and departmental liaison staff must identify services for which disruption may result in significant financial and/or operational losses and engage mitigation measures and proactive planning efforts accordingly.

**Purpose**

The purpose of the Shred-it Business Continuity Plan is to enable the rapid and cost-effective delivery of essential services in the event of a service disruption or disaster. The Business Continuity Plan documents essential services, our continuity organization, continuity strategies and other processes that will ensure the successful achievement of continuity time objectives.

**Policy Statement**

Shred-it shall develop, , validate and maintain a departmental Business Continuity Plan that will ensure the rapid, efficient and cost-effective continuity of our essential services.

**Scope**

Procedures and protocol identified within the Shred-it customer service operations Business Continuity Plan will apply to all branch units designated as critical or otherwise dependent on the service operations process identified herein.

**Authority**

This document is approved by the Director, Compliance of Shred-it.

Matt Krol  
Director, Compliance

## **Business Continuity Management Team**

### **Areas of Responsibility**

#### *Business Continuity Management Team*

The Business Continuity Management Team reports directly to members of the Executive Management Team and is responsible for the overall coordination, control, implementation, and maintenance of the Shred-it Business Continuity Plan.

#### *Shred-it Branches*

Branches are responsible for the development, activation and implementation of their plans as components of the Shred-it Business Continuity Plan. See Emergency Response Plan - Branch

Divisions and branches will administer their own exercise, maintenance and awareness programs, pursuant to larger Business Continuity initiatives perpetuated at the corporate level.

**Key Definitions**

Term	Definition
<b>acceptable down time</b>	The period of time a function or activity can be disrupted without significant impact to essential services, production, customer service, revenue, or public confidence. Each business activity should determine its individual maximum allowable down time.
<b>activation</b>	Actions taken to implement a plan or a procedure.
<b>business continuity management</b>	An ongoing process supported by senior management and funded to ensure that necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity of services through staff training, plan evaluation, and maintenance.
<b>business interruption</b>	An emergency that negatively affects regular operations
<b>business resumption</b>	<i>See recovery</i>
<b>communications</b>	Advisories, directives, information and messages that are transmitted.
<b>critical infrastructure</b>	Interdependent, interactive, interconnected systems and processes that meet vital business needs
<b>drill</b>	A coordinated, supervised exercise activity normally used to evaluate a specific operation, procedure or function. It can include notification, telecommunications etc.
<b>emergency</b>	A situation or an impending situation that constitutes a danger of major proportions that could result in serious harm to persons or substantial damage to property and that is caused by the forces of nature, a disease or other health risk, an accident or an act, whether intentional or otherwise.
<b>Emergency Control Group (ECG)</b>	The Group that is responsible for coordinating business recovery activities. The Emergency Control Group usually includes senior management, business continuity team members and other relevant staff.
<b>Emergency Operations Centre (EOC)</b>	The facility where the Municipal Emergency Control Group assembles to manage an emergency.
<b>exercise</b>	A simulated drill or sequence of events to evaluate plans and procedures.
<b>hazard (1)</b>	A risk that is a threat.

<b>hazard (2)</b>	An event or physical condition that has the potential to cause fatalities, injuries, property damage, infrastructure damage, agricultural loss, damage to the environment, interruption of business, or other types of harm or loss.
<b>mitigation</b>	Actions taken to reduce the effects of an emergency or disaster.
<b>preparedness</b>	Actions taken prior to an emergency or disaster to ensure an effective response.
<b>prevention</b>	Actions taken to prevent an emergency or disaster.
<b>probability</b>	The likelihood of something happening.
<b>recovery</b>	Actions taken to recover from an emergency or disaster.
<b>recovery plan</b>	A risk-based emergency plan that is developed and maintained to recover from an emergency or disaster.
<b>regular operations</b>	Typical field level operations resulting in standard service delivery at optimized levels
<b>response</b>	Actions taken to respond to an emergency or disaster.
<b>resumption plan</b>	<i>See recovery plan</i>
<b>risk</b>	A chance or possibility of danger, loss, injury, or other adverse consequences.
<b>risk assessment</b>	Identification of risks to business process, safety, property, critical infrastructure and financial stability from natural, human-caused and technological sources/activities, and evaluation of the importance of the activity to the continued operation of the business.
<b>severity</b>	It is the potential or intensity associated with a hazard to disrupt normal operations and/or cause damage to an entity.
<b>shall</b>	Indicates a mandatory requirement.
<b>should</b>	Indicates a recommendation or that which is advised but not required.
<b>threat</b>	A person, thing or event regarded as a likely cause of harm or damage.
<b>will</b>	<i>See shall</i>

## Business Continuity Assumptions

1. A designated BCP Coordination Committee will be responsible for the facilitation of organizational coordination of certain resources and services as part of the BCP activation process.
2. Current emergency response plans, e.g., building evacuation, are found in site-specific emergency plans and are not part of the BCP process; however, emergency plans may be included as supporting plans
3. Regardless of circumstance, some key personnel will not be available to participate in continuity activities within the first 24 hours of a disruption incident.
4. The offsite (geographically separate location) locations housing critical backed-up data are intact and accessible.
5. Existing dependencies with vendors and affiliates have been identified and coordinated, and a current contact lists are maintained.
6. Team Members are available to perform critical functions defined within the plan.
7. Team Members can be notified and can report to the backup site(s) to perform critical processing, recovery and restoration activities.
8. Off-site storage facilities and materials survive the event
9. Branch support facilities including Support Centre and SMS (Securit Manufacturing Solutions) survive the event.
10. The disaster recovery plan is maintained with regard to training, testing and updating.
11. Subsets of the overall plan can be used to recover from minor interruptions
12. An alternate "hot site" facility (geographically separate location) is available or can be secured as necessary.
13. An adequate supply of critical forms and supplies are stored off-site, either at an alternate facility or off-site storage, or are readily available from an external source.
14. A backup site is available for processing the operations specific administrative work.
15. Cell phones (including radio, pagers, email and other auxiliary forms of communication will be available.
16. Surface transportation in the local area is possible.

## **Business Impact Analysis**

### *Summary of Operations*

#### **Branch Service Operations**

##### *Key Customers (Internal & External):*

###### External:

- Major Account
- Recurring
- Purge
- Recycling

###### Internal:

- Customer Service - Operations
- Office Administration
- Customer Security Representatives
- Sales

##### Customer or Business Requirements for Delivery of Products or Services:

Shred-it relies primarily on secure mobile shredding vehicles, secure collection vehicles and trained operating Customer Security Representative personnel to provide key, *secure* services to customers.

##### Highlights of key business requirements for the delivery of services are:

- Technical infrastructure, including Data and Voice systems
- Application Systems for Business Processes
- Operational Vehicle Fleet
- Branch Office Administration
- Finance Administration

## **Hazard Identification and Risk Assessment (HIRA)**

### Summary of Identified Core Risk Elements

- Prolonged power failure (core service area)
- Prolonged telecommunications failure (core service area)
- Fire – Catastrophic/Severe
- Technical hardware resource disruption (power flux, crime)
- Hurricane/Typhoon – impact and evacuation potential



**Disruption Time allowances**

<b>Branch Level - Critical Functions or Supplies/Utilities</b>	<b>Customer Impact (Hours)</b>	<b>Operation Impact (Hours)</b>	<b>Financial Impact (Hours)</b>	<b>Image Impact (Hours)</b>	<b>Maximum Acceptable Down Time (Hours)</b>
Telecommunications (Voice)	1	6	1	1	2.25
Facility/Facility Maintenance	24	6	12	12	13.5
Technical infrastructure (utilities, outside services, other)	1	12	1	120	33.5
Vehicle Fleet	24	0	72	120	54
SAP/ARP	24	1	72	120	54.25
Supplier (vehicle - fuel, fluids, other)	24	12	72	120	57
Telecommunications (Data)	24	12	72	120	57
Route Availability	72	1	72	120	66.25
AP/AR - Billings	120	240	72	120	138

# **Emergency Declaration and Plan Activation**

Levels of Emergency and Response Procedures

**General**

For the purposes of the Shred-it Business Continuity Plan, the process of emergency declaration and plan activation is dependent on the level of emergency considered. Partial, activation can be a precautionary step to provide operational mitigation for a potential emergency.

Emergency Declaration and Plan Activation will precede emergency asset activation such as the ECG and EOC.

**Authority to Activate**

The Shred-it Business Continuity Plan is activated by order of the Board of Directors, Senior Vice President Operations, Vice President Compliance, Regional Vice President or the District Manager responsible for the location of interruption.

**Activation Notification Protocol**

On appropriate authority to activate the Business Continuity Plan in either a full or partial capacity, a notification protocol must proceed to ensure all affected support parties can be alerted and engaged if necessary. This protocol is a primary step for Emergency Operations Center, Emergency Control Group, and Emergency Operations Site Team mobilization and/or engagement.

Pursuant to the level of emergency, the activating authority shall ensure contact is made to field operations sections including leadership of the Emergency Operations Site Team (if activation criteria permits) and senior members of the Shred-it regional, country, and global management teams as outlined in Figure – 1.1 below. The activating authority shall also contact the duty EOC member directly.

**Fig – 1.1 - Activation Notification Sequence**



**(Note: Activation authority may be provided at any point in the escalation process. In such cases, appropriate direction must be conveyed to field operations levels)**

The activating authority may make recommendations for escalation of the level of emergency and/or the application of Business Continuity Plan procedures and protocols based on the nature of the business interruption.

Levels of Emergency – General Criteria

	Plan Referral/Stand-by	Activation Considered	Activation Probable
Condition	Level I	Level II	Level III
<b>Threat or Injury to People</b>	No immediate threat to the people	Some injury or threat to people	Serious injury or fatality and/or ongoing threat to the public
<b>Containment within Company Property</b>	No threat to company facility infrastructure. No effects outside company property	Potential threat to company facility infrastructure. No immediate threat outside company property but the potential exists to extend beyond boundaries	Ongoing or imminent threat to facility infrastructure.  Effects extend beyond company boundaries
<b>Control of Product</b>	Control of released product is completed or pending	Imminent control of released product is likely but not yet established	Uncontrolled release of product continuing and control is not imminent
<b>Environmental Effects</b>	Minimal environmental effects	Moderate environmental effects	Significant and ongoing environmental effects
<b>Media Interest</b>	Little or no media interest	Local/regional media interest	National/regional media interest
<b>Response</b>	Incident is handled by company	First responders and government agencies are likely to be directly involved	Immediate and significant government agency involvement
<b>Potential to Escalate</b>	Low potential to escalate	Moderate potential to escalate based on potential for fire, explosion, increased release of product or other hazard	High Potential to escalate based on potential fire, explosion, increased release or other hazard

**Stand-by Alert**

At times, field emergency situations may not warrant the full or partial activation of the Shred-it Business Continuity Plan. In such circumstances, a Stand-by Alert may be directed.

Stand-by operations require steps to be taken to identify service impact levels and/or damage assessments. In some cases, a Stand-by Alert may prompt certain personnel to make provisions for activation.

**Authority for Stand-by Alert**

A Stand-by Alert may be issued by the District Manager, Regional Manager, or SVP as determined appropriate.

In cases where a Stand-by Alert is issued, notification shall extend to SVP as outlined in Figure – 1.2 below.

**Fig – 1.2 - Stand-by Alert Notification Sequence**



**Branch Operations Personnel Action Checklists**

Initial action checklists for key branch and support members have been included as part of this plan. These checklists outline critical processes that must occur pursuant to BCP activation and emergency declaration.

Included Critical Role Action Checklists

Title:	Type:	Response to:
First on scene	Stand-by or Activation	All levels emergency
District Manager	Stand-by	Level I emergency
District Manager	Activation	All levels emergency
Regional Manager	Activation	All levels emergency
Service Manager	Activation	All levels emergency

**Emergency Operations Support Action Checklists**

Emergency Operations support members, otherwise defined as members of the Emergency Control Group under the provisions of this plan hold action checklists approved by the BCP Management Team. Such checklists are held under separate cover as part of the corporate EOC protocol.

# **Emergency Operations Center**

Corporate – Support Centre

**General**

Provided the Business Continuity Plan has been activated to address a business interruption, Emergency Operations Center (EOC) activation shall occur. In cases of partial plan activation or Stand-by Alert as determined in the Emergency Declaration and Plan Activation Section partial EOC activation may be considered in lieu of full activity.

**Corporate EOC Location**

**Primary:** Shred-it Support Centre 1383 North Service Rd E, Oakville Ontario, Canada L6H 1A7 – Executive Board Room

**Secondary:** Shred-it Toronto 7040 Davand Drive Mississauga, ON L5T 1J5 – Board Room

**Third:** Shred-it USA Head Quarters 2355 Waukegan Road, Bannockburn, IL 60015

**Function and Purpose**

The primary role of the EOC is to function as a support utility and information hub for a field-based Emergency Operations Site Team.

**Central Point of Contact**

The EOC support staff acts as a clearinghouse for response and recovery information in support of the Emergency Operations Site Team (EOST). The EOST will call to report injuries; to update the progress in their area; to find a specific manager; to pass along media inquiries; etc. All actions and decisions that occur during the emergency operations and recovery phases of a business interruption will eventually be recorded at the EOC.

**EOC Key Functions**

- Recovery Team Notification and Support
- Administration and Records
- Resource Procurement
- Global Status Advisory
- Information Networking
- Media Relations (Direct to Public Information Officer)

**Authority to Activate**

The EOC is activated by order of the Board of Directors, Senior Vice President, Vice President, Compliance, Regional Vice President or the District Manager (pursuant to BCP activation) responsible for the location of interruption.

EOC Activation - General Criteria

Level of Emergency	Categories	Condition	EOC
Level II	Threat or Injury to people	There is non-serious injury to people.	No
		There is some threat to people with low potential consequence.	No
	Containment within Company Property	There is potential threat to company infrastructure.	No
		No immediate threat outside company property but the potential exists to extend beyond boundaries.	No
	Control of Product	Imminent control of released product is likely but not yet established.	No
	Environmental Effects	There are moderate environmental effects.	No
	Media Interest	There is local/regional media interest.	No
	Response	Other first responders and government agencies are likely to be directly involved.	Yes
Potential to Escalate	There is moderate potential to escalate based on the potential for fire, explosion, increased release or other hazard.	No	
Level III	Threat or Injury to People	There is serious injury or fatality of member of the public or company personnel.	No
		There is ongoing threat to the company personnel or the public.	Yes
	Containment within Company Property	There is ongoing threat to infrastructure.	Yes
		Effects extend beyond the company boundaries.	Yes
	Control of Product	Uncontrolled release of product is continuing and control is not imminent.	Yes
	Environmental Effects	There are significant and ongoing environmental effects.	Yes
	Media Interest	There is national/regional media interest.	Yes
	Response	Immediate and significant involvement of government agencies and other first responders.	Yes
Potential to Escalate	There is high potential to escalate based on the potential for fire, explosion, increased release or other hazard.	Yes	

**Emergency Control Group (ECG) Activation Notification Protocol**

Emergency Operations Center Staffing

Where EOC activation is required, the Emergency Control Group will respond to the EOC. Personnel attendance will vary based on the activation level required pursuant to the business interruption event.

Primary Contact

At all times, an EOC staff member shall be assigned as the primary contact person for EOC activation. This duty EOC staff member is centrally located in the Support Center and on call 24 hours a day, 7 days a week.



Current Duty EOC Staff Member

	Title	Phone	E-mail
Primary	BC Team Leader	Distribution Copy – Redacted	
Secondary	Director, Compliance		

*Members of the Emergency Control Group*

Shred-it EOC Emergency Control Group	
EOC Manager	BC Team Leader
Public Information Officer	Strategic Communications Specialist
Administrative Officer	Executive Administrator
Legal Services Officer	SVP General Council or Designate
Safety Officer	Health and Safety Specialist
Fleet Operations Officer	Fleet Manager*
Human Resource Officer	VP Human Resources or Designate
Security and Compliance Officer	Director, Compliance
Information Officer	Vice President Information Officer
Agency Liaison	<i>Designated as required</i>

\*Key Support to the EOST

Activation Notification Sequence

Once contacted, the duty EOC staff member will immediately contact the EOC Manger via telephone and proceed to the primary EOC. The notified EOC Manager is responsible for the initial Emergency Control Group (ECG) call out to all EOC Emergency Control Group members.

Staffing Determination

Staffing requirements are determined by the type of emergency and subsequent preliminary operations resumption plan execution. For level I and II type emergencies, activation levels are at the discretion of the EOC Manager. For the purposes of the Shred-it Business Continuity Plan, EOC activations for level I and II emergencies will be identified as “partial activations.” For level III emergencies, the EOC Manager shall engage all EOC members or designates for “full activation.”

**Activation Levels / Staffing**

<b>Level I</b>	The incident impacts, or is likely to impact, a number of critical functions and possible use of Recovery teams. <u>Staff:</u> EOC Manager on standby alert EOC staff on standby alert.
<b>Level II</b>	The incident impacts, or is likely to impact, a moderate number of critical functions and a limited use of Recovery Teams. <u>Staff:</u> EOC Manager EOC staff members. <u>Users:</u> Emergency Operations Site Team Leader
<b>Level III</b>	The incident impacts or is likely to impact a large number of critical functions and all Recovery Teams are activated. <u>Staff:</u> EOC Manager EOC staff members <u>Users:</u> Emergency Operations Site Team

**(Note: EOC Staffing requirements are determined according to activation level protocol. No non-EOC staff shall be permitted access to the EOC facility without the expressed approval of the EOC Manager.)**

EOC Arrival and Setup Protocol

On arrival to the EOC, all members shall contact the duty EOC member to confirm attendance. The EOC Manager shall immediately contact the activating official to confirm that the EOC is operational. If the activating official cannot be reached, the EOC Manager should page, e-mail, or communicate this message by other means if necessary.

On arrival, the Emergency Operation Center Manager (EOC) Manager shall assume control of EOC operations.

## **Emergency Control Group (ECG) Operations**

### Emergency Operation Center (EOC) Setup

All activated Emergency Operation Center (EOC) Members are required to assist in Emergency Operation Center (EOC) setup upon arrival to the primary location. Setup must occur as soon as practicable with priority given to communications utilities.

The duty EOC member is responsible for ensuring all EOC setup boxes are brought to the primary EOC site.

### EOC Supplies and Equipment

#### **Communications**

##### ***Portable***

12 Cisco IP 7941 Telephones  
 12 Cisco IP Phone Auxiliary Power Cables  
 3 Routers with Power Adapters 1 Fax Machine  
 1 Television

1 DVD Player AM/FM Radio ***Static***

4 Ethernet Ports  
 2 Telephones Ports  
 1 Cable Port  
 4 (2x) Power Ports

##### **Office Supplies - Portable**

1 (20x) Pencils  
 1 (20x) Pens  
 1 Manual Pencil Sharpener  
 15 Standard Paper Pads (white) 1 Box white board markers  
 1 white board eraser 1 roll masking tape  
 6 Flashlights with spare batteries

3 Boxes Printer/Copier paper  
 3 A-frame easels with white paper pads 3 White board easels  
 1 (100x) File Folders 1 Box paper clips  
 2 Rulers  
 2 Staplers  
 Additional Equipment as required

##### **Office Equipment - Static/Portable**

2 PC Printers  
 1 Photocopier  
 1 Three-hole punch 2 Tape recorders  
 12 Laptops (if not user supplied) 2 USP Power Supplies  
 Chairs as required Tables as required

**Documents**

**Print Preferred (12x)** Business Continuity Plan Recovery SOPs  
Payroll and Benefit SOPs Building Blueprints Maps  
Routing SOPs  
S&T SOPs  
Operations SOPs

Service Location Printout  
Routing report (if available) Daily route schedule (if available) Other Recovery SOPs  
Local Telephone Directory Branch Office Contact Lists  
Other Critical SOPs  
Health and Safety Manual

**EOC Physical Organization**

For optimal operations integrity, the EOC should be organized by the following:

- Communications Room
- Meeting Room
- Workspace for individual team representatives
- Media Center (off-site [if applicable])

**Communications Room**

This is the primary general operations space for EGC personnel. Dedicated Ethernet ports and primary communications utilities should be setup in this space. This room should have limited access to outside personnel and should be of sufficient quality to limit outside sound and/or communications interference.

**Meeting Room**

This is the dedicated space for all operations cycle meetings, EOC leadership meetings, and similar activities. This room should be equipped with an appropriate number of status boards, wall mounted presentation boards and white boards to track recovery progress, needs and hazard events. This room should have at least one television to monitor any media broadcasts detailing a given emergency.

**Team Workspaces**

Each EGC sub-group should be supplied with a workspace close to the EOC communication and meeting facilities. Such workspaces should be used for coordination, strategy, and private meetings.

**Media Center**

The Media Center should be located in a facility separate from the EOC. As part of the Media Center, briefing rooms, preparation workspaces, and associated utilities should be allocated. The facility designated as the Media Center should be setup to ensure press access and corporate communication facilitation.

**Support Level Personnel Notification**

The ECG holds primary responsibility for the notification of key support level staff. On arrival to the EOC, ECG personnel shall ensure that all support level managers with field operations level influence are contacted and briefed on situational parameters as provided in the preliminary EOST Situation Report.

Initial notification of key support level managers shall be logged in both personal log books and on the Key Manager Contact Notification Record. Ensure that the time, and call status is recorded. Be sure to leave room for multiple call logs if initial communication attempts are unsuccessful.

*Notification Message*

The EOC Manager shall inform ECG members of the appropriate message to distribute to key management personnel. This message should be subject to change as emergency information becomes more precise. ECG members shall ensure that an accurate record of the message is kept and when possible, this should be confirmed with the EOC Manager.

*Call-out Protocol*

All calls being made pursuant to emergency operations *notification* must start and finish with the words “This is an emergency message. This is not a drill.”

**Sample Emergency Notification Message**

“This is an emergency message. This is not a drill.

We are currently experiencing a service outage at \_ due to a \_ emergency. The Emergency Operations Center has been activated. You have been requested to participate in action to mitigate this business interruption.

This is an emergency message. This is not a drill.”

If the calling ECG member receives an answering machine, a brief message outlining the reason for the call must be left. It is critical to ensure that the individual is logged as a way and that the call-out protocol is followed.

Once a call has been made and the message delivered, the caller shall initial logged remarks.

**Administration and Records**

Record keeping during emergency operations is critical. During EOC operations, ECG members are required to keep personal logs as well as a general Operations Log. The owner of the Operations Log is the EOC Manager or designated scribe.

All operational information flowing through the EOC must be recorded concisely and reported to affected members accordingly. The General Message Form should be the primary information distribution tool.

*Point in Time Status Reporting*

Continual reporting and updating is required to maintain global understanding of emergency mitigation measures. The EOC Manager is primarily responsible for the maintenance of reporting scripts and ongoing point in time records.

All reporting completed pursuant to operations or emergency status shall be posted on reporting bulletin boards/white boards in order to ensure continued operational understanding in the EOC

#### *Information Tracking System*

In addition to point in time status reporting that aims to ensure universal working knowledge of a given situation, critical information tracking is also important. Information flowing into the EOC is varied based on the source and type. As such, separate logs, utility forms, and/or reporting may be kept for each possible input type.

The EOC Manager is responsible for establishing an information tracking system for critical information outside of the point in time reporting scope. The ECG will be responsible for the adherence to any formulated protocol.

#### *Unresolved and Ongoing Issues*

To ensure effective resource allocation in the EOC, unresolved issues shall be posted with point in time reporting notifications.

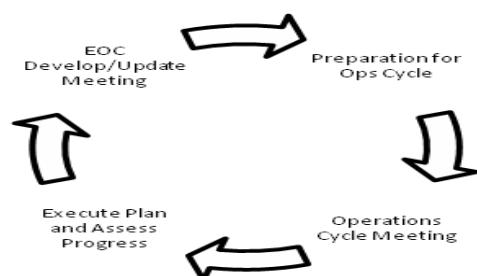
Information organized around ongoing and unresolved issues should focus on the following:

- Personnel (Field Operations)
- Personnel (EOST Staffing)
- Health and Safety
- Business Units
- IT Operations
- Service Operations
- Communications
- Equipment
- Purchasing
- Facilities
- Response/Recovery Situation
- Disaster situation (e.g. road closings, emergency declarations, storm conditions, losses, etc.)

#### EOC Operations Cycle

In order to ensure efficient and effective information dissemination during emergency management operations in the EOC, an emergency operations cycle is required. The emergency operations cycle is timed, recurrent meeting schedule that requires all members of the ECG to pause individual efforts and reconnect based on global directives defined by the EOC Manager.

**Fig 2 – EOC Operations Cycle**



*Operations Cycle Meeting*

EOC Operations cycles meetings shall occur on schedule determined by the EOC Manager. During the operations cycle meeting, all EGC personnel shall be in attendance unless absence is otherwise authorized by the EOC Manager.

*Operations Cycle Meeting Protocol*

- a. 15 minutes prior to the operations cycle meeting the EOC Manager shall instruct all EGC staff that the meeting is pending
- b. The EOC Manager shall chair the meeting
- c. The EOC Administrative member shall make note of the time and record minutes
- d. EGC members will provide briefing of operations current to the time of the meeting
- e. The EOC Manager shall record all operational elements pertinent to business resumption protocols and identify global strategy

*Cycle Timeline*

Typically, the operations cycle occurs hourly. However, frequency of meetings can increase or decrease depending on particular situations.

Resource Procurement

Resource request processing and procurement is one of the prime functions of the EOC. As such, all requests for resources must be logged, considered, and facilitated if such resources are designated as a requirement for emergency operations. As requests for resources flow into the EOC, appropriate EGC members shall ensure that they are applied to a resource specific log and posted to the unresolved/ongoing information boards.

**(Note: Critical requests must be marked as such. The EOC Manager should facilitate procurement of critical supplies as soon as practicable)**

Examples of requested resources include:

- |  |                                   |
|--|-----------------------------------|
| -Personnel (EOST)                      | -Health and Safety Supplies       |
| -Security Guards                       | -Food and Water                   |
| -Personnel (Operations)                | -Sanitary Equipment               |
| -Temporary Employees                   | -Replacement Production Equipment |
| -Supporting Vendors                    | -Auxiliary Vehicles               |
| -Supplies                              | -Computer Equipment               |
| -Replacement Office Supplies           | -Special Recovery Equipment       |
| -Recovery Supplies                     | -Furniture                        |
| -Computer Printer Paper, Invoice Slips |                                   |

### Global Information Action

As information is input through Emergency Operation Center ( EOC) communications channels, critical information must be conveyed to the appropriate management and associate parties for action. When information deemed to be critical is received by the ECG, such information shall be logged on the appropriate reporting board. Based on the posted information, the ECG Manager may require information to be actioned by an ECG member immediately. In such cases, it is the EOC Managers responsibility to list action taken on the appropriate recovery board.

Due to the fluid nature of business interruptions, personnel tasks may change. To ensure efficiency, task changes must be updated in the Operational Log as they occur.

As action items become resolved, the EOC Manager shall communicate or ensure communication of status to the EOTC Team Leader. Once resolution is communicated, the action item can be marked as resolved on the recovery board.

### Information Networking

Many circumstances require the efficient update of all ECG members. In such cases the General Message Form template should be used to convey information.

Information received via a General Message Form shall be logged by the receiving ECG member and updated on the recovery board as necessary.

**(Note: The General Message Form is a universal template. This form can be used for field information transmissions to the EOST or members of the company outside the ECG. All communications made on the General Message Form template are to be logged as communications entries.)**

### Media Relations

During a business interruption where the Business Continuity Plan has been activated, all media requests for information and/or situation updates shall be forwarded to the Public Information Officer via the Emergency Operation Center (EOC).

No ECG member, employee, or contractor is permitted to speak to any member of the media without written consent from the Public Information Officer or designate.  
Refer to the Crisis Communications section for information on media information relay and public information protocols.



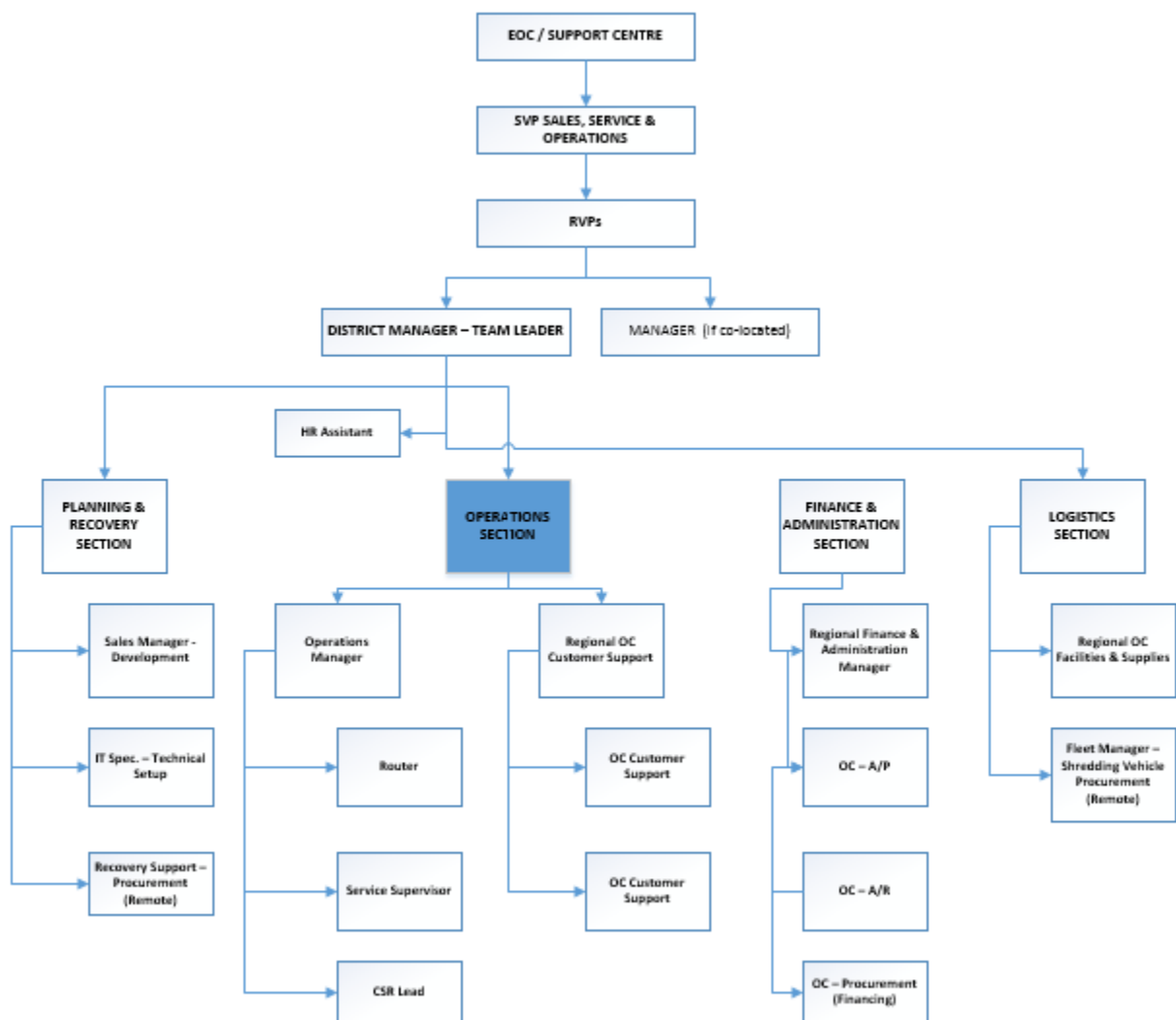
# Emergency Operations Plan

Emergency Operations Site Team and Response

### Emergency Operations Site Team (EOST)

The Emergency Operations Site Team is organized to provide the most effective operational capacity in instances of displacement or other business interruption. While organized atypically to regular Shred-it branch structures, this team-based model allows for service operations to continue with direct customer support while utilizing all regular branch personnel. The section specific positions outlined serve to support operational functions.

An important element of the EOST is the support relationship with surrounding Shred-it branches, the EOC, and assisting departments at the Support Centre. While primarily structured to deliver service operations, the structure is supported by teams facilitating ‘return to normal’ efforts.



The EOST is scalable to the scope of the business interruption and may be altered by the Regional Vice President, District Manager, or designate controller of the team. Depending on branch capacities and functions beyond regular service operations, additional leadership elements can be added under any of the four section groups as required.

**Team Directive**

The primary directive of the Emergency Operations Site Team is the resumption of business processes. Relocation, service routing, and administrative operations are the priority tasks of personnel designated as EOST members.

**Post Emergency Team Coordination/Activation**

During the initial days of a business interruption, the EOST role expands depending on the particular emergency phase and/or scope of the business interruption. As such, the initial response phase requires activation and coordination of EOST sections as soon as practicable.

**BC Phases and Timeline for EOST Coordination**

Phase	Actions	Involvement
Emergency Response Phase (0-6 hours)  EOST ACTIVATION	<ul style="list-style-type: none"> <li>* Deal with Incident</li> <li>* Life &amp; Safety issues</li> <li>* Property protection</li> <li>* Communicate with staff &amp; Central teams/management</li> </ul>	<ul style="list-style-type: none"> <li>*EOST</li> <li>*Communications</li> <li>*Management</li> <li>*Staff</li> <li>*Fire Wardens/First Aiders</li> <li>*Business Continuity Team</li> </ul>
The Utilization of emergency procedures beyond the scope of the BCP is permitted for purposes of life safety and property		
Crisis Management Phase (1 hour – 7 days)  EOST OPERATION	<ul style="list-style-type: none"> <li>* Invoke the Plan &amp; deal with:                             <ul style="list-style-type: none"> <li>- Human Resources issue</li> <li>- Coordinate with EOC</li> <li>- Property salvage &amp; restoration</li> </ul> </li> <li>- Set up alternative working arrangements at a temporary recovery site</li> <li>- Set up alternative office</li> <li>- Channel Media requests</li> <li>- Communicate with clients, staff, management</li> <li>- Restore infrastructure (data &amp; communications)</li> </ul>	<ul style="list-style-type: none"> <li>*Emergency Controller</li> <li>*Communications</li> <li>*Business Continuity Team</li> <li>*EOST</li> <li>*Infrastructure Recovery Team</li> <li>*Business Recovery Teams</li> </ul>
Business Recovery Phase (2 days – 30 days)	<ul style="list-style-type: none"> <li>*Recover key functions in priority order of urgency</li> </ul>	<ul style="list-style-type: none"> <li>*Business Continuity Team</li> <li>*Communications</li> </ul>
EOST OPERATION (Return to Normal)	<ul style="list-style-type: none"> <li>*Involve Support Centre staff as necessary</li> <li>*Keep clients advised</li> <li>*Return to normal working at the alternative office</li> </ul>	<ul style="list-style-type: none"> <li>*Infrastructure Recovery Team – Operations/Procurement</li> <li>*Business Recovery Team</li> <li>*Departmental Managers</li> <li>*Regional Staff</li> </ul>

**Leadership Authority/Action**

Specific action undertaken with regard to coordination and activation of the EOST is the responsibility of the Regional Vice President, District Manager or designate. The table (Fig – 5) outlines potential events that may trigger EOST activation. Generally, the EOST will only need to be activated if emergency circumstances require offsite operation or if external circumstances are such that regular operations cannot commence without significant changes to service operation routing.

For smaller emergencies that do not require significant operational adaptation, Shred-it localized emergency procedures are to be utilized. In such circumstances, support level assistance can be made available if EOC operations have yet to commence.

**Activation of the EOST**

Level of Emergency	Categories	Condition	EOST	Local procedure
<b>All Levels</b>	Property Loss	Facility or primary facility functionality disrupted by event	Yes	Yes
	Threat or Injury to people	There is non-serious injury to people.	No	Yes
		There is some threat to people with low potential consequence.	No	Yes
	Containment within Company Property	No immediate threat outside company property but the potential exists to extend beyond boundaries.	No	Yes
	Control of Product	Imminent control of released product is likely but not yet established.	No	Yes
	Environmental Effects	There are moderate environmental effects.	No	Yes
	Media Interest	There is local/regional media interest.	No	Yes
	Response	Other first responders and government agencies are likely to be directly involved.	No	Yes
	Potential to Escalate	There is moderate potential to escalate based on the potential for fire, explosion, increased release or other hazard.	Yes	No

## Activation Protocol

### Emergency Response Phase – INOPERABILITY

***Use this protocol when circumstances prohibit use of regular facility or disable regular routing operations from static branch location.***

*Prior to any action with regard to activating the EOST the branch District Manager or designate shall ensure that all personnel are made safe pursuant to standing emergency procedures and protocols.*

Immediate actions to be taken by the District Manager or designate:

#### *Normal Business Hours Response*

1. Determine extent of loss or interruption
2. Contact Regional Vice President, District Manager or member of the Business Continuity Team
3. Assess EOST personnel availability
4. If instructed by EOC engage notification procedure – contact all branch personnel (Utilize branch contact list included in this document)
5. Instruct EOST personnel to report to primary alternate operations site

#### *After Normal Business Hours Response*

When notified by the Emergency Management Team that the Business Resumption Plan has been activated, the team leader will:

1. Determine extent of loss or interruption
2. Contact Regional Vice President, District Manager or member of the Business Continuity Team
3. Assess EOST personnel availability
4. If instructed by EOC engage notification procedure – contact all branch personnel (Utilize branch contact list included in this document)
5. Instruct EOST personnel to report to primary alternate operations site

### Emergency Response Phase – ALTERED OPERATIONS

***Use this protocol when circumstances require substantially altered operations, but emergency has not disabled facility.***

***Prior to any action with regard to activating the EOST the branch District Manager or designate shall ensure that all personnel are made safe pursuant to standing emergency procedures and protocols.***

Immediate actions to be taken by the District Manager or designate:

#### *Normal Business Hours Response*

1. Determine extent of loss or interruption
2. Contact Regional Manager or member of the Business Continuity Team
3. Assess EOST personnel availability

#### 4. Notify all EOST personnel that immediate situation briefing is required

##### Call-out to EOST Members

Utilizing the EOST team member contact list found in the appendix, contact shall be attempted with every member of the branch staff. Personnel assigned to this communication task should convey the following:

- Brief description of the business interruption type and severity
- Location of the primary recovery site (if applicable)
- Mitigation action currently under way
- Regular facility status
- Meeting location and time of EOST team meeting
- EOST Team Members must wear valid Shred-it identification at all times while on duty
- Contact with any member of the media regarding Shred-it business operations is prohibited

All information must be conveyed directly to the EOST Team Member. At no time shall the assigned caller leave a message with an alternate individual. If a message must be provided, callers shall provide instruction to return the call.

Record must be made of each call outlining employee status. Upon task completion, the record of calls must be submitted to the EOST Team Leader

##### Guidelines for Travel to the Business Recovery Site

The majority of emergencies resulting in business disruption have a limited footprint. As such, in situations where an alternate recovery site is required to carry on service operations a Shred-it branch local to the affected area will be used as a primary recovery site.

The EOST leader should provide directions to the personnel that will be traveling to the backup site. In the event that personnel cannot drive to the backup site and will need air transportation, hotel accommodations, and advance expense money, the team leader should arrange the details through the Administrative team leader or EOC Manager.

The team leader will provide the Administration team leader or EOC Manager with the names of the individuals, their destination, hotel requirements, an estimate of any travel money needed.

The EOC Staff will make the travel arrangements and will provide personnel with itineraries, tickets, and advance travel money.

**Primary Location – Branch Specific**

<b>Facility Name:</b>	
<b>Street Address:</b>	<b>Floor:</b>
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No:</b>
<b>Alternate Contact:</b>	<b>24 Hour No:</b>
	<b>FAX No:</b>
	<b>Other No.:</b>
<b>Considerations:</b>	

**Alternate Location**

<b>Facility Name:</b>	
<b>Street Address:</b>	<b>Floor:</b>
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No:</b>
<b>Alternate Contact:</b>	<b>24 Hour No:</b>
	<b>FAX No:</b>
	<b>Other No.:</b>
<b>Considerations:</b>	

**EOST Operational Requirements**

The EOST Operational Requirements are based on emergency operations best practices. In the event of an actual emergency, circumstances may require some of the steps documented to be altered. Procedural alteration is at the discretion of the EOST Team Leader.

Business Resumption Plan Distribution

Immediately following EOST activation, the team leader shall ensure that all members are provided with a copy of the Business Resumption Plan section of the Shred-it Business Continuity Plan

Contact Information

Each member of the EOST shall be given a complete listing of EOST contact information. Pertinent ECG and support level manager contact information shall also be posted

EOST Initial Recovery Protocol

1. EOST Team Leader will contact EOC Manager once confirmation of EOC setup is received. (For partial activations, communications may flow through the Regional Manager)
  - Determine communications equipment status (if disabled)
  - Determine data coordination with secondary location (if applicable) for service operations continuity

2. Call out to EOST Team Members by Section leaders (call tree defined by EOST Operational Structure)
3. EOST Team Leader will organize a team meeting to outline the EOST function, highlight roles and responsibilities (included in this section) and highlight key operational priorities
4. Determine personnel travel and accommodation requirements for recovery site operation (if required) and complete a Personnel Location Control Form
5. Distribute copies of the Business Resumption Plan
6. Distribute copies of the Primary and Secondary recovery site location address and directions
7. EOST Team Leader will contact the coordinating District Manager (if required) to arrange shared workspace provisions
  - **Determine workspace requirements**
  - **Determine equipment requirements (use Equipment Request Form as part of the Status Report to engage EOC for procurement)**
  - **Determine any additional personnel requirements (Operations and Support Sections)**
8. EOST Team Leader will provide direction for EOST member activation
  - **Section setup and location at the discretion of the EOST Team Leader**
9. EOST Team Leader will designate personnel to initiate contact with impacted vendors

#### Status Report

The EOST team leader shall ensure a written status report is submitted to the EOC Manager at least every 24 hours or pre-determined operational period. Use the Status Report Form in the appendix as a guide.

#### Personnel Location Form

After EOST deployment, the EOST Team Leader shall complete the Personnel Location Form found in the appendix. This form must be forwarded to the EOC Manager and to the Administrative Section Leader. In the event that an employee's accommodation or contact information changes, a revised Personnel Location must be completed and submitted.

#### Travel Arrangements

The EOST Team lead may require additional personnel to attend the primary operations site to facilitate auxiliary operations. In such cases, travel arraignments may be required. The EOST team leader may request EOC assistance to schedule travel and accommodation by utilizing the Travel Request Form found in the appendix.

#### Vendor Notification

Upon activation of the EOST Team Leader shall prepare a statement to be forwarded to any branch vendors identifying this business interruption.

**(Note: Any external communications must be approved by the Public Information Officer as part of the Crisis Communications Plan)**



**EOST Member General Responsibility Outlines**

Included below are general responsibilities for members of the (on site) EOST. Provisions for support services exist in separate, department controlled auxiliary support plans.

*EOST Team Leader (District Manager or designate)*

1. Coordinate emergency operations with ECG and EOST Unit Leaders and staff
2. Develop and coordinate objectives, set processes and strategies for business unit optimization.
3. Maintain branch budget for optimal emergency recovery.
4. Manage resources (financial, technical, people, infrastructure) and ensure that schedules/ timelines for branch or emergency secondary site are executed in order to support business continuity outcomes.
5. Oversee overall service delivery on all customer needs within the branch; conduct a strategic assessment of current and future customer needs within the local business market and across the region with the support of the Planning Unit.
6. Oversee the resolution of all issues within the branch and ensure that highly critical issues regularly outside of established procedures are resolved; refer, with highly respected recommendations, strategic issues with regional and/ or broader organizational implications to the Regional Manager and ECG.
7. Develops and recommends creative modifications to branch emergency processes.
8. Provide input and recommendations for regional recovery strategies to the ECG.

*Operations/Facility/Transportation Manager*

1. Responsible for the processing of supplier invoices for payment in a timely fashion.
2. Process and summarize daily services and submit to EOST Team Leader and Transportation Supervisor (TS) daily.
3. Maintain, track, process truck work orders and update truck summaries and period cost summaries for EOST Team Leader and TS weekly.
4. Verify Route Sheets with corresponding invoices for daily CSR service operations.
5. Other duties as assigned pertaining to the effective operation and coordination of the branch.
6. Communicate with the CSRs on any special services for the day
7. Coordinate auxiliary services personnel and dispatch to other supporting CSRs for full service recovery.
8. Contact customers for carry-overs to reschedule per standard SOP.
9. Co-ordinate carry-overs by 3:00 p.m. daily and submit to TS for next day run sheets.

*Transportation Supervisor*

1. Prepare and distribute daily work schedules for CSR
2. Resolve service problems associated with emergency routing detours and/or delays
3. Available for support for CSRs before, during, and after regular shifts
4. Prepare Routing / Route audits of client calls so as to ensure optimization of return on assets and client satisfaction.

5. Fleet Maintenance of all vehicles of the Branch
6. Review CSR Log Sheets daily and take corrective action as appropriate
7. Monitor on road observations of CSRs to ensure safety and any concerns are addressed

#### *Sales Manager*

1. Optimizing efficiency and performance of the sales team in business recovery capacity.
2. Development and implementation of business resumption protocols and.
3. Execution of the Crisis Communications Plan in conjunction with the EOST Team Leader.
4. Manage ongoing relationships with information management groups to promote the brand.
5. Participation in EOST operations cycle meetings and projects.
6. Management ongoing client relationships in order to develop customer loyalty, retention and increase revenue through Account Development Reps.

#### *Branch Accountant*

1. Optimization and performance of EOST financial administration
2. Development and implementation of process and systems improvements.
3. Participation in EOST business cycle meetings and projects.
4. Provide Sales and Operational Support as required.
5. Oversee branch payroll and benefit information accurately and in a timely manner.
6. Oversee and maintain vendor management for the procurement of recovery supplies

# **Crisis Communications Plan**

Media Relations Protocol

**General**

The manner in which Shred-it conveys information during a business interruption situation is extremely important to the global understanding and perception of how the company is handling the situation. Every effort must be made to provide the media, the team members and most importantly, our customers that Shred-it is in complete control of continuity and recovery efforts and that every possible measure has been taken to ensure that we can provide the appropriate levels of service in the most expeditious manner.

**Policy**

In the event of a major business interruption, Shred-it SVP, Marketing & Customer Experience will designate a Strategic Communications Specialist who will oversee and co-ordinate all public and media information related to business continuity activities. In addition, it will be the responsibility of the Strategic Communications Specialist to ensure that the Executive committee is kept up to date with recent developments and the proper of continuity media-related activities.

If asked for comment regarding the business interruption, branch-level personnel shall refer all media enquiries to the Strategic Communications Specialist at or the Communication Team located at the Shred-it Support Centre (905) 829-1999. Specific contact information relating to those who are authorized to speak with the media is shown below:

Title	Role	Work#	Cell #	Home#
SVP, Marketing & Customer Experience	Executive Media Relations Support	<b><i>Distribution Copy - Numbers Redacted</i></b>		
Sr. Manager, Public Relations & Communications	Public Information Officer			
Manager, Brand Strategy	Alternate Media Relations Liaison			

*Notes:*

1. Unless otherwise specified, the area code will be 905.
2. The SVP, Marketing & Customer Experience or the Sr. Manager, Public Relations & Communications may authorize additional individuals to speak with media based on both the nature and severity of the event.

**External Communications**

In the rare cases where an incident disrupts or otherwise ceases regular customer service operations for a period of 24 business hours, Shred-it Corporate Communications will develop a written statement to be posted on the external website. Such statement will be forwarded to media agencies upon request.

*Note: Media correspondence will be delivered in the standard Shred-it media release format according to existing communications policies and protocols.*

Information contained in media release messages will include:

- a. The nature and extent of the event.
- b. The number of services affected and possible duration of disruption (this needs to be carefully coordinated to ensure that accurate and timely information is being relayed).
- c. The measures being taken to restore services and projected continuity of interim services.
- d. Any pertinent customer related instructions

In cases of widespread or long-term disruptions to service operations due to circumstances external to Shred-it and media coordination will occur through the EOC’s media center.

Information requests relayed through the EOC will be the responsibility of the Public Information Officer (Strategic Communications Specialist). In addition to participating in EOC operations cycle meetings, the PIO is required to submit a Daily Major Event Log to the EOC Manager summarizing media events

Updates will be issued regularly, especially during the initial stages of the continuity and recovery process. A tentative schedule is shown below:

<b>Communications Schedule</b>	
<b>Timeline</b>	<b>Communication type</b>
<b>48 hours</b>	<b>Media release – posted to Shredit.com</b>
<b>72 hours</b>	<b>Media update – posted to Shredit.com</b>
<b>2 Weeks</b>	<b>Webcast – posted to Shredit.com</b>
<b>3 Weeks</b>	<b>Written Letter to all client main contacts</b>
<b>To full recovery of service</b>	<b>Media release – posted to Shredit.com on required basis</b>

Realizing that a great deal of information can be passed electronically, when possible, Shredit.com will be updated daily. Specific situations requiring updates action can include the following:

- a. where changes to previous announcements related to the provision of services must be made;
- b. Where clarification of erroneous reports from the media is required.

### **Internal Communications**

Internal communications can increase global concern and result in incorrect information release if managers are not fully cognizant of information protocols. All personnel involved in internal communications with regard to a business interruption must be fully aware of situation status and the process that should be followed within Shred-it to facilitate business resumption efforts.

When phoning team members on the established contact lists, the following guidelines should be used:

- a. If the staff member is contacted: Advise them of the event prompting the call and provide them specific instructions on where they are to go and appropriate actions that they should take. Remind the team member of the policy regarding media requests and who is responsible for responding to any media requests.
- b. If the staff member is not contacted: Leave a name and number where you may be contacted and ask that the team member contact you as soon as possible. You should not leave any detailed messages as these are easily misinterpreted, which can lead to future difficulties.

*Note:*

*All internal communications pertaining to a service interruption or emergency situation where the EOC has been activated are subject to approval by the VP, Human Resources or designate member of the EOC.*

### Existing Communication Directive

This plan was developed to supplement existing detailed communications plans that are held and maintained by Shred-it Communications.

In cases of BCP activation, existing communications plans will be utilized to supplement on-going media relations efforts.

# **Business Resumption Plan**

Recommencement of Service Operations

**Interacting Business Unit Priorities**Key Process Resumption Protocols  
Service Operations

<b>Key Support Level Units – Customer Service Operations</b>						
Department	Systems and Operations to be Actioned FIRST	Specific Timeline	Systems and Operations to be Actioned SECOND	Specific Timeline	Systems and Operations to be	Specific Timeline
IT	Technical Infrastructure (i.e. telecommunications phone/data)	4 Hours	SAP and ARP to alternate Hot site (if required)	8 Hours	Hardware Setup	10 Days
National Accounts	Optimize Service Request Distribution	12 Hours	Service Request Re-distribution to Hot site(s) (if required)	24 Hours	Customer Contact Re: Service Timelines (if impacted)	48 Hours
Payroll	Determine Employee Scheduling	24 Hours	Manual Payroll Input	48 Hours	Reroute Ceridian Output	72 Hours

<b>Branch Level Units – Customer Service Operations</b>						
Department	Systems and Operations to be Restored FIRST	Specific Timeline	Systems and Operations to be Restored SECOND	Specific Timeline	Systems and Operations to be Restored THIRD	Specific Timeline
Office Administration	Client Service Support	4 Hours	Invoice closing	48 Hours	Post Payment A/R - Collections	1 week
Operations	SAP ARP Database Scheduling	16 Hours	Routing systems	24 Hours	Vehicle Operations	36 Hours

**Interacting Business Unit Priorities**Data Center Utility

(Reference Data Center Recovery Processes in Corporate Information y Plan)

<b>Key Support Level Units – Customer Service Operations</b>						
Department	Systems and Operations to be Actioned FIRST	Specific Timeline	Systems and Operations to be Actioned SECOND	Specific Timeline	Systems and Operations to be Actioned THIRD	Specific Timeline
TBD	TBD	TBD	TBD	TBD	TBD	TBD



**Business Unit – Information Technology**

*Type: Support Level Operation*

**Recovery Processes**


*Interruption Mitigation Objective:*

Restoration of telecommunications and technical infrastructure including employee database (SCII) and routing systems, if required.

**Business Unit Processes/Activities**

- Information Technology**
  - **Technical support and assistance to field operations through remote connection and on-site control**
  - **Data warehousing and central server maintenance**
  - **Hardware support**
  - **Information y protocol development and system maintenance**

**Initial Response**

Treatment	Details
	Primary emphasis shall be placed on reactivation of primary data and voice telecommunications utilities.  If primary business operations location is not viable for continued technical operations, procedures to switch communications shall be executed.
<b>ORGANIZATION(S) RESPONSIBLE</b>	Information Technology Department Core Partners: Verizon Cogix Virtustream Microsoft (Cloud)
<b>COMMUNICATION</b>	Communication protocol (separate to this plan) executed. Affected EOSt team lead primary contact for setup requirements

**Interim Processing**

Treatment	Time to Achieve	Additional Comments
1. Restoration of telecommunications infrastructure <ul style="list-style-type: none"> <li>● (phone/data) and/or;</li> <li>● transfer of primary communications utilities to hot site</li> </ul>	4 Hours	EOST will set core vendor and team requirements based on specific underlying situation details. Virtually all Shred-it infrastructure is provisioned and managed by the internal IT team and core vendor team summarized above so most response requirements can be actioned from within this set of resources.
2. SAP and ARP setup (if necessary) <ul style="list-style-type: none"> <li>● Technical assistance for primary hot site setup</li> <li>● Data recovery from primary server backup</li> <li>● Ongoing system maintenance and troubleshooting</li> </ul>	Ongoing	All mission critical Shred-it business systems are physically held at the Shred-it Data Center. This means that branch or region levels events will typically require continuity actions for <u>access</u> only to systems, not recovery of the systems themselves.  There may be alternative situations that require a more robust response and specific situations involving franchise service order execution systems.
3. Hardware Setup <ul style="list-style-type: none"> <li>● Order technical components from vendor</li> <li>● Hardware setup</li> <li>● Distribution to field</li> <li>● Ongoing maintenance and troubleshooting</li> </ul>	~ 10 Days	Timeline and cost dependent on loss type and severity. Required deliveries from national hardware vendors.

**Restoration**

Treatment	Time to	Additional Comments
1. Technical re-routing and repair <ul style="list-style-type: none"> <li>● Advanced operability hardware transferred to primary</li> <li>● Troubleshooting and setup of components</li> </ul>	2 Days	May require the use of external vendor
2. SAP and ARP restoration to normal <ul style="list-style-type: none"> <li>● Branch operations to transfer data to primary via regular PC</li> </ul>	24 Hours	Data backup from interim phase exists on acquired hardware

3. Restoration of Telecommunications infrastructure to primary site (if applicable) <ul style="list-style-type: none"> <li>• transfer of primary communications utilities to primary site</li> </ul>	4 Hours	Technical assistance required from US telecommunications vendor: Frontier. Refer to Frontier services manual for process guidance
--	---------	---

**Contact List**

	Name	Title	Special Responsibility	Phone / Home Address <i>(o) Office (h) Home (m) Mobile (f) Fax Address</i>
<b>Unit Team Leader</b>	<i>Redacted</i>	<i>Sr. Manager Business Enablement</i>	<i>IT systems maintenance and emergency identification</i>	<i>Distribution Copy – Redacted</i>
<b>Alternative Unit Team Leader</b>	<i>Redacted</i>	<i>Senior Technical Engineer</i>		
<b>Team Member responsible for maintenance of plan</b>	<i>Redacted</i>	<i>Sr. Manager Business Enablement</i>	<i>Plan maintenance and alternate</i>	

Business Unit – Operations

*Type: Branch Level Operation*

*Interruption Mitigation Objective:*

Restoration of vehicle routing operations pursuant to SCII pre-interruption scheduling necessities

**Business Unit Processes/Activities**

- Branch Operations**
  - **Scheduling and CSR Assignments**
  - **Invoice (COD)**
  - **Routing and deployment assignments**
  - **Travel and Customer Service (Field)**
  - **COD distribution and return for processing**
  - **Vehicle maintenance**

**Initial Response**

<b>Treatment</b>	<b>Details</b>
------------------	----------------

<b>RESUMPTION OF ROUTING AND VEHICLE OPERATIONS</b>	Primary emphasis shall be placed on vehicle-based operations pursuant to pre-scheduled service dates and routing coordination. If primary business operations location not viable for continued vehicle service operations procedures to re-locate operational utilities including vehicles will be executed.
<b>ORGANIZATION(S) RESPONSIBLE</b>	Branch Operations Department Fleet Management Department (Support Centre) EOST Operations Department
<b>COMMUNICATION</b>	Communication protocol executed. Affected EOST team lead primary contact for setup requirements

**Interim Processing**

<b>Treatment</b>	<b>Time to Achieve</b>	<b>Additional Comments</b>
1. Confirm operations location viability <ul style="list-style-type: none"> <li>• If regular service operations facility impacted, make provisions to re-locate to primary operations site per EOST procedure</li> <li>• Contact IT Unit Leader to determine routing system re-location requirements</li> <li>• Obtain all technical tools (computers, telephones) necessary to facilitate routing operations and/or inform IT Unit Leader of requirements</li> </ul>	1 Hour	Supporting IT systems to be forwarded to (hot site) automatically. IT Support availability to assist.
2. Confirm available CSRs and Vehicles <ul style="list-style-type: none"> <li>• Utilize internal call out procedure (if duty hours using two- way cellular phones, if after hours utilizing branch telephone directory)</li> <li>• Determine operational vehicle allotment</li> <li>• Determine needs based on vehicle allotment</li> <li>• Contact Manager, Fleet Operations to determine vehicle distribution allowances</li> </ul>	4 Hours	If staffing or equipment deficiencies prohibit adequate routing additional employees and vehicles will be temporarily tasked to assist
3. Routing and Service Assignments <ul style="list-style-type: none"> <li>• Utilizing SCII/ARP upload to hot site generate customer service schedule for lost days (primary) and current customers (secondary)</li> <li>• Utilizing ARP determine routing requirements and assess vehicle/CSR capacity</li> </ul>	24 Hours - Ongoing	

<p>4. Vehicle Service Operations</p> <ul style="list-style-type: none"> <li>• CSRs to complete service on pre-assigned routes</li> <li>• Re-evaluate routing based on performance and misses CSR return COD to primary backup site (hot site) for processing</li> </ul>	<p>36 Hours – Ongoing</p>	<p>If vehicle operations are delayed longer than 48 hours, sales office administration department shall initiate customer contact</p>
<p>5. Paper Recycling</p> <ul style="list-style-type: none"> <li>• Site baler to be utilized (if equipped)</li> <li>• EOST to designate approved vendor in area (same as used by hot site) as recycler if primary unavailable</li> </ul>	<p>24 Hours - Ongoing</p>	<p>Local vendor agreement will be in place per secondary (hot site) branch operation</p>

**Restoration**

Treatment	Time to Achieve	Additional Comments
<p>1. Vehicle Operations Re-routing</p> <ul style="list-style-type: none"> <li>• Route vehicles to finish at primary operations site</li> </ul>	<p>24 Hours</p>	
<p>2. Return to Normal Routing</p> <ul style="list-style-type: none"> <li>• Execute movement of Scheduling utilities to primary location</li> <li>• Re-establish routing (if equipped)</li> </ul>	<p>24 Hours</p>	<p>SAP/ARP updated automatically as it is secured database resource</p>
<p>3. Evaluate Schedule and Routing (Customer Service Compliance)</p> <ul style="list-style-type: none"> <li>• Return supplemental vehicles (if equipped) to originating location</li> </ul>	<p>36 Hours</p>	

**Contact List**

	Name	Title	Special Responsibility	Phone / home Address <i>(o) Office (h) Home (m) Mobile (f) Fax Address</i>
<p>Unit Team Leader</p>				

Alternative Unit Team Leader	<i>Distribution Copy - Redacted</i>
Team Member responsible for maintenance of plan	

Business Unit – Sales Office Administration

*Type: Branch Level Operation*

*Interruption Mitigation Objective:*

Restoration of operations support capabilities and customer support activities

**Business Unit Processes/Activities**

- Office Administration**
- **Customer Service**
- **Facilities Support**
- **Customer Setup (SAP)**
- **Invoice Closing (SAP)**
- **Post Payment and Collections**

**Initial Response**

Treatment	Details
<b>RESUMPTION OF CLIENT AND OPERATIONS SUPPORT ACTIVITIES</b>	Primary emphasis on client services tasks and operations/finance support  If primary business operations location not viable for continued client service operations procedures to re-locate operational utilities and keystaff will be executed
<b>ORGANIZATION(S) RESPONSIBLE</b>	Sales Office Administration Operations Department Regional Sales Office Administration Support Team
<b>COMMUNICATION</b>	Active external communication with clients will be tasked through the Communications Department per the Communications Plan. Client communications regarding service delays shall occur 24 hours after first delay if scheduling cannot accommodate service within 48 hours.

**Interim Processing**

Treatment	Time to Achieve	Additional Comments
1. Continued Passive Client Service Support <ul style="list-style-type: none"> <li>● SOC personnel to continue answering telephones and answering other customer communications during interruption</li> <li>● If telecommunications are inoperable then alternate site must be considered</li> </ul>	4 Hours - Ongoing	Pursuant to adequate communications utilities
2. Active Client Service Support <ul style="list-style-type: none"> <li>● Contact customer per standard SOP and Service Level Agreement to inform of any delays exceeding 1 week</li> </ul>	48 Hours	Corporate communications via EOC will accommodate media requests for information.
3. Invoice Closing <ul style="list-style-type: none"> <li>● Apply COD invoices to SCII system per existing SOP</li> <li>● Resolve any CSR / Service invoicing discrepancies</li> </ul>	48 Hours - Ongoing	Tasking can be transferred to alternate branch in the event of temporary systems failure.
4. Post Payment A/R – Collections <ul style="list-style-type: none"> <li>● Run Daily Invoice History Report Post payments on continuing basis</li> <li>● After 30 days initiate active collections per branch SOP</li> </ul>	1 week – Ongoing	Tasking can be transferred to alternate branch in the event of temporary systems failure.

**Restoration**

Treatment	Time to Achieve	Additional Comments
1. Facilities setup and resource procurement <ul style="list-style-type: none"> <li>● Per direction of EOC determine resource requirements prior to customer service and operations support activities transfer to primary location</li> <li>● Arrange deployment of required resources prior to administrative shift back to primary location</li> <li>● Coordinate with IT Unit Leader to ensure SCII utilities backed up in database</li> </ul>	48 Hours	

2. Administrative record recovery <ul style="list-style-type: none"> <li>• Ensure branch records collected and (SCII) inputs are up to date</li> <li>• Print (SCII) report outputs (collections, customers, service) for confirmation of Return to normal</li> </ul>	3 Hours	Networked SCII may not have any anomalies. This operation is preventative
3. Return to normal <ul style="list-style-type: none"> <li>• Upon startup of SCII systems confirm report outputs are congruent with those printed prior to RTN</li> </ul>	3 hours	

**Contact List**

	Name	Title	Special Responsibility	Phone / Home Address (o) Office (h) Home (m) Mobile (f) Fax Address
Unit Team Leader	<i>Distribution Copy - Redacted</i>			
Alternative Unit Team Leader				
Team Member responsible for maintenance of plan				

Business Unit – Major Accounts  
 Type: Support Level Operation

*Interruption Mitigation Objective:*  
 Major Account client service support services and branch scheduling assistance

**Business Unit Processes/Activities**

- National Accounts
  - National Account client services
  - Service distribution
  - Location setup (roll out)
  - Service Operations data collection
  - National Account Billing

**Initial Response**



Treatment	Details
<b>RESUMPTION OF CLIENT AND OPERATIONS SUPPORT ACTIVITIES</b>	Primary emphasis on client services tasks and operations/finance support Service request re-distribution based on secondary location and/or service area of impacted location(s)
<b>ORGANIZATION(S) RESPONSIBLE</b>	National Accounts Department / Branch Operations Department
<b>COMMUNICATION</b>	Active external communication with clients will be tasked through the Communications Department per the Communications Plan. Client communications regarding service delays shall occur per the branch Office Administration procedure

**Interim Processing**

Treatment	Time to Achieve	Additional Comments
1. Continued Passive Client Service Support <ul style="list-style-type: none"> <li>• NA personnel to continue answering telephones and other customer communications during interruption</li> <li>• If telecommunications are inoperable to service center (branch) then confirm secondary site with EOC</li> </ul>	4 Hours - Ongoing	Pursuant to adequate communications utilities
2. Active Client Service Support <ul style="list-style-type: none"> <li>• Contact customer per standard SOP and Service Level Agreement to inform of any delays exceeding 1 week</li> </ul>	48 Hours	Corporate communications via EOC will accommodate media requests for information.
3. Service Routing <ul style="list-style-type: none"> <li>• Determine affected service area and extent of delay</li> <li>• Direct Requests for service to secondary branch location (if activated)</li> </ul>	8 Hours	EOST Team Leader primary contact for support  SLA to remain 24 hours for scheduling unless service delay >1week
4. Billing and regular client contact <ul style="list-style-type: none"> <li>• Billing will occur per the normal operations SOP</li> </ul>	Ongoing	

**Restoration**

Treatment	Time to Achieve	Additional Comments
-----------	-----------------	---------------------

<p>1. Return to normal service routing</p> <ul style="list-style-type: none"> <li>On confirmation from EOST Team Leader service request routing to primary service location can re-commence</li> </ul>	<p>1 Hour</p>	
<p>2. Customer Contact</p> <ul style="list-style-type: none"> <li>If notice was distributed to primary client contacts regarding service delays, then subsequent confirmation of resolution must be distributed</li> </ul>	<p>12 Hours</p>	<p>Dependent on length of service interruption and/or scale of disruption</p>

**Contact List**

	Name	Title	Special Responsibility	Phone / Home Address (o) Office (h) Home (m) Mobile (f) Fax Address
<p><b>Unit Team Leader</b></p>	<p><i>Redacted</i></p>	<p><i>Senior Manager, Major Accounts</i></p>	<p><i>Emergency Plan execution and MA team communication</i></p>	<p><i>Distribution Copy - Redacted</i></p>
<p><b>Alternative Unit Team Leader</b></p>	<p><i>Redacted</i></p>	<p><i>Vice President, Finance</i></p>	<p><i>Alternate</i></p>	
<p><b>Team Member responsible for maintenance of plan</b></p>	<p><i>Redacted</i></p>	<p><i>Senior Manager, Major Accounts</i></p>		

Business Unit – Payroll

Type: Support Level Operation Interruption Mitigation

*Type: Support Level Operation Interruption Mitigation Objective: Bi-weekly payroll continuity*

**Business Unit Processes/Activities**

- Payroll
  - Payment of internal client wages (salary & hourly)
  - Primary payroll data backup (via third-party)
  - Payroll Support
  - Personnel update data flow

**Initial Response**

TREATMENT	DETAILS
Maintain Wage Payments and Payroll Support Services	Primary emphasis on regular employee wage payment  If payroll time indicators not received for hourly employees, average weekly wage will determine correct payout for timely distribution
Organization Responsible	Sales Office Administration Regional Sales Office Administration Support Team Payroll Department
Communication	Communication to internal eligible employees will be distributed only in cases of nil value time data or missed payroll All request for internal information specific to the affected location shall go through the EOST Team Leader

**Interim Processing**

	Time to Achieve	Additional Comments
1. Obtaining Payroll Information <ul style="list-style-type: none"> <li>● Employee payroll based on Average Weekly Wage, or;</li> <li>● Determine employee payroll base on manual processing of employee time sheets</li> <li>● Utilize regular payroll SOP provided correct documentation received</li> </ul>	48 Hours	EOST Team Leader to designate payroll contact on activation
2. Payroll output <ul style="list-style-type: none"> <li>● Run payroll based on regular pre-event schedule</li> </ul>	Ongoing	If regular payroll schedule inadequate, temporary alterations can be made at the request of the EOC Manager
3. Ceridian output routing <ul style="list-style-type: none"> <li>● Route Ceridian output to secondary operations location (if utilized), or;</li> <li>Route to EOST Team Leader direct, or;</li> <li>Route to Regional Manager overseeing affected area</li> </ul>	24 Hours	When at all possible, utilize regular routing for payroll information.

**Restoration**

Treatment	Time to Achieve	Additional Comments
1. Return to Normal <ul style="list-style-type: none"> <li>• Ensure payroll time documentation from affected area is accurate</li> <li>• Record any employee changes and facilitate HCM input</li> <li>• Correct Ceridian/ADP output (if required)</li> </ul>	24 Hours	

**Contact List**

	Name	Title	Special Responsibility	Phone / Home Address <i>(o) Office (h) Home (m) Mobile (f) Fax Address</i>
<b>Unit Team Leader</b>	<i>Redacted</i>	<i>Manager, Payroll</i>	<i>Emergency Plan execution and Payroll communication</i>	<i>Distribution Copy- Redacted</i>
<b>Alternative Unit Team Leader</b>	<i>Redacted</i>	<i>Team Lead, Payroll</i>	<i>Alternate</i>	
	<i>Redacted</i>	<i>Sr Manager Global Payroll Accounts</i>	<i>Emergency Plan execution and Payroll communication</i>	

**Accountabilities**

**General**

In order to ensure proper documentation, accounting, and understanding of a business interruption, it is critical that records developed during the emergency be collected and examined.

Examination will take place by way of record audit and interviews. The purpose of this activity is to clarify events and coordinate effective recovery.

**Post Activation Records**

Following activation, all emergency management leadership outlined in this plan are required to submit all records surrounding emergency operations to the Business Continuity Management Team within 1 week of business resumption to normal operations.

Emergency Management leadership includes but is not limited to:

- *ECG Members*
- *EOC Manager*
- *Support Level Managers*
- *EOST Section Leaders*
- *EOST Team Leader*
- *Regional Manager*
- *SVP*

**Reporting**

The Business Continuity Management team will develop a post-interruption report based on the findings of the record audit. This report will be provided to the Board of Directors and Executive Leadership Committee and will serve as the official consolidated record of incident

## **Emergency Response Plan – Branch**

Initial Action Plan for Business Interruptions, Emergencies, and Disasters

Dedicated Branch specific emergency response plans are maintained in each Shred-it facility

# Appendix

## Regional BCP Activation CONTACT LIST

Name	Title	Special Responsibility	Phone <i>(o) Office</i> <i>(h) Home</i> <i>(m) Mobile</i> <i>(f) Fax</i>	Home Address

**Emergency Control Group (ECG) CONTACT LIST**

<b>Name</b>	<b>Title</b>	<b>Special Responsibility</b>	<b>Phone</b> <i>(o) Office</i> <i>(h) Home</i> <i>(m) Mobile</i> <i>(f) Fax</i>	<b>Home Address</b>



**Emergency Operations Site Team (EOST) CONTACT LIST**

<b>Name</b>	<b>Title</b>	<b>Special Responsibility</b>	<b>Phone</b> <i>(o) Office</i> <i>(h) Home</i> <i>(m) Mobile</i> <i>(f) Fax</i>	<b>Home Address</b>

**Evacuation/Safe Meeting Locations**

**Primary Location**

<b>Facility Name:</b>	
<b>Street Address:</b>	<b>Floor:</b>
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No:</b>
<b>Alternate Contact:</b>	<b>24 Hour No:</b>
	<b>FAX No:</b>
	<b>Other No.:</b>
<b>y Considerations:</b>	

**Alternate Location**

<b>Facility Name:</b>	
<b>Street Address:</b>	<b>Floor:</b>
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No:</b>
<b>Alternate Contact:</b>	<b>24 Hour No:</b>
	<b>FAX No:</b>
	<b>Other No.:</b>
<b>y Considerations:</b>	

Accountability: All branches shall have specific designated alternate location Full Evacuation and Safe Meeting Locations to posted on Intranet

**Key Customers**

<b>Product/Service:</b>	
<b>Customer Name:</b>	
<b>Street Address:</b>	
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No.:</b>
<b>Alternate Contact:</b>	<b>24 Hour No.:</b>
	<b>FAX No.:</b>
	<b>Other No.:</b>
<b>Comments:</b>	

<b>Product/Service:</b>	
<b>Customer/Client Name:</b>	
<b>Street Address:</b>	
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No.:</b>
<b>Alternate Contact:</b>	<b>24 Hour No.:</b>
	<b>FAX No.:</b>
	<b>Other No.:</b>
<b>Comments:</b>	

<b>Product/Service:</b>	
<b>Customer/Client Name:</b>	
<b>Street Address:</b>	
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No.:</b>
<b>Alternate Contact:</b>	<b>24 Hour No.:</b>
	<b>FAX No.:</b>
	<b>Other No.:</b>
<b>Comments:</b>	

Accountability: Senior Manager, Major Accounts

Minimum Customer requirement is all customers with contracts requiring emergency notification

**Additional copies can be made as necessary**

**Primary Location**

**Business Recovery Site Information**

<b>Facility Name:</b>	
<b>Street Address:</b>	<b>Floor:</b>
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No:</b>
<b>Alternate Contact:</b>	<b>24 Hour No:</b>
	<b>FAX No:</b>
	<b>Other No.:</b>
<b>y Considerations:</b>	

**Alternate Location**

<b>Facility Name:</b>	
<b>Street Address:</b>	<b>Floor:</b>
<b>City/State/Zip:</b>	
<b>Contact Person:</b>	<b>Phone No:</b>
<b>Alternate Contact:</b>	<b>24 Hour No:</b>
	<b>FAX No:</b>
	<b>Other No.:</b>
<b>y Considerations:</b>	

Directions to the Business Recovery Site

TBD

**FIRST ON SCENE**

**In Response to  
STAND BY OR ACTIVATION SITUATION**

Task	
<input type="checkbox"/>	Contact appropriate emergency authorities (if required)
<input type="checkbox"/>	Ensure personnel arriving on scene are made safe and instructed to meet at rally point (in cases of evacuation utilize branch emergency evacuation procedure)
<input type="checkbox"/>	Contact General Manager (GM) via cellular phone or home phone (found in branch contact list)
<input type="checkbox"/>	Proceed to safe area and await arrival of General Manager (GM)
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

## **Action Checklist DISTRICT MANAGER**

### **In Response to STAND BY SITUATION**

<b>Task</b>	
<input type="checkbox"/>	Contact appropriate emergency authorities (if required)
<input type="checkbox"/>	Ensure personnel arriving on scene are made safe and instructed to meet at rally point (in cases of evacuation utilize branch emergency evacuation procedure)
<input type="checkbox"/>	Start personal log – ensure it is maintained throughout the interruption period
<input type="checkbox"/>	Contact Regional Manager (RM) via cell phone or home phone – notify branch status, damage (if any), and service capability
<input type="checkbox"/>	Contact Office Coordinator (OC) to inform of standby situation
<input type="checkbox"/>	Instruct Office Coordinator (OC) to contact sales team - inform of standby situation and direct to wait for further instruction
<input type="checkbox"/>	Engage Regional Manager (RM) and Service Supervisor (SS) in conference call
<input type="checkbox"/>	Re-assess situation to determine if plan activation is required – Regional Manager Authority
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

*Additional tasks may be added as required*

## Action Checklist DISTRICT MANAGER

### In Response to PLAN ACTIVATION SITUATION

Task	
<i>To be completed <u>after</u> stand-by checklist</i>	
<input type="checkbox"/>	Attempt to gather (or have gathered) critical resource items from branch location utilizing the Critical Resources Form
<input type="checkbox"/>	Attempt to gather (or have gathered) all recovery boxes utilizing the Recovery Boxes Identification List
<input type="checkbox"/>	Engage Emergency Operations Site Team (EOST) Activation Plan – distribute General Message Form outlining activation
<input type="checkbox"/>	Provide Key EOST personnel with copy of Business Continuity Plan
<input type="checkbox"/>	If decision has been made to re-locate operations to secondary site provide all personnel with EOST contact listing and secondary address information (include directions to site)
<input type="checkbox"/>	Ensure all personnel requiring special travel accommodations are recorded on a Travel Request Form
<input type="checkbox"/>	On arrival to secondary site ensure that an Employee Location Control Form is completed (daily)
<input type="checkbox"/>	Arrange EOST meeting with key section lead personnel and coordinating branch (secondary site) staff
<input type="checkbox"/>	Complete Organization Assignment list and provide copies to all operational personnel
<input type="checkbox"/>	As soon as practicable – complete Incident Briefing Form (daily) and submit to Regional Manager
<input type="checkbox"/>	Engage Regional Manager (RM), Coordinating District Manager (DM), Operations Section Leader, Finance and Administration Section Leader, Logistics Section Leader, and Planning Section Leader in Conference Call with EOC – Ensure IT systems transfer has been completed and support available
<input type="checkbox"/>	Pursuant to the above contact all Operations Section personnel and arrange meeting
<input type="checkbox"/>	Task Operations personnel with functional objectives according to acceptable down time and crisis communications protocol. Instruct customer contact personnel not to operate outside of standard customer contact SOP for service lag calls unless service laps >48hours
<input type="checkbox"/>	Ensure all IT- dependent systems are have been setup pursuant to the EOST/EOC conference call
<input type="checkbox"/>	Complete General Message Form and distribute to EOST as required for team update purposes

**Action Checklist  
REGIONAL MANAGER**

**In Response to  
PLAN ACTIVATION SITUATION**

<b>Task</b>	
<input type="checkbox"/>	Upon receiving notification from District Manager (DM) direct to await further instructions
<input type="checkbox"/>	Start personal log – ensure it is maintained throughout the interruption period
<input type="checkbox"/>	Contact Senior Vice President, Sales, Service & Operations and notify of situation
<input type="checkbox"/>	Coordinate conference call with District Manager (DM) and Transportation Supervisor (TS)
<input type="checkbox"/>	Authorize Business Continuity Plan activation if required and warranted and indicate terms of activation
<input type="checkbox"/>	Inform Senior Vice President, Sales, Service & Operations of activation decision
<input type="checkbox"/>	Coordinate conference call with coordinating location District Manager (DM) and Transportation Supervisor (TS) to arrange continuing operations plan for unaffected customers
<input type="checkbox"/>	Coordinate operations resource deployment with EOC staff
<input type="checkbox"/>	Receive ongoing reporting from EOST Team Leader
<input type="checkbox"/>	Monitor effectiveness of EOST response and modify as necessary
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

*Additional tasks may be added as required*



### Action Checklist SERVICE SUPERVISOR

#### In Response to PLAN ACTIVATION SITUATION

Task	
<input type="checkbox"/>	Participate in conference call with District Manager (GM) and Regional Manager (RM)
<input type="checkbox"/>	Start personal log – ensure it is maintained throughout the interruption period
<input type="checkbox"/>	Determine Customer Security Representative CSR personnel availability –contact and notify all CSR personnel of activation and rally point (if different than secondary location)
<input type="checkbox"/>	Attempt to recover critical resources (operations) as outlined on the Critical Resources Form
<input type="checkbox"/>	Attempt to recover documents required for current day service
<input type="checkbox"/>	Contact coordinating branch Transportation Supervisor (TS) and request resource summary for SAP and ARP/S&T systems deployment
<input type="checkbox"/>	Coordinate routing from secondary site or alternate start point with Coordinating branch Transportation Supervisor (TS) or Support Center IT
<input type="checkbox"/>	Request additional resources from EOST Team Lead if required
<input type="checkbox"/>	Obtain re-routing authority from EOST Team Lead if not already provided
<input type="checkbox"/>	Route vehicles to secondary location per operational requirement determined by RM and EOST Team Lead
<input type="checkbox"/>	Facilitate CSR deployment to routes
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

*Additional tasks may be added as required*

**Incident Briefing Form**

INCIDENT BRIEFING	1. Incident Name	2. Date Prepared	3. Time Prepared
<b>4. Operations Status</b>			
Page 1 of 4	5. Prepared by (Name and Position)		

**6. Summary of Current Actions**

--

**7. Current Organization**

8. Resources Summary				
Resources Ordered	Resource Identification	ETA	On Scene	Location/Assignment
Page 4 of 4				

**Organization Assignment List**

<b>ORGANIZATION ASSIGNMENT LIST</b>		<b>1. INCIDENT NAME</b>	<b>2. DATE PREPARED</b>	<b>3. TIME PREPARED</b>
POSITION NAME		<b>4. OPERATIONAL PERIOD (DATE/TIME)</b>		
<b>5. INCIDENT COMMAND AND STAFF</b>		<b>9. OPERATIONS SECTION</b>		
TEAM LEADER		TEAM LEADER		
ASSISTANT		CSS (Routing)		
OPERATIONS COORDINATOR		a. BRANCH I-DIVISION/GROUPS		
LEAD OC		BRANCH DIRECTOR		
LEAD CSR		DEPUTY		
<b>6. AGENCY REPRESENTATIVES</b>		DIVISION/GROUP		
<b>AGENCY</b>	<b>NAME</b>	DIVISION/ GROUP		
		DIVISION/ GROUP		
		DIVISION/ GROUP		
		DIVISION/ GROUP		
		DIVISION /GROUP		
<b>7. PLANNING SECTION</b>		b. BRANCH II-DIVISIONS/GROUPS		
SECTION LEADER		BRANCH DIRECTOR		
TECHNICAL SUPPORT ASSIT.		DEPUTY		
RECOVERY		DIVISION/GROUP		
		DIVISION/GROUP		
		DIVISION/GROUP		
		DIVISION/GROUP		
		DIVISION/GROUP		
		c. BRANCH III-DIVISIONS/GROUPS		
		BRANCH DIRECTOR		
		DEPUTY		
		DIVISION/GROUP		
		DIVISION/GROUP		
		DIVISION/GROUP		
<b>8. LOGISTICS SECTION</b>				
TEAM LEADER				
FLEET MGR.				
<b>a. SUPPORT BRANCH</b>				
DIRECTOR				
SUPPLY UNIT				
FACILITIES UNIT				
GROUND SUPPORT UNIT				
<b>b. SERVICE BRANCH</b>		<b>10. FINANCE/ADMINISTRATION SECTION</b>		
DIRECTOR		TEAM LEADER		
COMMUNICATIONS UNIT		ASSISTANT		
		OC AP		
		OC AR		
		PROCURMENT UNIT		
<b>PREPARED BY (RESOURCES UNIT)</b>				

<b>GENERAL MESSAGE</b>		
TO:	POSITION:	
FROM:	POSITION:	
SUBJECT:	DATE:	TIME:
MESSAGE:		
SIGNATURE:	POSITION:	
REPLY:		
DATE:	TIME:	SIGNATURE/POSITION:

### General Message Form

<b>Section Log</b>		1. Incident Name	2. Date Prepared	3. Time Prepared
4. Section Name/Designators		5. Section Leader (Name and Position)		6. Operational Period
<b>7. Personnel Roster Assigned</b>				
<b>Name</b>		<b>Position</b>		<b>Home Base</b>
<b>8. Activity Log</b>				
<b>Time</b>		<b>Major Events</b>		
9. Prepared by (Name and Position)				



**Critical Vendors List**

<b>Product/Service:</b>	
<b>Vendor Name:</b>	
<b>Street Address:</b>	
<b>City/State/Zip:</b>	
<b>Contact Person:</b>  <b>Alternate</b>	<b>Phone No.:</b> <b>24 Hour No.:</b> <b>FAX No.:</b> <b>Other No.:</b>
<b>Comments:</b>	

<b>Product/Service:</b>	
<b>Vendor Name:</b>	
<b>Street Address:</b>	
<b>City/State/Zip:</b>	
<b>Contact Person:</b>  <b>Alternate</b>	<b>Phone No.:</b> <b>24 Hour No.:</b> <b>FAX No.:</b> <b>Other No.:</b>
<b>Comments:</b>	

<b>Product/Service:</b>	
<b>Vendor Name:</b>	
<b>Street Address:</b>	
<b>City/State/Zip:</b>	
<b>Contact Person:</b>  <b>Alternate</b>	<b>Phone No.:</b> <b>24 Hour No.:</b> <b>FAX No.:</b> <b>Other No.:</b>
<b>Comments:</b>	

**Additional copies can be made as necessary**

Name _____	Destination _____	Departure Date    /    / _____	Departure Time    : _____
Hotel Reservation	Yes ( ) No ( )	Departure	Departure
Rental Car	Yes ( ) No ( )	Date    /    / Time    :	_____
Cash Advance \$	_____	_____	_____

Name _____	Destination _____	Departure Date    /    / _____	Departure Time    : _____
Hotel Reservation	Yes ( ) No ( )	Departure	Departure
Rental Car	Yes ( ) No ( )	Date    /    / Time    :	_____
Cash Advance \$	_____	_____	_____

Name _____	Destination _____	Departure Date    /    / _____	Departure Time    : _____
Hotel Reservation	Yes ( ) No ( )	Departure	Departure
Rental Car	Yes ( ) No ( )	Date    /    / Time    :	_____
Cash Advance \$	_____	_____	_____

Name _____	Destination _____	Departure Date    /    / _____	Departure Time    : _____
Hotel Reservation	Yes ( ) No ( )	Departure	Departure
Rental Car	Yes ( ) No ( )	Date    /    / Time    :	_____
Cash Advance \$	_____	_____	_____

Name _____	Destination _____	Departure Date    /    / _____	Departure Time    : _____
Hotel Reservation	Yes ( ) No ( )	Departure	Departure
Rental Car	Yes ( ) No ( )	Date    /    / Time    :	_____
Cash Advance \$	_____	_____	_____

**Recovery Boxes Identification List**

<b>Team:</b>
<b>Storage Location:</b>
<b>Contact Name:</b>

**Box Identification:**

Contents	Comments

**Box Identification:**

Contents	Comments

1. Storage location refers to the name of the offsite storage facility (facility or under contract).
2. Contact name refers to the person who coordinates retrieval of recovery boxes.
3. Box Identification refers to the identifying code on the outside of the box.
4. Contents/Comments identify the items stored in the box and special concerns such as update / maintenance or shelf life.

**Critical Resources Form**

This form is to be utilized in the event that personnel can regain entry into a non-operational Shred-it facility following a business interruption event.

**Business Unit:** \_\_\_\_\_

Bldg./Floor:	Location on Floor: (e.g. Northwest Corner)	
Items To Be Retrieved	Comments	Condition*
<b>CRITICAL RECORDS:</b>		
<b>EQUIPMENT:</b>		
<b>OTHER:</b>		

\* Complete "Condition" at the time of the incident.

**Personnel Location Control Form**

**COMPLETE DAILY**

Date: \_\_\_/\_\_\_/\_\_\_

Completed by: \_\_\_\_\_

Operations Team

Name	Recovery Location	Phone Number	Work Schedule From To	
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____

**Key Manager Contact Notification Record**

For ECG Key Contact Activities

Name	Title	Telephone	Received	Time Called
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	



We protect what matters.

Dear Customer,

With over 30 years of experience partnering with businesses, we recognize the importance of continuing to serve you reliably, safely, and compliantly during the Coronavirus (COVID-19) pandemic. We write to assure you that since the onset, we've taken measures to continue to provide you industry-leading guidance and service.

We want to make it clear that *we are in it together and we always have been*. Our team has successfully protected our team members, customers, and communities through natural disasters, pandemics (and the spread of infectious diseases like Ebola), and other states of emergency. Because we are also the leading medical waste service provider, our regulatory team is in close contact with the Centers for Disease Control and Prevention (CDC), other relevant regulatory agencies, and healthcare organization administrators to ensure we deploy the most current protocols for safe, efficient, and compliant management of your secure information.

We have a global, cross-functional team monitoring the situation to ensure precautions are taken and communicated internally to minimize the spread of the virus, and our business continuity plans are executed to continue reliable service. To date at Stericycle and Shred-it:

- We have readied business continuity plans which include pre-designated, alternative transportation routes and treatment locations in the event of shut-downs. We are also ready to deploy operational team members to alternate locations in the event of a facility-specific staffing shortage
- We are providing guidance and ongoing communication to all team members on proper risk mitigation practices including following CDC-approved hand hygiene, operating at safe distances, and proper use of PPE, including gloves
- We are encouraging voluntary quarantine for team members who believe they are at risk and/or report or show signs of symptoms related to COVID-19
- We continue to communicate within our organization to provide guidance on precautionary measures to minimize disease spread at home and work
- We have established a ban on all travel to high-risk countries. Additionally, we are limiting business travel to matters critical to ensuring safety, compliance, and essential customer support

Visit our [COVID-19 Resource Page on Stericycle.com](#) for regular updates, training/webinar details, helpful links, documents, and guidance. In addition, the following resources are available to you:

- Our Customer Experience team by calling 1-800-697-4733
- Access to our regulatory team by emailing [ask-regulatory@stericycle.com](mailto:ask-regulatory@stericycle.com)

- Comprehensive webinar “Coronavirus Waste Management – Facts Not Fear” scheduled for Wednesday, March 25 at 1pm. [Click here to register](#)

Nothing is more important to us than protecting the health and safety of our customers, team members and community. We are grateful for your loyalty and appreciate the privilege to serve you.

With care and respect,

A handwritten signature in black ink that reads "Cindy". The signature is written in a cursive, flowing style.

Cindy J. Miller

Chief Executive Officer



# Stericycle Inc.

is Hereby Granted **NAID AAA Certification**  
by the National Association for Information Destruction



*The National Association for Information Destruction (NAID®) is the non-profit trade association recognized globally as the secure data destruction industry's standards setting and oversight body.*

*The certificate holder has met the rigorous requirements of the NAID AAA Certification program and demonstrated through announced and unannounced audits that its security processes, procedures, systems, equipment, and training meet the standards of care required by all known data protection regulations.\**

*As a result, NAID AAA Certification also serves to meet all data controller vendor selection due diligence regulatory requirements.*

*Valid Through: November 30, 2019*

*The certificate holder is NAID AAA Certified for the following services and media types:*

- Mobile Operation & Plant-based Operations for Paper/Printed Media, Micro Media, Physical Hard Drive, Non-Paper Media & Product Destruction (varies by location)

*Applicable to the following location(s):*

- All North American Locations Providing Information Destruction Services

*\*NAID AAA Certification specifications are regularly evaluated/amended as necessary and service provider compliance is verified to ensure ongoing conformance with all known data protection regulations including The Privacy Act (Australia), GDPR (Europe), HIPAA, GLBA, FACTA, State-level requirements (USA), and PIPEDA, PIPA, PHIPA (Canada) in their relevant jurisdiction(s), as well as with related risk assessment, incident reporting and data breach reporting procedures and training as required therein or separately.*

*Ronald Manning*  
NAID Certification Program Official



# SERVICE RECORD CERTIFICATE of DESTRUCTION

PLEASE KEEP THIS FOR YOUR RECORDS : THIS IS NOT AN INVOICE

## Customer Profile

**Site Number: XXXXXXXX**  
Customer Name  
Street Address  
City, State Zipcode

Number of trees saved  
by your firm this year:

**85.364**



## Service Summary



**Order:** XXXXXXXX  
**Order Date:** 10/25/2018  
**Customer PO:**  
**Service Type:** OFF-SITE REGULAR SERVICE  
**Contact:**  
**Time In:** 01:04 PM  
**Time Out:** 01:05 PM  
**Next Shred Date:** 11/07/2018

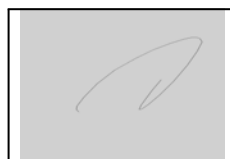
## Service Confirmation



**Service Time:** 1 min  
**Number of Equip Service:** 4  
**Number of Extra Items Collected:** 0  
**Estimated Weight:**

**Customer Name:**  
[NAME]

**CSR Name:** [NAME]



Shred-it is committed to the secure destruction of its customer's confidential information. This certification will affirm that Shred-it destroys the customer confidential material, pursuant to our customer's request and instructions. The following services are NAID certified: Hard Drive Destruction, Mobile Destruction, Offsite Destruction, Non-Paper Destruction.

**Site Number: XXXXXXXX**

If you have any questions or concerns call us at **1-800-697-4733**  
Please have your site number available so we can get you to the right representative for your account.

Shred-it® is a Stericycle solution.



## Service Details

**Equip:** B000XXXXXX- STD. CONSOLE - TELLER - 1/2 Full 10/25/2018 01:04 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Equip:** B000XXXXXX - STD. CONSOLE - CUSTMER SEVICE DESK NUMBER

2 10/25/2018 01:04 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Equip:** D000XXXXXX - Med Tote (64Gal/240L) - UPSTAIRS BY VAULT 10/25/2018  
01:04 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Equip:** D000XXXXXX - Med Tote (64Gal/240L) - UPSTAIRS 10/25/2018 01:05 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Order: XXXXXXXX**

**Site Number: XXXXXXXX**

If you have any questions or concerns call us at **1-800-697-4733**  
Please have your site number available so we can get you to the  
right representative for your account.

[Shred-it® is a Stericycle solution.](#)





Security  
Policies and Procedures  
Summary

Marla L. Sandlin  
Security & Compliance Manager  
January 30, 2020

## Index

Security and Compliance Program Overview .....	3
<b><u>ADMINISTRATIVE</u></b>	
Security Management Process .....	3
<b><u>TECHNICAL</u></b>	
Information Access Management .....	4
Unique User Identification .....	4
<b><u>PHYSICAL SECURITY</u></b>	
Team Member Security .....	4
Background Checks .....	5
Drug Screen .....	6
Security Awareness and Training .....	6
Security and Compliance Training .....	7
Security Specific Training .....	7
Facility Security Summary .....	8
Visitor Procedures .....	8
Restricted Access to Restricted Areas .....	9
Overhead Doors .....	9
Windows .....	10
Fencing .....	10
Lighting .....	10
Exterior Trash Containers .....	10
Alarm System .....	10
CCTV Monitoring System .....	10
Repairs and Maintenance .....	11
Fire Protection .....	11
<b><u>SERVICE PROCESS</u></b>	
<b><i>CUSTOMER SECURITY REPRESENTATIVE</i></b>	
Safety .....	11
Licensing Requirements .....	11
Vehicle Insurance Cards .....	11
Vehicle Safety .....	11
Vehicle Security .....	11
Vehicle Accident Procedures .....	12
Containers .....	12
Communications .....	12
Service Types .....	13
Start of Day Procedures .....	13
At the Customer Site .....	13
After Taking Possession of CCM .....	14
CSR Security Matters .....	14
<b><u>PLANT OPERATIONS</u></b>	
Pre-Destruction .....	14
Destruction Timeframe .....	14
Destruction Process .....	15
Witnessed Destruction .....	15
Maintenance .....	15
Contingency Plan .....	15
Post Destruction .....	16
Facility End of Shift Closing .....	16
Quality Control .....	16
Security Incident Procedures .....	16
Disaster Recovery Plan .....	17

## **Security and Compliance Program**

The Shred-it Security and Compliance Program outlines the steps taken at Shred-it to ensure compliance with safeguarding customer information. Shred-it, acting as a service provider, is required to implement appropriate measures designed to meet the objectives of the safeguarding guidelines.

Shred-it has developed the Security and Compliance Program to document the required guidelines for service providers to implement a written security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the service provider and the nature and scope of its activities. The program is designed to ensure the security and confidentiality of customer information, protect against unanticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. As a service provider, Shred-it must assess risks to customer information and implement appropriate policies, procedures and training to manage and control these risks. Customer information is defined as any record, in paper or other form, containing non-public personal information of a customer. Shred-it's business operation model is to provide information security to our customers and therefore treats all customer information, in all formats, as protected personal information. The personal identifiable information is considered in our chain of custody from the pick up at the customer location and throughout the life of the document.

The following administrative, technical and physical safeguards are identified as part of the Security and Compliance Program.

### **ADMINISTRATIVE**

#### **Security Management Process**

An overall information security management process is necessary to establish policy, provide oversight, and administer operational aspects of the Shred-it Security and Compliance Program. The process functions in a proactive, risk-appropriate manner and establishes the framework for safeguarding protected personal information. An information security policy commits Shred-it to safeguard protected personal information, to establish goals, and to assign responsibility. Supporting policy statements and procedures facilitate the prevention, detection, containment, and correction of security breaches.

The Security Team is responsible for security oversight and operational aspects of safeguarding customer personal information. Shred-it maintains security policies that identify and communicate security responsibilities of Team Members who access, or manage access, to protected personal information.

Shred-it has zero tolerance for compromising protected personal information. The Security Incident Reporting Policy notes that all Team Members are expected to follow the security protocols and abide by and fully comply with all of Shred-it's security policies and procedures. Shred-it will appropriately discipline and sanction Team Members for any violation of the security policies and procedures, will investigate and mitigate security violations and incidents in a timely manner, and will not intimidate or retaliate against any Team Members or individual who reports a security violation or incident. Sanctions against Team Members that do not comply with, or violate security policies and procedures shall be commensurate with the gravity of the violation. The sanctions shall include, but are not limited to, re-training, verbal and written warnings and termination.

## **TECHNICAL**

### **Information Access Management**

Shred-it maintains policies and procedures for granting access to protected personal information. Shred-it has established policies and procedures to assign, implement, revoke and modify access to all information systems. Proper controls over the user access to computer systems and data are maintained at all times. The system includes a technical means to control information access and access is terminated upon removal from the employment systems.

### **Unique User Identification**

Shred-it must be able to uniquely identify and track users or Team Members for the purpose of access control to all networks, systems, and applications that contain protected personal information. To monitor access to the networks, systems and applications which contain protected personal information, Team Members must be provided a unique user identification name. When requesting access to any network, system, or application that accesses, transmits, receives, or stores protected personal information, a user or Team Member must supply an assigned unique user identification name and a secure password. Team Members must not write down or allow other Team Members to use their unique identification name and password. It is the responsibility of all Team Members to ensure that their assigned user identification name and password are appropriately protected and only used for legitimate access to networks, systems, or applications. If Team Members believe their user identification name and password have been comprised, they must report that as a security incident.

## **PHYSICAL SECURITY**

### **Team Member Security Summary**

Shred-it has a Team Member security clearance process to determine administratively that Team Members are trustworthy before giving them access to personally identifiable information (PII). Awareness training on these policies and procedures is required both for those who are cleared for and given access and for those who have incidental access.

Any person that comes into a facility is an Access Team Member, a Non-Access Team Member or a Visitor (including vendors). Access Team Members must have all the proper documentation, security training and testing completed upon hire and updated annually before they will have access to all areas of the facility. Non-Access Team Members are limited to only areas that do not have customer confidential material (CCM). All visitors, maintenance and vendor personnel are required to sign a Confidentiality Agreement and be escorted at all times when in an area containing PII.

Shred-it maintains documentation regarding the levels of access granted to each Team Member, program and procedure. Shred-it periodically reviews access levels including when the status of the Team Member changes.

Shred-it conducts background checks on all applicants for pre-employment, including residence, employment, and drug testing (where permitted) whenever there is access to PII. All Shred-it Team Members with access to CCM are subject to an annual background and random drug test (where permitted). In regions where random drug testing may not be permitted, all supervisors and managers would be required to complete a Substance Abuse & Reasonable Suspicion training. All Team Members are required to sign Confidentiality Agreements at hire and annually thereafter.

### **Background Checks**

- All Team Members with access to customer material will complete a consent and authorization form for the purpose of conducting pre-hire and annual background checks.
- Federal District Court (7 years felony and misdemeanor based on residency history revealed from social security number trace – where permitted)
- Statewide Criminal – where available (7 years felony and misdemeanor based on residency history revealed from social security number trace – where permitted)
- County Criminal (7 years felony and misdemeanor based on residency history revealed from social security number trace – where permitted)
- Social Security Trace and Validation (reveals all addresses on file for the Team Member and validates the issuance of the social security number to the Team Member and date of issuance – where permitted)
- National Sex Offender Search (verified through name, social security number and date of birth – where permitted)
- Prohibited Parties Check (Office of Foreign Asset Control (OFAC), Specially Designated Nationals, Terrorists, Narcotics Traffickers, Blocked Persons and Vessels, Debarred Parties, Denied Persons List, Entity List, and Unverified List – where permitted)



- Background checks will be completed by Shred-it approved third party vendor and all results will be reviewed by Shred-it management and Human Resources to ensure compliance with Shred-it Policy, National Association of Information Destruction (NAID) standards, and customer requirements
- Background checks that do not meet Shred-it policy, NAID standards, or customer requirements will be reviewed by the Human Resources Compliance Department
- If the Human Resources Compliance Department determines that background checks do not meet Shred-it policy, NAID Standards, and customer requirements, this may result in the Team Member's termination of employment

### **Drug Screens**

- All Team Members with access to customer material will complete a consent and authorization form for the purpose of conducting a drug screen pre-hire and randomly (where permitted)
- Drug screens will be completed by Shred-it approved third party vendors and all results will be reviewed by Shred-it management to ensure compliance with Shred-it policy, NAID standards, and customer requirements
- Refusal to submit to the drug screening will result in immediate termination
- Positive test results, as determined by Human Resources Compliance Department will result in immediate termination
- Negative dilute test results, as determined by the HR Compliance, will result in a second drug screen being administered. Two consecutive negative dilute test results, as determined by HR Compliance, will result in immediate termination
- Drug screens that do not yield a negative result for any other reason, as determined by HR Compliance, will result in a second drug screen being administered. Two consecutive tests that do not yield a negative result for any other reason, as determined by HR Compliance, will result in immediate termination

### **Security Awareness and Training**

Security training is provided for all employees who access PII. This training includes overall security awareness, periodic reminders, virus awareness, password management, and user-specific topics necessary for individual workstation security. The facility is responsible for the tracking of annual security awareness training.

Topics include:

- Protecting personally identifiable information
- Reporting security incidents
- Managing individual passwords

- Types of confidential information
- Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA) and Fair and Accurate Credit Transactions Act (FACTA)
- Payment Card Industry (PCI) Compliance
- Code of Conduct and Business Ethics

Shred-it requires additional security awareness training for Access Team Members that addresses, at a minimum:

- Monthly Compliance Self-Audits/Inspections (physical security access, alarm tests, uniforms, badges and key cards)
- Monthly review of security policies
- Annual review and signature of Team Member Confidentiality Agreement
- Annual review and acknowledgement of Security Incident Reporting Policy

### **Security Specific Training**

- All Access Team Members shall be trained for compliance with Security and Operating Policies and Procedures within 5 days of their start date. Training shall be based on the most current version of Security and Operating Policies & Procedures.
- Until training and satisfactory background check has been completed, new Team Members shall be treated as Non-Access.
- Team Members shall be made aware that consumers are provided protection against unauthorized disclosure and use of CCM that is in the possession of others. Protections are afforded through GLBA, HIPAA Privacy Rules, and FACTA as well as through a variety of other federal and state laws. There shall be no instances in which CCM shall be disclosed to anyone, unless specifically required by law.
- Team Members re-training shall be required in the event of any of the following:
  - Significant changes in or additions to privacy laws and/or policies
  - Significant changes in NAID Certification requirements
  - Team Members violation of a Security Policy
  - Security Breach or more than one security incident involving the same Team Members
  - At the discretion of management
- All Access Team Members shall be required to review all Security and Operating Policies and Procedures and to sign – Operations and Security Policy Acknowledgement annually. The District Operations Manager (DOM) shall verify completion of Operations and Security Policy Acknowledgement and successfully completed Security Training Assessment.

- All facilities are required to complete weekly service and production security meetings for the purpose of brief training sessions and reminders on Shred-it security rules.
  - Training topics should include items covered in security policies, NAID, HIPAA and industry information.

### **Facility Security Summary:**

Shred-it maintains policies and procedures to limit physical access to its facilities while ensuring that properly authorized access is allowed. This ensures that access to facilities used to house PII is appropriately controlled and that procedures are properly documented to safeguard all facilities, systems, and equipment from unauthorized physical access, tampering, or theft. The Facility Security Policy provides guidelines to control and validate Team Members' access to all facilities used to house protected information. The policy also provides procedures to control, validate, and document visitor access to any facility. This procedure applies to vendors, repair personnel, and other non-workforce members.

Shred-it facilities shall ensure the utmost in security by meeting or exceeding certification standards established by NAID. Additionally, facility security shall be sufficient to meet applicable state and federal privacy regulations such as HIPAA and GLBA. In order to meet these requirements, the following are the minimum expectations for any facility that processes or retains CCM.

**Visitor Procedures:** All visitors must sign the Visitor Log which requires them to show a government issued ID and sign a Confidentiality Agreement stating they will abide by all the facility's procedures. If the visitor is an official inspector or third party auditor, they must first show their credentials documentation when signing the Visitor Log and Confidentiality Agreement, then be escorted to a conference room until executive leadership is contacted. If the visitor is entering the Restricted Area, their phone should be kept in the Non-Restricted Area. The visitor must also be briefed by Team Members on the facility's Environmental and Health & Safety protocol.

Each facility will maintain a Visitor Log for 12 months. The Visitor Log should include date, time, name of visitor, what is the purpose of their visit, which Team Member will be escorting, confidentiality agreement number and visitor badge ID#. Confidentiality Agreement and Visitor Code of Conduct are valid for and shall be maintained for 12 months.

All Team Members must prominently wear their Shred-it identification badge while performing Shred-it duties on or off the facility premises. All damaged, outdated and terminated Team Member badges will be destroyed through the shredding process.

Visitors shall conspicuously wear a visitor badge at all times while on Shred-it premises. Badges shall not be issued to a visitor until after the Visitor Log entry and signing of Confidentiality and

Visitor Code of Conduct Agreement have been completed. Badges shall be retrieved upon exit of the premises. No visitor, regardless of the regularity of their visits, shall be allowed to retain their visitor badge. Should any individuals be found in a Restricted Area or on premise that does not have a visitor badge, the person shall be immediately escorted to the office Non-Restricted Area, and the Facility Authorized Team Member shall be contacted to resolve the matter and follow visitor sign in procedures.

All visitors shall be escorted and kept under the direct visual supervision of an Access Team Member at all times while in a Restricted Area. An exception may be granted to emergency personnel only when responding to an emergency.

Restricted Area - while in a Restricted Area, visitors may NOT:

- Bring anything into or out of the area (i.e. brief cases, bags, notebooks, purses, etc.) except to carry tools or other equipment that may be needed to conduct repairs. No cell phones with cameras will be allowed into a Restricted Area. Auditors may take audit forms and pertinent audit documentation into and out; however, nothing that may constitute CCM or that originated in a Restricted Area may be taken out. All forms, papers and other materials from a Restricted Area shall be subject to the inspection by the Facility Authorized Team Member prior to exit of the Restricted Area. An exception may be granted to emergency personnel only when responding to an emergency and only for such items that may be required to properly respond to the emergency situation.
- Observe operations including the unloading of containers, conveyor system, shredded paper, or bales of paper, etc. from closer than a 10' distance. Exceptions include witnessed destruction in which a customer is witnessing the destruction of CCM that originated from their business, safety or regulatory audits Occupational Safety and Health Administration (OSHA) audits, repair or maintenance performed by visitors.

**Access to Restricted Areas:** Access to any Restricted Area shall be limited to Access Team Members and appropriately escorted Visitors through the use of card/electronic access or combination door locks. All Restricted Area doors shall be self-closing and auto-locking. Access numbers/cards and combinations shall not be distributed to anyone other than Access Team Members. Access numbers/cards, keys, combinations or other methods of gaining access to CCM or areas containing CCM shall be immediately retrieved from any terminated Team Members to whom these items were issued.

**Roll-up Doors:** Roll-up doors shall remain closed and locked at all times when not in use. These are secured with padlocks after hours. Adjustable dock plates must meet with the roll-up door (when closed) to prohibit access between the plate and door. When opened, the doors must be physically guarded or continuously supervised to prevent unauthorized access. If not continuously supervised, doors shall be affixed with a full open height security gate with a mesh size no greater than 2 square inches (gate must reach from the floor to the open height of the door, with no openings at either the floor or door height level). Screen mesh applied to accordion style gates is acceptable.

**Windows:** Windows shall remain locked at all times during when facility is unoccupied.. Windows shall also be visually secured to prevent the ability to view any Restricted Area or CCM. Windows may be opened to allow air flow during plant operation, as long as they are screened to prevent paper loss and visual security is maintained.

**Fencing:** If allowed by local regulations or leaseholder, facilities shall have secure perimeter fencing of the maximum allowable height up to 12' high and not more than 2" mesh. Fencing shall start at grade level and reach to full height without break. Internal fencing or walls used to create a Restricted Area and/or separation from another operation shall extend to the ceiling. If fencing does not go to the ceiling it shall have a motion sensor alarm and Closed Circuit Television (CCTV) inside and over the perimeter of the Restricted Area to detect if individuals have climbed over or come through a section of the secured fence/wall.

**Lighting:** Outside lighting shall be set to be on from dusk to dawn. Inside lighting shall be sufficient for CCTV to record activity with clarity.

**Exterior Trash Containers:** Exterior trash containers are fully locked or equivalently secured with access limited to the Facility Manager or their designee. Trash containers may be opened to receive office/shop trash and to be emptied by trash haulers. An alternate to locking is storage of the containers in the Restricted Area. Placing CCM or documents (shredded or unshredded) in a trash dumpster is not allowed under any circumstances. No paper shall be baled without first being shredded.

**Alarm System:** All facilities that contain CCM have an actively monitored security system in place. Security systems must be:

- Activated at all times when the facility is not manned
- Actively monitored such that the local authority having jurisdiction and an Access Individual will be contacted immediately (within industry standards or local code) by representatives from a third-party monitoring company on notification of an alarm
- Activated or deactivated only by Access Team Members only unless the facility is mobile only and no unshred CCM is received or housed
- Maintained to prevent false alarms. There should be a test by the monitoring company at least monthly to ensure the system is in good working order. Notification of such test shall be provided and retained by the location for 12 months

**CCTV Monitoring System:** All facilities that contain CCM have an operating CCTV system that:

- Monitors all points of ingress and egress into Restricted Areas (including enclosures, cages, shipping containers, etc.)
- Provides sufficient image clarity as to readily enable identification of individuals accessing Restricted Areas and the nature of their activities
- System must maintain a stored record of all images for a minimum of 90 days

- The stored record must be secured from theft or vandalism by being locked inside a lockable cage or lockable cabinet. Accordingly, it should only be accessible by management Team Members
- All processing areas must have coverage to a minimum of entry and exit portals
- The system utilizes a hard drive and/or cloud based back-up system versus compact discs, VCR tapes, or other
- All non-compliant safety and/or security actions taken by Team Members viewed on the CCTV system must be documented and appropriate disciplinary action taken

**Repairs and Maintenance:** Any and all repairs or modifications to the physical components of a Shred-it facility (including but not limited to alarms, CCTV and Access Controls) shall be recorded with downtime information submitted on a weekly basis.

Operational security maintenance checks shall be completed on a weekly and monthly basis by the FM or their designee. These checks are designed to verify proper functioning of the facility alarm and CCTV systems, as well as proper visitor procedures and other security items.

**Fire Protection:** Locations shall maintain compliance with applicable local fire codes. A fire protection assessment and service shall be conducted at least annually.

### **SERVICE PROCESS**

**NAID AAA Certification:** NAID AAA Certification standards set forth certain criteria specific to the Customer Security Representative (CSR).

**Safety:** CSRs shall at all times wear proper personal protective equipment while handling any CCM. These include but are not be limited to safety glasses, gloves, hats, ear protection, etc.

**Licensing Requirements:** A CSR must possess a current, valid driver's license which meets all state and federal requirements for the class of vehicle they will operate. The CSR must immediately notify their supervisor if the license status changes. CSRs shall keep their license and medical card current and in their possession while operating a Shred-it vehicle.

**Vehicle Insurance Cards:** Prior to driving any Shred-it vehicle, CSRs shall ensure that Shred-it insurance cards are in the vehicle. The CSR must immediately inform their supervisor and follow their directions for resolution if there is no insurance card in the vehicle.

**Vehicle Safety:** All CSRs shall exercise extreme caution in all phases of vehicle operation. No Team Member shall place themselves or others at risk for any reason.

### **Vehicle Security:**

- Except in the case of an emergency, no unauthorized person shall be permitted access to the cab, body, box, payload or tail-lift of any vehicle. No unauthorized person shall be transported as a passenger at any time except in case of an emergency.

- All vehicles used for transfer or destruction of CCM shall be fully lockable. Cabs, boxes, and any storage areas must remain locked at all times when not attended by a Shred-it Access Individual.
- All un-shredded CCM shall be securely contained during transport to the facility.
- All Collection vehicles will have a corporate approved audible alarm system or a high security padlock on the rear to ensure the security of the customer material inside the truck.

**Vehicle Accident Procedures:**

- When a Stericycle/Shred-it truck is involved in an accident while transporting CCM, the driver must remain with the vehicle and immediately notify facility management of the facility receiving the material for further instruction. CCM may not be left unattended.
- If the truck is inoperable, the facility will send a second truck to transfer materials safely and securely back to the warehouse for final destruction.
- Facility Management is required to file the Accident Reporting for Claims Management and enter the accident into SEMS.

**Containers:** All containers used to transport customer confidential material (CCM) must have operable locks. Containers must remain locked at all times during which they contain CCM unless attended directly by an Access Individual. Once emptied, containers shall be completely free from un-shredded material. All security containers must be checked by the location/warehouse Team Members when emptied. All security containers must be checked again prior to loading on the collection trucks and checked again prior to servicing at the customer site.

**Communications:** All CSRs and helpers shall have fully operating two-way communication devices in their possession at all times. This includes driving to and from customer sites and during the collection or destruction process. Exception is made only for customer environments in which the possession and/or use of two-way communication devices is prohibited (some hospitals, clinic buildings, etc.).

- Handheld or other wireless electronic devices are prohibited to be used while operating a moving vehicle. These items are considered “additional equipment and accessories” and decrease the safe operation of the vehicle.
- Vehicle operators are required to operate wireless phones in a “hands free” mode where both hands can remain on the wheel or required to safely pull off the road. The Company has more strict requirements for DOT regulated drivers to include a strict prohibition of any wireless communication device unless the driver is legally parked in an appropriate safe location. Texting is not allowed while operating a moving vehicle.

## **SERVICE TYPES**

- **On-site destruction** shall take place fully while at the customer site using a mobile shred truck. CSRs shall ensure all CCM is fully destroyed prior to leaving the customer site.
- **Off-site destruction** allows Shred-it to collect the materials from the customer site and transfer it back to the secure facility where the final destruction takes place using state of the art document shredding equipment.

**Start of Day Procedures:** CSRs shall comply with the following in preparing for their daily route.

- Must wear a uniform and display Photo I.D. Badge ensuring the customer can see it at all times.
- CSRs shall:
  - Review their schedule for services, start of day instructions and special instructions. CSRs are expected to resolve any questions with their supervisor prior to beginning their route.
  - Ensure their truck is loaded with security containers, pallets or any other items that may be required to execute the assigned services.
  - Ensure that all supplies needed are on their truck. For example: straps, shrink-wrap, blank work orders, locks, city maps, etc.
  - Request the assistance of a helper if needed.

### **At the Customer Site**

CSRs shall be courteous, professional, and polite and shall conduct themselves with appropriate interaction with customer personnel. CSRs are expected to provide superior service with a minimum level of distraction to customer operations.

If a customer makes a reasonable, policy compliant request, CSR shall comply. If the request is unusual but does not seriously delay the route or violate policy, CSR should accommodate the request and notify their supervisor. If a customer makes a request that is unreasonable, delays the route, compromises security, violates policy or is otherwise inappropriate, CSR shall not comply and shall notify their supervisor immediately. The supervisor shall advise CSR on how to proceed.

If a customer expresses any complaint, the CSR shall listen to and document the matter and offer to convey the information to the Facility Manager (FM). CSR shall also invite the customer to convey their comments to the FM. The CSR shall also communicate the customer's concerns to their supervisor.



### **After taking possession of CCM:**

- No container may be left unattended outside of the customer's facility.
- Containers that remain in the customer's facility but will not be physically attended shall be locked.
- Containers that are physically attended by a CSR may be unlocked during the collection process. Containers must be locked whenever unattended and always during transfer to and from the vehicle.
- No person, including the customer, shall be allowed to examine or retrieve materials once taken into possession. If a person claims to have the right to look through the materials or retrieve something from a locked container, the CSR should determine if the request is from the authorized contact and they must contact their supervisor.
- Once in possession, the CCM will be continuously attended or physically secured from unauthorized access.
- Under no circumstances shall any Team Member discard any un-shredded paper, product, or other material into any unsecured area.

Service orders shall be properly completed for services provided and may contain any customer concerns or comments (missing locks, moved or missing containers, key requests, etc.).

**CSR Security Matters:** CSRs are required to attempt to secure all CCM and immediately report any incident where customer confidential information was compromised to their supervisor.

## **PLANT OPERATIONS – OFFSITE DESTRUCTION**

### **NAID Certification Standards for Destruction of CCM**

NAID Certification standards set forth certain criteria for operational security and plant-based operations. This section outlines those items specific to plant operations.

**Pre-Destruction:** All CCM received from routine service will enter the destruction process upon arrival at the facility. Incoming service containers will be completely emptied, cleaned and rotated back into service. Facility Team Members must check all service containers to ensure they are completely empty of CCM.

**Destruction Timeframe:** All CCM from routine service shall be destroyed within three business days of receipt. An exception may be made for acts of God, breakdowns, written customer instructions to retain the media for a longer period or other circumstances beyond Shred-it's control. Destruction of CCM from customer purges must take place within the requirements as defined by the facility NAID Certification type. In any case in which an exception is made, security of materials shall be maintained.

**Destruction Process:** Destruction processes shall comply with NAID Certification standards for maximum particle size of the media type destroyed. NAID requirements for particle size of cross cut or pierce and tear – ¾" x 2.5" length (19mm x 63mm).

- Paper or printed media:
  - ✓ Mobile Shred truck: Shredtech and ShredFast truck types: ¾" x 2.5" length (19mm x 63mm). Size may vary for non-paper CCM.
  - ✓ SMS Truck: 1 ½" x 5/8" (38mm x 16mm). Size may vary for non-paper CCM.
  - ✓ Plant-based Equipment –Rotary grinder – 2" diameter screen
- Micro media: Microfilm and Microfiche must be reduced to 1/8" or less in width. A location may not accept micro media or must send it out for incineration if it cannot meet this requirement.
- Hard drives: Hard drives shall be destroyed using the shearing method or hydraulic punch to ensure that the hard drive is rendered irreparably un-readable. Any location destroying Hard Drives shall be NAID Certified for this service.

**Witnessed Destruction:** Only the FM or their designee may authorize an appointment for witnessed destruction. Customer scheduling needs will be accommodated on a best efforts basis. CCM may be delivered to the facility either by a CSR or by the customer. If delivered by the CSR, the materials shall be securely stored until the customer representative arrives. The Facility Security Policy outlines proper security measures for all visitors and contains the Confidentiality and Visitor Code of Conduct Agreement which must be signed by all visitors. Upon compliance with all proper security measures, the witness will be escorted to the witnessing area. No other CCM may be readily visible. The destruction process shall be conducted as close to the time of the customer's arrival as possible.

**Maintenance:** The FM shall ensure that all equipment is properly maintained, including the performance of any required or recommended preventative maintenance procedures and the performance of any needed repairs.

**Contingency Plan:** In the event of equipment breakdown such that the time for repair is expected to be greater than 48 hours, the Facility Manager shall immediately notify the Regional Vice President and trigger a local contingency plan per the following parameters:

- Collection of CCM may continue so long as it is stored in a Restricted Area.
- On-site shredding trucks may be utilized for shredding within the Restricted Area provided that proper ventilation for exhaust is maintained.
- Materials may be taken to another Shred-it location for processing provided that transportation of materials is made in a secure vehicle.
- Should insufficient Restricted Area space be available for the time required for repair, and other contingency actions unavailable, additional security containers may be delivered to customers with notification of any temporary schedule change.

**Post Destruction:** All recycling must only be sent to approved recycling vendors. Any deviations to this must be reviewed and approved through the exception process. In no cases, shall shredded paper be utilized for any other purpose (animal bedding, package fill, etc.) than recycling.

**Facility End of Shift Closing:**

- Production Team Members shall sweep the entire exposed floor and pass the sweepings through the destruction process.
- The FM or their designee shall dismiss Team Members. At this time, Team Members shall return any company-related items (including all keys) and necessary paperwork that were used or completed.
- At the end of each day the FM or their designee shall perform a visual quality control and security inspection.

**Quality Control:**

- Process Control – All destroyed CCM shall be verified to comply with the standards set forth in “Destruction Process”. Examinations shall be made by the FM or their designee. Should any non-compliant CCM be found, the destruction process shall be stopped, root cause identified, and corrective action taken prior to restarting the plant operation.
- Visual Inspection – The FM or their designee shall complete a visual inspection of the facility at the beginning and end of each shift, ensuring that:
  - There are no breaches in security.
  - The areas surrounding the plant are free from shredded and un-shredded paper.
  - The shredded material (paper and non-paper) size is in compliance with NAID Certification standards.
  - Collection trucks have been completely emptied and are properly locked.
  - Unlocked containers have been completely emptied.
  - All non-shredded CCM is properly stored in a Restricted Area.
  - Any discovery that may result in a security weakness is properly remedied immediately or within a reasonable timeframe if immediate remedy is not possible. This must be reported immediately to the Security Team.

**Security Incident Procedures**

- A Security incident occurs when there is either loss or breach of company confidential or proprietary data/information. Loss of information/data may take either paper/hard copy or electronic form.
- All Shred-it Team Members, regardless of job description, have the responsibility to take all reasonable and safe means necessary to ensure the security of the confidential material at all times. This includes summoning of additional assistance, police or local authorities to assist or secure an area, the vehicle, the facility or any other reasonable

measures which do not compromise safety of Team Member or the security of confidential materials.

- All Shred-it Team Members that knowingly or unknowingly cause, initiate, or participate in any violation of security policy or procedure or have knowledge of any actual, potential or threatened security policy or procedure violation, shall immediately report such knowledge to the District Operations Manager/Facility Manager or their supervisor.
- Any incident will be reported electronically through SEMS, an online portal and be promptly reported to their immediate Supervisor, District Operations Manager/Facility Manager, Regional Vice President and Security Team.
- A conference between the DOM/FM, RVP and a member of the Security Team shall be held as soon as possible following receipt of notice to discuss the investigation results, disciplinary action, any requirements to retrain or change policy and to notify the customer.
- Customer notification will include the details collected during the investigation and must include any retraining of Team Members. The customer notification will include any further action or communication for follow up until both parties can close the case. All customer notification will either take the form of a phone call or in writing.
- All Security Incident/breach reports will be reviewed in detail by the Security Team which will determine if changes to policies or procedures could have prevented the incident and/or should be made to prevent future occurrences. Policy and/or procedural changes recommended will be presented to the Security Working Group for approval.
- All incidents are fully investigated by the location, the Security Team, the RVP and the appropriate HR Representative to provide final determination. All security matters are reported weekly to the Senior Vice President – SCS Operations US and Canada.
- Shred-it provides an Ethics and Compliance Hot Line procedure (1-800-451-5340) for receiving and addressing complaints regarding the practices or the actions of Shred-it Team Members and temporary workers. Shred-it prohibits all forms of retribution against any individual who reports actual or suspected violations of regulations, or policies. Shred-it Team Members will not discharge, demote, suspend, threaten, harass, or in any manner, discriminate against any Team Member in terms and conditions of employment based upon any actions of such Team Member with respect to good faith reporting.
- Each Team Member has a responsibility to comply with the laws and behave in an honest and ethical manner. Violating regulations, Shred-it policies, or failing to report such violations can result in serious disciplinary action up to and including termination. In addition, violators could be subject to civil and criminal charges by outside regulatory agencies. Shred-it has a policy of progressive discipline for infractions committed by Team Members, except where immediate termination is identified as the discipline.

#### **DISASTER RECOVERY PLAN**

- Shred-it has policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain protected personal information.

- Shred-it requires each location to maintain a contingency plan/disaster recovery plan for implementation in the event of an emergency, disaster, or other occurrence (i.e. fire, vandalism, system failure, or natural disaster). All facilities are required to update and test their Emergency Action Plans annually.
- Shred-it maintains a contingency plan for responding to system emergencies involving systems that contain protected personal information. Shred-it performs periodic backups of data, has facilities for continuing critical operations in the event of an emergency, and has disaster recovery procedures in place for such systems.



## ATTACHMENT C: REQUIRED BIDDER INFORMATION & CERTIFICATIONS EQUALIS GROUP: RECORDS MANAGEMENT, SHREDDING, STORAGE, STORAGE, AND DESTRUCTION WITH RELATED SERVICES & SOLUTIONS PROGRAM

**Purpose of this Attachment C:** CCOG requires the following information about Bidders who submit proposals in response to any CCOG request for proposal (“RFP”) in order to facilitate the execution of the master group purchasing agreement (“Master Agreement”) with the winning supplier (“Winning Supplier”). CCOG reserves the right to reject a Bidder’s proposal if a Bidder fails to provide this information fully, accurately, and by the deadline set by CCOG in RFP Section 1.3 – Anticipated Procurement Timetable. Further, some of this information (as identified below) **must** be provided in order for CCOG to accept and consider a Bidder’s proposal. **Failure to provide such required information may result in a Bidder’s proposal being deemed nonresponsive to this RFP.**

**Instructions:** provide the following information about the Bidder. Bidders may a) complete this document in Microsoft Word by completing the form fields, print this attachment, and sign it in the designated signature areas, b) complete this document using the form fields, print to .pdf, and provide certified electronic signatures in the designated signature areas, or c) print this attachment, complete it, and sign it in the designated signature areas. It is mandatory that the information provided is certified with an original signature (in [blue ink](#), please) or signed using a certified electronic signature by a person with sufficient authority and/or authorization to represent Bidder. Bidders are to provide the completed and signed information and certifications in **Tab 1** of the Technical Proposal submitted to CCOG as described in RFP Section 4.2 – Format for Organization of the Proposal.

*[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]*

**Bidders must provide all the information outlined below**

<p>1. Equalis Group RFP Name:</p> <p style="text-align: center;"><u>RFP # CCOG-2109</u></p>	<p>2. Proposal Due Date:</p> <p style="text-align: center;"><u>November 5, 2020</u></p>
<p>3. Bidder Name:</p> <p><u>Stericycle, Inc.</u> (legal name of the entity responding to RFP)</p>	<p>4. Bidder Federal Tax ID # or Social Security #:</p> <p style="text-align: center;"><u>36-3640402</u></p>
<p>5. Bidder Corporate Address:</p> <p>2355 Waukegan Road Street Address 2 Bannockburn, IL, 60015</p>	<p>6. Bidder Remittance Address (or "same" if same as Item #5):</p> <p>Same or Street Address 1 Street Address 2 City, State Zip</p>

**7. Print or type information about the Bidder representative/contact person authorized to answer questions regarding the proposal submitted by your company:**

Bidder Representative: Pete Sansone

Representative's Title: National Account Executive

Address 1: 2355 Waukegan Rd.

Address 2: Click or tap here to enter text.

City, State Zip: Bannockburn, IL 60015

Phone #: 636-856-7558

Fax #: N/A

E-Mail Address: Peter.Sansone@Stericycle.com

---

**8. Print or type the name of the Bidder representative authorized to address contractual issues, including the authority to execute a contract on behalf of Bidder, and to whom legal notices regarding contract termination or breach, should be sent (if not the same individual as in #7, provide the following information on each such representative and specify their function):**

Bidder Representative: Jimmy Randall

Representative's Title: RVP, National Accounts

Address 1: 2355 Waukegan Rd.

Address 2: Click or tap here to enter text.

City, State Zip: Bannockburn, IL 60015

Phone #: 470-373-5284

Fax #: N/A

E-Mail Address: Jimmy.Randall@Stericycle.com

9. Is this Bidder an Ohio certified Minority Business Enterprise (“MBE”)? Yes  No

If yes, attach a copy of current certification to your proposal as an appendix in the third section of your proposal.

**10. Mandatory Supplier Certifications:**

CCOG may not enter into contracts with any suppliers who have been found to be ineligible for state contracts under specific federal or Ohio statutes or regulations. Bidders responding to any CCOG RFP MUST certify that they are NOT ineligible by signing each of the four statements below. **Failure to provide proper affirming signature on any of these statements will result in a Bidder’s proposal being deemed nonresponsive to this RFP.**

I, Pete Sansone (insert signature of representative shown in Item #7 above), hereby certify and affirm that Stericycle (insert Bidder name as shown in Item #3 above), has not been debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions by the United States Department of Labor, the United States Department of Health and Human Services, or any other federal department or agency as set forth in 29 CFR Part 98, or 45 CFR Part 76, or other applicable statutes.

AND

I, Pete Sansone (insert signature of representative shown in Item #7 above), hereby certify and affirm that Stericycle (insert Bidder name as shown in Item #3 above), is in compliance with all federal, state, and local laws, rules, and regulations, including but not limited to the Occupational Safety and Health Act and the Ohio Bureau of Employment Services and the following:

- Not penalized or debarred from any public contracts or falsified certified payroll records or any other violation of the Fair Labor Standards Act in the last three (3) years;
- Not found to have violated any worker’s compensation law within the last three (3) years;
- Not violated any employee discrimination law within the last three (3) years;
- Not have been found to have committed more than one (1) willful or repeated OSHA violation of a safety standard (as opposed to a record keeping or administrative standard) in the last three (3) years;
- Not have an Experience Modification Rating of greater than 1.5 (a penalty-rated employer) with respect to the Bureau of Workers’ Compensation risk assessment rating; and
- Not have failed to file any required tax returns or failed to pay any required taxes to any governmental entity within the past three (3) years.

AND

I Pete Sansone (insert signature of representative shown in Item #7 above) hereby certify and affirm that Stericycle (insert Bidder name as shown in Item #3 above), is not on the list established by the Ohio Secretary of State, pursuant to ORC Section 121.23, which identifies persons and businesses with more than one unfair labor practice contempt of court finding against them.

AND

I Pete Sansone (insert signature of representative shown in Item #7 above) hereby certify and affirm that Stericycle (insert Bidder name as shown in Item #3, above), either is not subject to a finding for recovery under ORC Section 9.24, or has taken appropriate remedial steps required under that statute to resolve any findings for recovery, or otherwise qualifies under that section to enter into contracts with CCOG.

**11. Supplemental Bidder Contract and Equal Employment Opportunity Information:**

A. Provide data on Bidder employees both nationwide (inclusive of Ohio staff) and the number of Ohio employees:

	<u>Nationwide:</u>	<u>Ohio Offices:</u>
Total Number of Employees:	<u>22,500</u>	<u>      </u>



% of those who are Women: 23% \_\_\_\_\_

% of those who are Minorities: 50% \_\_\_\_\_

B. If you are selected as the Winning Supplier and this RFP involves the provision of services to Equalis Group Members, will you subcontract any part of the work?

- NO -or-
- YES, but for less than 50% of the work -or-
- YES, for 50% or more of the work

C. If any part of your proposal would be performed by any subcontractors, provide the following information on each subcontractor (additional pages may be added as needed):

Subcontractor Name: Varies by Location

Street Address 1: Street Address 1

Street Address 2: Street Address 2

City, State Zip: City, State Zip

Work to be Performed: Description of Work

Estimated percentage of total proposal to be performed by subcontractors: Varies by Location & will be negotiated at the local level %  
 (Do NOT show dollar amounts here; show % of WORK sub-contractors will perform/provide). Define the part of the work that will be performed by each subcontractor.

**Subcontractor's employee information** (attach additional pages if needed):

	Nationwide:	Ohio Offices:
Total Number of Employees:	<u>Varies by Location</u>	_____
% of those who are Women:	<u>Varies by Location</u>	_____
% of those who are Minorities:	<u>Varies by Location</u>	_____

12. Bidder has reviewed the Model Master Agreement attached to the RFP as Attachment E, and if awarded a contract,  Bidder will not (or)  Bidder will request changes to the standard language and has marked the requested changes and returned the model document with this proposal for consideration by CCOG and Equalis Group, LLC. (All requested changes to Model Master Agreement contract language are subject to negotiation and CCOG and Equalis Group, LLC approval.)

13. Bidder has reviewed the Model Administration Agreement attached to the RFP as Attachment E, and if awarded a contract,  Bidder will not (or)  Bidder will request changes to the standard language and has marked the requested changes and returned the model document with this proposal for consideration by Equalis Group, LLC. (All requested changes to Model Administration Agreement contract language are subject to negotiation and Equalis Group, LLC approval.)

14. I       Pete Sansone      , (insert signature of representative shown in Item #7 above) hereby affirm that this proposal accurately represents the capabilities and qualifications of Stericycle (insert Bidder name as shown in item #3, above), and I hereby affirm that the cost(s) proposed to CCOG for the performance of services and/or provision of goods covered in this proposal in response to this CCOG RFP is a firm fixed price structure as described in the Cost Proposal, inclusive of all incidental as well as primary costs. (Failure to provide the proper affirming signature on this item may result in the disqualification of your proposal.)

**15. Additional Documents:**

CCOG makes every attempt to meet the varying legal requirements of public agencies across the country. The documents included in this section are intended to give our contracts the broadest geographic reach by meeting the procurement requirements of other states outside of Ohio.

**15.1. Lobbying Certification**

Submission of this certification is a prerequisite for making or entering into this transaction and is imposed by Section 1352, Title 31, U.S. Code. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Any person who fails to file the required certification shall be subject to civil penalty of not less than ten thousand dollars (\$10,000) and not more than one hundred thousand dollars (\$100,000) for each such failure.

The undersigned certifies, to the best of his/her knowledge and belief, on behalf of Bidder that:

1. No Federal appropriated funds have been paid or will be paid on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement.
2. If any funds other than Federal appropriated funds have been or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract or cooperative agreement, the undersigned shall complete and submit Standard Form LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.
3. The undersigned shall require that the language of this certification be included in the award documents for all covered sub-awards exceeding one hundred thousand dollars (\$100,000) in Federal funds at all appropriate tiers and that all sub-recipients shall certify and disclose accordingly.

      Pete Sansone        
Signature of Bidder representative

**15.2. Boycott Certification**

Bidder must certify that during the term of any Agreement, it does not boycott Israel and will not boycott Israel. "Boycott" means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations specifically with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory, but does not include an action made for ordinary business purposes.

      Pete Sansone        
Signature of Bidder representative

### 15.3. Federal Funds Certification Form (EDGAR)

When a participating agency seeks to procure goods and services using funds under a federal grant or contract, specific federal laws, regulations, and requirements may apply in addition to those under state law. This includes, but is not limited to, the procurement standards of the Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards, 2 CFR 200 (sometimes referred to as the “Uniform Guidance” or “EDGAR” requirements). All bidders submitting proposals must complete this Federal Funds Certification Form regarding bidder’s willingness and ability to comply with certain requirements which may be applicable to specific participating agency purchases using federal grant funds. This completed form will be made available to Members for their use while considering their purchasing options when using federal grant funds. Members may also require Supplier Partners to enter into ancillary agreements, in addition to the contract’s general terms and conditions, to address the member’s specific contractual needs, including contract requirements for a procurement using federal grants or contracts.

For each of the items below, respondent should certify **bidder’s agreement and ability to comply, where applicable, by having respondents authorized representative complete and initial the applicable lines after each section and sign the acknowledgment at the end of this form.** If a respondent fails to complete any item in this form, CCOG will consider the respondent’s response to be that they are unable or unwilling to comply. A negative response to any of the items may, if applicable, impact the ability of a participating agency to purchase from the Supplier Partner using federal funds.

#### 15.3.1. Supplier Partner Violation or Breach of Contract Terms

Contracts for more than the simplified acquisition threshold currently set at one hundred fifty thousand dollars (\$150,000), which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 USC 1908, must address administrative, contractual, or legal remedies in instances where Supplier Partners violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Any contract award will be subject to Terms and Conditions of the Master Agreement, as well as any additional terms and conditions in any purchase order, participating agency ancillary contract, or Member construction contract agreed upon by Supplier Partner and the participating agency which must be consistent with and protect the participating agency at least to the same extent as the CCOG Terms and Conditions.

The remedies under the contract are in addition to any other remedies that may be available under law or in equity. By submitting a proposal, you agree to these Supplier Partner violation and breach of contract terms.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### 15.3.2. Termination for Cause or Convenience

When a participating agency expends federal funds, the participating agency reserves the right to immediately terminate any agreement in excess of ten thousand dollars (\$10,000) resulting from this procurement process in the event of a breach or default of the agreement by Offeror in the event Offeror fails to: (1) meet schedules, deadlines, and/or delivery dates within the time specified in the procurement solicitation, contract, and/or a purchase order; (2) make any payments owed; or (3) otherwise perform in accordance with the contract and/or the procurement solicitation. Participating agency also reserves the right to terminate the contract immediately, with written notice to offeror, for convenience, if participating agency believes, in its sole discretion that it is in the best interest of participating agency to do so. Bidder will be compensated for work performed and accepted and goods accepted by participating agency as of the termination date if the contract is terminated for convenience of participating agency. Any award under this procurement process is not exclusive and participating agency reserves the right to purchase goods and services from other offerors when it is in participating agency’s best interest.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

### 15.3.3. Equal Employment Opportunity

Except as otherwise provided under 41 CFR Part 60, all participating agency purchases or contracts that meet the definition of “federally assisted construction contract” in 41 CFR Part 60-1.3 shall be deemed to include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, “Equal Employment Opportunity” (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity,” and implementing regulations at 41 CFR Part 60, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor.”

The equal opportunity clause provided under 41 CFR 60-1.4(b) is hereby incorporated by reference. Supplier Partner agrees that such provision applies to any participating agency purchase or contract that meets the definition of “federally assisted construction contract” in 41 CFR Part 60-1.3 and Supplier Partner agrees that it shall comply with such provision.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

### 15.3.4. Davis-Bacon Act

When required by Federal program legislation, Supplier Partner agrees that, for all participating agency prime construction contracts/purchases in excess of two thousand dollars (\$2,000), Supplier Partner shall comply with the Davis-Bacon Act (40 USC 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, “Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction”). In accordance with the statute, Supplier Partner is required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determinate made by the Secretary of Labor. In addition, Supplier Partner shall pay wages not less than once a week.

Current prevailing wage determinations issued by the Department of Labor are available at [www.wdol.gov](http://www.wdol.gov). Supplier Partner agrees that, for any purchase to which this requirement applies, the award of the purchase to the Supplier Partner is conditioned upon Supplier Partner’s acceptance of the wage determination.

Supplier Partner further agrees that it shall also comply with the Copeland “Anti-Kickback” Act (40 USC 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, “Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States”. The Act provides that each Supplier Partner or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

### 15.3.5. Contract Work Hours and Safety Standards Act

Where applicable, for all participating agency contracts or purchases in excess of one hundred thousand dollars (\$100,000) that involve the employment of mechanics or laborers, Supplier Partner agrees to comply with 40 USC 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 USC 3702 of the Act, Supplier Partner is required to compute the wages of every mechanic and laborer on the basis of a standard work week of forty (40) hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of forty (40) hours in the work week. The requirements of 40 USC 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

### 15.3.6. Right to Inventions Made Under a Contract or Agreement

If the participating agency's Federal award meets the definition of "funding agreement" under 37 CFR 401.2(a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance or experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

Supplier Partner agrees to comply with the above requirements when applicable.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### **15.3.7. Clean Air Act and Federal Water Pollution Control Act**

Clean Air Act (42 USC 7401-7671q.) and the Federal Water Pollution Control Act (33 USC 1251-1387), as amended – Contracts and subgrants of amounts in excess of one hundred fifty thousand dollars (\$150,000) must contain a provision that requires the non-Federal award to agree to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act (42 USC 7401-7671q.) and the Federal Water Pollution Control Act, as amended (33 USC 1251-1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

When required, Supplier Partner agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Clean Air Act and the Federal Water Pollution Control Act.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### **15.3.8. Debarment and Suspension**

Debarment and Suspension (Executive Orders 12549 and 12689) – A contract award (see 2 CFR 180.220) must not be made to parties listed on the government-wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR Part 1966 Comp. p. 189) and 12689 (3CFR Part 1989 Comp. p. 235), "Debarment and Suspension." SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Supplier Partner certifies that Supplier Partner is not currently listed on the government-wide exclusions in SAM, is not debarred, suspended, or otherwise excluded by agencies or declared ineligible under statutory or regulatory authority other than Executive Order 12549. Supplier Partner further agrees to immediately notify the Cooperative and all Members with pending purchases or seeking to purchase from Supplier Partner if Supplier Partner is later listed on the government-wide exclusions in SAM, or is debarred, suspended, or otherwise excluded by agencies or declared ineligible under statutory or regulatory authority other than Executive Order 12549.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### **15.3.9. Byrd Anti-Lobbying Amendment**

Byrd Anti-Lobbying Amendment (31 USC 1352) – Supplier Partners that apply or bid for an award exceeding one hundred thousand dollars (\$100,000) must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 USC 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award. As applicable, Supplier Partner agrees to file all certifications and disclosures required by, and otherwise comply with, the Byrd Anti-Lobbying Amendment (31 USC 1352).

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### 15.3.10. Procurement of Recovered Materials

For participating agency purchases utilizing Federal funds, Supplier Partner agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm estimates and otherwise comply. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds ten thousand dollars (\$10,000) or the value of the quantity acquired during the preceding fiscal year exceeded ten thousand dollars (\$10,000); procuring solid waste management services in a manner that maximizes energy and resource recovery, and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### 15.3.11. Profit as a Separate Element of Price

For purchases using federal funds in excess of one hundred fifty thousand dollars (\$150,000), a participating agency may be required to negotiate profit as a separate element of the price. See, 2 CFR 200.323(b). When required by a participating agency, Supplier Partner agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Supplier Partner agrees that the total price, including profit, charged by Supplier Partner to the participating agency shall not exceed the awarded pricing, including any applicable discount, under Supplier Partner's Group Purchasing Agreement.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### 15.3.12. General Compliance and Cooperation with Members

In addition to the foregoing specific requirements, Supplier Partner agrees, in accepting any purchase order from a Member, it shall make a good faith effort to work with Members to provide such information and to satisfy such requirements as may apply to a particular participating agency purchase or purchases including, but not limited to, applicable recordkeeping and record retention requirements.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

#### 15.3.13. Applicability to Subcontractors

Offeror agrees that all contracts it awards pursuant to the Contract shall be bound by the foregoing terms and conditions.

Does Supplier Partner agree? Jimmy Randall  
(Initials of Authorized Representative)

By signature below, I certify that the information in this form is true, complete, and accurate and that I am authorized by my company to make this certification and all consents and agreements contained herein.

Stericycle  
Bidder Name

James W. Randall

Signature of Authorized Company Official

Jimmy Randall  
Printed Name

RVP, National Accounts  
Title

11/2/2020  
Date

## 16. Required Documents for Supplier Partners Intending to Do Business in New Jersey

### 16.1. Ownership Disclosure Form

Pursuant to the requirements of P.L. 1999, Chapter 440 effective April 17, 2000 (Local Public Contracts Law), Bidder shall complete the form attached to these specifications listing the persons owning 10 percent (10%) or more of the firm presenting the proposal.

Bidder Name: Stericycle, Inc.  
Street Address: 2355 Waukegan Rd  
City, State Zip: Bannockburn, IL, 60015

Complete as appropriate:

Click or tap here to enter text., certify that I am the sole owner of Click or tap here to enter text., that there are no partners and the business is not incorporated, and the provisions of N.J.S. 52:25-24.2 do not apply.

OR:

Click or tap here to enter text., a partner in Click or tap here to enter text., do hereby certify that the following is a list of all individual partners who own a 10 percent (10%) or greater interest therein. I further certify that if one (1) or more of the partners is itself a corporation or partnership, there is also set forth the names and addresses of the stockholders holding 10 percent (10%) or more of that corporation's stock or the individual partners owning 10% or greater interest in that partnership.

OR:

Click or tap here to enter text., an authorized representative of Click or tap here to enter text., a corporation, do hereby certify that the following is a list of the names and addresses of all stockholders in the corporation who own 10% or more of its stock of any class. I further certify that if one (1) or more of such stockholders is itself a corporation or partnership, that there is also set forth the names and addresses of the stockholders holding 10 percent (10%) or more of the corporation's stock or the individual partners owning a 10 percent (10%) or greater interest in that partnership.

**(Note: If there are no partners or stockholders owning 10% or more interest, indicate none.)**

NAME	ADDRESS	% INTEREST
<b>N/A – Stericycle is a publicly traded Company</b>	Click or tap here to enter text.	
Click or tap here to enter text.	Click or tap here to enter text.	
Click or tap here to enter text.	Click or tap here to enter text.	
Click or tap here to enter text.	Click or tap here to enter text.	
Click or tap here to enter text.	Click or tap here to enter text.	

I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.

\_\_\_\_\_  
*Authorized Signature and Title*

Enter Date Signed  
 Date

**16.2. Non-Collusion Affidavit (to be completed and included with each proposal submitted to Members in NJ)**

**Bidder Name:** Not Applicable

**Street Address:** Not Applicable

**City, State Zip:** Not Applicable

*State of New Jersey*

*County of Customer County*

*I, Your Name of the Your City in the County of Your County, State of Your State of full age, being duly sworn according to law on my oath depose and say that:*

*I am the Your Title of the firm of Bidder Name, the Bidder making the proposal for the goods, services, or public work specified under the attached proposal, and that I executed the said proposal with full authority to do so; that said respondent has not directly or indirectly entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free, competitive bidding in connection with the above proposal, and that all statements contained in said bid proposal and in this affidavit are true and correct, and made with full knowledge that the **Customer Name** relies upon the truth of the statements contained in said bid proposal and in the statements contained in this affidavit in awarding the contract for the said goods, services, or public work.*

*I further warrant that no person or selling agency has been employed or retained to solicit or secure such contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee, except bona fide employees or bona fide established commercial or selling agencies maintained by:*

Bidder Name

\_\_\_\_\_  
*Authorized Signature*

Title



Subscribed and sworn before me

this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_

\_\_\_\_\_  
Notary Public of New Jersey

My commission expires \_\_\_\_\_, 20\_\_\_\_

SEAL

**16.3. Affirmative Action Affidavit  
(P.L. 1975, C.127)**

**Bidder Name:** Stericycle, Inc.

**Street Address:** 2355 Waukegan Rd

**City, State Zip:** Bannockburn, IL, 60015

*Bid Proposal Certification:*

*Indicate below your compliance with New Jersey Affirmative Action regulations. Your proposal will be accepted even if you are not in compliance at this time. No contract and/or purchase order may be issued, however, until all Affirmative Action requirements are met.*

*Required Affirmative Action Evidence:*

*Procurement, Professional & Service Contracts (Exhibit A)*

*Supplier Partners must submit with proposal:*

1. A photocopy of their Federal Letter of Affirmative Action Plan Approval

OR

2. A photocopy of their Certificate of Employee Information Report

OR

3. A complete Affirmative Action Employee Information Report (AA302)

*Public Work – Over Fifty Thousand Dollars (\$50,000) Total Project Cost:*

Check One –

*No approved Federal or New Jersey Affirmative Action Plan. We will complete Report Form AA201-A upon receipt from the Stericycle, or*

*Approved Federal or New Jersey Plan – certificate enclosed*

*I further certify that the statements and information contained herein, are complete and correct to the best of my knowledge and belief.*

Stericycle

*James W. Randall*

Authorized Signature

RVP, National Accounts

11/2/2020

P.L. 1995, c. 127 (N.J.A.C. 17:27)

MANDATORY AFFIRMATIVE ACTION LANGUAGE

PROCUREMENT, PROFESSIONAL & SERVICE CONTRACTS

During the performance of this contract, the Supplier Partner agrees as follows:

The Supplier Partner or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. The Supplier Partner will take affirmative action to ensure that such applicants are recruited and employed, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The Supplier Partner agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this non-discrimination clause.

The Supplier Partner or subcontractor, where applicable will, in all solicitations or advertisement for employees placed by or on behalf of the Supplier Partner, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation.

The Supplier Partner or subcontractor, where applicable, will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice, to be provided by the agency contracting officer advising the labor union or workers' representative of the Supplier Partner's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The Supplier Partner or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to P.L. 1975, c. 127, as amended and supplemented from time to time and the Americans with Disabilities Act.

The Supplier Partner or subcontractor agrees to attempt in good faith to employ minority and female workers trade consistent with the applicable county employment goal prescribed by N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time or in accordance with a binding determination of the applicable county employment goals determined by the Affirmative Action Office pursuant to N.J.A.C. 17:27-5.2 promulgated by the Treasurer pursuant to P.L. 1975, C.127, as amended and supplemented from time to time.

The Supplier Partner or subcontractor agrees to inform in writing appropriate recruitment agencies in the area, including employment agencies, placement bureaus, colleges, universities, labor unions, that it does not discriminate on the basis of age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The Supplier Partner or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the state of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

The Supplier Partner or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and lay-off to ensure that all such actions are taken without regard to age, creed, color, national origin, ancestry, marital status, sex, affectional or sexual orientation, and conform with the applicable employment goals, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The Supplier Partner and its subcontractors shall furnish such reports or other documents to the Affirmative Action Office as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Affirmative Action Office for conducting a compliance investigation pursuant to Subchapter 10 of the Administrative Code (NJAC 17:27).

  
\_\_\_\_\_  
Signature of Procurement Agent

#### 16.4. Political Contribution Disclosure Form

##### Public Agency Instructions

This page provides guidance to public agencies entering into contracts with business entities that are required to file Political Contribution Disclosure forms with the agency. **It is not intended to be provided to Supplier Partners.** What follows are instructions on the use of form local units can provide to Supplier Partners that are required to disclose political contributions pursuant to N.J.S.A. 19:44A-20.26 (P.L. 2005, c. 271, s.2). Additional information on the process is available in Local Finance Notice 2006-1 ([www.nj.gov/dca/lgs/lfns/lfnmenu.shtml](http://www.nj.gov/dca/lgs/lfns/lfnmenu.shtml)).

1. The disclosure is required for all contracts in excess of seventeen thousand five hundred dollars (\$17,500) that are **not awarded pursuant to a “fair and open” process** (N.J.S.A. 19:44A-20.7).
2. Due to the potential length of some Supplier Partner submissions, the public agency should consider allowing data to be submitted in electronic form (i.e., spreadsheet, pdf file, etc.). Submissions must be kept with the contract documents or in an appropriate computer file and be available for public access. **The form is worded to accept this alternate submission.** The text should be amended if electronic submission will not be allowed.
3. The submission must be **received from the Supplier Partner and** on file at least ten (10) days prior to award of the contract. Resolutions of award should reflect that the disclosure has been received and is on file.
4. The Supplier Partner must disclose contributions made to candidate and party committees covering a wide range of public agencies, including all public agencies that have elected officials in the county of the public agency, state legislative positions, and various state entities. The Division of Local Government Services recommends that Supplier Partners be provided a list of the affected agencies. This will assist Supplier Partners in determining the campaign and political committees of the officials and candidates affected by the disclosure.
  - a) The Division has prepared model disclosure forms for each county. They can be downloaded from the “County PCD Forms” link on the Pay-to-Play web site at [www.nj.gov/dca/lgs/p2p](http://www.nj.gov/dca/lgs/p2p). They will be updated from time-to-time, as necessary.
  - b) A public agency using these forms **should edit them to properly reflect the correct legislative district(s)**. As the forms are county-based, **they list all legislative districts** in each county. **Districts that do not represent the public agency should be removed from the lists.**
  - c) Some Supplier Partners may find it easier to provide a single list that covers all contributions, regardless of the county. These submissions are appropriate and should be accepted.
  - d) **The form may be used “as-is”, subject to edits as described herein.**
  - e) The “Supplier Partner Instructions” sheet is intended to be provided with the form. It is recommended that the Instructions and the form be printed on the same piece of paper. The form notes that the Instructions are printed on the back of the form; where that is not the case, the text should be edited accordingly.
  - f) The form is a Word document and can be edited to meet local needs, and posted for download on web sites, used as an e-mail attachment, or provided as a printed document.

5. It is recommended that the Supplier Partner also complete a "Stockholder Disclosure Certification." This will assist the local unit in its obligation to ensure that Supplier Partner did not make any prohibited contributions to the committees listed on the Business Entity Disclosure Certification in the twelve (12) months prior to the contract. (See Local Finance Notice 2006-7 for additional information on this obligation) A sample Certification form is part of this package and the instruction to complete it is included in the Supplier Partner Instructions. **NOTE: This section is not applicable to Boards of Education.**

### C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM Supplier Partner Instructions

Supplier Partners receiving contracts from a public agency that are NOT awarded pursuant to a "fair and open" process (defined at N.J.S.A. 19:44A-20.7) are subject to the provisions of P.L. 2005, c. 271, s.2 (N.J.S.A. 19:44A-20.26). This law provides that ten (10) days prior to the award of such a contract, the Supplier Partner shall disclose contributions to:

- 1) any State, county, or municipal committee of a political party,
- 2) any legislative leadership committee<sup>1</sup>,
- 3) any continuing political committee (a.k.a., political action committee),
- 4) any candidate committee of a candidate for, or holder of, an elective office:
  - a) of the public entity awarding the contract,
  - b) of that county in which that public entity is located,
  - c) of another public entity within that county,
  - d) or of a legislative district in which that public entity is located or, when the public entity is a county, of any legislative district which includes all or part of the county. The disclosure must list reportable contributions to any of the committees that exceed three hundred dollars (\$300) per election cycle that were made during the twelve (12) months prior to award of the contract. See N.J.S.A. 19:44A-8 and 19:44A-16 for more details on reportable contributions.

N.J.S.A. 19:44A-20.26 itemizes the parties from whom contributions must be disclosed when a business entity is not a natural person. This includes the following:

- 1) individuals with an "interest" ownership or control of more than ten percent (10%) of the profits or assets of a business entity or 10% of the stock in the case of a business entity that is a corporation for profit,
- 2) all principals, partners, officers, or directors of the business entity or their spouses,
- 3) any subsidiaries directly or indirectly controlled by the business entity,
- 4) IRS Code Section 527 New Jersey based organizations, directly or indirectly controlled by the business entity and filing as continuing political committees, (PACs). When the business entity is a natural person, "a contribution by that person's spouse or child, residing therewith, shall be deemed to be a contribution by the business entity." [N.J.S.A. 19:44A-20.26(b)] The contributor must be listed on the disclosure. Any business entity that fails to comply with the disclosure provisions shall be subject to a fine imposed by ELEC in an amount to be determined by the Commission which may be based upon the amount that the business entity failed to report. The enclosed list of agencies is provided to assist the Supplier Partner in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the Supplier Partner's responsibility to identify the specific committees to which contributions may have been made and need to be disclosed. The disclosed information may exceed the minimum requirement. The enclosed form, a content-consistent facsimile, or an electronic data file containing the required details (along with a signed cover sheet) may be used as the Supplier Partner's submission and is disclosable to the public under the Open Public Records Act. The Supplier Partner must also complete the attached Stockholder Disclosure Certification. This will assist the agency in meeting its obligations under the law.

**NOTE: This section does not apply to Board of Education contracts.**

<sup>1</sup> N.J.S.A. 19:44A-3(s): "The term "legislative leadership committee" means a committee established, authorized to be established, or designated by the President of the Senate, the Minority Leader of the Senate, the Speaker of the General Assembly or the Minority Leader of the General Assembly pursuant to section 16 of P.L.1993, c.65 (C.19:44A-10.1) for the purpose of receiving contributions and making expenditures."





Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount
Contributor Name	Recipient Name	Date	\$Amount

Check here if the information is continued on subsequent page(s)

**List of Agencies with Elected Officials Required for Political Contribution Disclosure**

N.J.S.A. 19:44A-20.26

**County Name:**

State: Governor, and Legislative Leadership Committees

Legislative District #s:

State Senator and two members of the General Assembly per district.

County:

Freeholders  
{County Executive}

County Clerk  
Surrogate

Sheriff

Municipalities (Mayor and members of governing body, regardless of title):

**USERS SHOULD CREATE THEIR OWN FORM, OR DOWNLOAD FROM [WWW.NJ.GOV/DCA/LGS/P2P](http://WWW.NJ.GOV/DCA/LGS/P2P) A COUNTY-BASED, CUSTOMIZABLE FORM.**

**16.5. Stockholder Disclosure Form**

**Name of Business:**

I certify that the list below contains the names and home addresses of all stockholders holding ten percent (10%) or more of the issued and outstanding stock of the undersigned.

OR

I certify that no one stockholder owns ten percent (10%) or more of the issued and outstanding stock of the undersigned.

**Check the box that represents the type of business organization:**

- Partnership
- Corporation
- Sole Proprietorship
- Limited Partnership
- Limited Liability Corporation
- Limited Liability Partnership
- Subchapter S Corporation

Sign and notarize the form below, and, if necessary, complete the stockholder list below.

Stockholders:

Name: Stockholder Name	Name: Stockholder Name
Home Address: Home Address	Home Address: Home Address
Name: Stockholder Name	Name: Stockholder Name
Home Address: Home Address	Home Address: Home Address
Name: Stockholder Name	Name: Stockholder Name
Home Address: Home Address	Home Address: Home Address
Subscribed and sworn before me this ____ day of _____, 2 ____.	_____ (Affiant)
(Notary Public)	_____ (Print name & title of affiant)
My Commission expires:	_____ (Corporate Seal)

**17. Required Documents for Supplier Partners Intending to Do Business in Arizona**

**17.1. Arizona Supplier Partner Requirements**

AZ Compliance with Federal and state requirements. Supplier Partner agrees when working on any federally assisted projects with more than two thousand dollars (\$2,000.00) in labor costs, to comply with all federal and state requirements, as well as Equal Opportunity Employment requirements and all other federal and state laws, statutes, etc. Supplier Partner agrees to post wage rates at the work site and submit a copy of their payroll to the member for their files. Supplier Partner must retain records for three years to allow the federal grantor agency access to these records, upon demand. Supplier Partner also agrees to comply with the Arizona Executive Order 75-5, as amended by Executive Order 99-4.

When working on contracts funded with Federal Grant monies, Supplier Partner additionally agrees to comply with the administrative requirements for grants, and cooperative agreements to state, local and federally recognized Indian Tribal Governments.

AZ Compliance with workforce requirements. Pursuant to ARS 41-4401, Supplier Partner and subcontractor(s) warrant their compliance with all federal and state immigration laws and regulations that relate to their employees, and compliance with ARS 23-214 subsection A, which states, "...every employer, after hiring an employee, shall verify the employment eligibility of the employee through the E-Verify program".

CCOG reserves the right to cancel or suspend the use of any contract for violations of immigration laws and regulations. CCOG and its members reserve the right to inspect the papers of any Supplier Partner or subcontract employee who works under this contract to ensure compliance with the warranty above.

**AZ Supplier Partner Employee Work Eligibility.** By entering into this contract, Supplier Partner agrees and warrants compliance with A.R.S. 41-4401, A.R.S. 23-214, the Federal Immigration and Nationality Act (FINA), and all other Federal immigration laws and regulations. CCOG and/or Equalis Group members may request verification of compliance from any Supplier Partner or subcontractor performing work under this contract. CCOG and Equalis Group members reserve the right to confirm compliance. In the event that CCOG or Equalis Group members suspect or find that any Supplier Partner or subcontractor is not in compliance, CCOG may pursue any and all remedies allowed by law, including but not limited to suspension of work, termination of contract, suspension and/or debarment of the Supplier Partner. All cost associated with any legal action will be the responsibility of the Supplier Partner.

**AZ Non-Compliance.** All federally assisted contracts to members that exceed ten thousand dollars (\$10,000.00) may be terminated by the federal grantee for noncompliance by Supplier Partner. In projects that are not federally funded, respondent must agree to meet any federal, state or local requirements as necessary. In addition, if compliance with the federal regulations increases the contract costs beyond the agreed on costs in this solicitation, the additional costs may only apply to the portion of the work paid by the federal grantee.

**Registered Sex Offender Restrictions (Arizona).** For work to be performed at an Arizona school, Supplier Partner agrees that no employee or employee of a subcontractor who has been adjudicated to be a registered sex offender will perform work at any time when students are present, or reasonably expected to be present. Supplier Partner agrees that a violation of this condition shall be considered a material breach and may result in the cancellation of the purchase order at the Equalis Group member's discretion. Supplier Partner must identify any additional costs associated with compliance to this term. If no costs are specified, compliance with this term will be provided at no additional charge.

**Offshore Performance of Work Prohibited.** Due to security and identity protection concerns, direct services under this contract shall be performed within the borders of the United States.

**Terrorism Country Divestments.** In accordance with A.R.S. 35-392, CCOG and Equalis Group members are prohibited from purchasing from a company that is in violation of the Export Administration Act. By entering into the contract, Supplier Partner warrants compliance with the Export Administration Act.

The undersigned hereby accepts and agrees to comply with all statutory compliance and notice requirements listed in this document.

A handwritten signature in black ink that reads "James W. Randall". The signature is written over a yellow rectangular highlight.

Signature of Authorized Representative

11/2/2020





We protect what matters.

Dear Customer,

With over 30 years of experience partnering with businesses, we recognize the importance of continuing to serve you reliably, safely, and compliantly during the Coronavirus (COVID-19) pandemic. We write to assure you that since the onset, we've taken measures to continue to provide you industry-leading guidance and service.

We want to make it clear that *we are in it together and we always have been*. Our team has successfully protected our team members, customers, and communities through natural disasters, pandemics (and the spread of infectious diseases like Ebola), and other states of emergency. Because we are also the leading medical waste service provider, our regulatory team is in close contact with the Centers for Disease Control and Prevention (CDC), other relevant regulatory agencies, and healthcare organization administrators to ensure we deploy the most current protocols for safe, efficient, and compliant management of your secure information.

We have a global, cross-functional team monitoring the situation to ensure precautions are taken and communicated internally to minimize the spread of the virus, and our business continuity plans are executed to continue reliable service. To date at Stericycle and Shred-it:

- We have readied business continuity plans which include pre-designated, alternative transportation routes and treatment locations in the event of shut-downs. We are also ready to deploy operational team members to alternate locations in the event of a facility-specific staffing shortage
- We are providing guidance and ongoing communication to all team members on proper risk mitigation practices including following CDC-approved hand hygiene, operating at safe distances, and proper use of PPE, including gloves
- We are encouraging voluntary quarantine for team members who believe they are at risk and/or report or show signs of symptoms related to COVID-19
- We continue to communicate within our organization to provide guidance on precautionary measures to minimize disease spread at home and work
- We have established a ban on all travel to high-risk countries. Additionally, we are limiting business travel to matters critical to ensuring safety, compliance, and essential customer support

Visit our [COVID-19 Resource Page on Stericycle.com](#) for regular updates, training/webinar details, helpful links, documents, and guidance. In addition, the following resources are available to you:

- Our Customer Experience team by calling 1-800-697-4733
- Access to our regulatory team by emailing [ask-regulatory@stericycle.com](mailto:ask-regulatory@stericycle.com)

- Comprehensive webinar “Coronavirus Waste Management – Facts Not Fear” scheduled for Wednesday, March 25 at 1pm. [Click here to register](#)

Nothing is more important to us than protecting the health and safety of our customers, team members and community. We are grateful for your loyalty and appreciate the privilege to serve you.

With care and respect,

A handwritten signature in black ink that reads "Cindy". The signature is written in a cursive, flowing style.

Cindy J. Miller

Chief Executive Officer

# Stericycle Inc.

is Hereby Granted **NAID AAA Certification**  
by the National Association for Information Destruction



*The National Association for Information Destruction (NAID®) is the non-profit trade association recognized globally as the secure data destruction industry's standards setting and oversight body.*

*The certificate holder has met the rigorous requirements of the NAID AAA Certification program and demonstrated through announced and unannounced audits that its security processes, procedures, systems, equipment, and training meet the standards of care required by all known data protection regulations.\**

*As a result, NAID AAA Certification also serves to meet all data controller vendor selection due diligence regulatory requirements.*

*Valid Through: November 30, 2019*

*The certificate holder is NAID AAA Certified for the following services and media types:*

- Mobile Operation & Plant-based Operations for Paper/Printed Media, Micro Media, Physical Hard Drive, Non-Paper Media & Product Destruction (varies by location)

*Applicable to the following location(s):*

- All North American Locations Providing Information Destruction Services

\*NAID AAA Certification specifications are regularly evaluated/amended as necessary and service provider compliance is verified to ensure ongoing conformance with all known data protection regulations including The Privacy Act (Australia), GDPR (Europe), HIPAA, GLBA, FACTA, State-level requirements (USA), and PIPEDA, PIPA, PHIPA (Canada) in their relevant jurisdiction(s), as well as with related risk assessment, incident reporting and data breach reporting procedures and training as required therein or separately.

*Ronald Manoung*  
NAID Certification Program Official



# SERVICE RECORD CERTIFICATE of DESTRUCTION

PLEASE KEEP THIS FOR YOUR RECORDS : THIS IS NOT AN INVOICE

## Customer Profile

**Site Number: XXXXXXXX**  
Customer Name  
Street Address  
City, State Zipcode

Number of trees saved  
by your firm this year:

**85.364**



## Service Summary



**Order:** XXXXXXXX  
**Order Date:** 10/25/2018  
**Customer PO:**  
**Service Type:** OFF-SITE REGULAR SERVICE  
**Contact:**  
**Time In:** 01:04 PM  
**Time Out:** 01:05 PM  
**Next Shred Date:** 11/07/2018

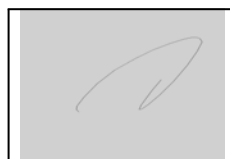
## Service Confirmation



**Service Time:** 1 min  
**Number of Equip Service:** 4  
**Number of Extra Items Collected:** 0  
**Estimated Weight:**

**Customer Name:**  
[NAME]

**CSR Name:** [NAME]



Shred-it is committed to the secure destruction of its customer's confidential information. This certification will affirm that Shred-it destroys the customer confidential material, pursuant to our customer's request and instructions. The following services are NAID certified: Hard Drive Destruction, Mobile Destruction, Offsite Destruction, Non-Paper Destruction.

**Site Number: XXXXXXXX**

If you have any questions or concerns call us at **1-800-697-4733**  
Please have your site number available so we can get you to the right representative for your account.

Shred-it® is a Stericycle solution.



## Service Details

**Equip:** B000XXXXXX- STD. CONSOLE - TELLER - 1/2 Full 10/25/2018 01:04 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Equip:** B000XXXXXX - STD. CONSOLE - CUSTMER SEVICE DESK NUMBER

2 10/25/2018 01:04 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Equip:** D000XXXXXX - Med Tote (64Gal/240L) - UPSTAIRS BY VAULT 10/25/2018  
01:04 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Equip:** D000XXXXXX - Med Tote (64Gal/240L) - UPSTAIRS 10/25/2018 01:05 PM

**Truck:** 1402B 10/25/2018 01:05 PM

**Order: XXXXXXXX**

**Site Number: XXXXXXXX**

If you have any questions or concerns call us at **1-800-697-4733**  
Please have your site number available so we can get you to the  
right representative for your account.

[Shred-it® is a Stericycle solution.](#)





Security  
Policies and Procedures  
Summary

Marla L. Sandlin  
Security & Compliance Manager  
January 30, 2020

## Index

Security and Compliance Program Overview .....	3
<b><u>ADMINISTRATIVE</u></b>	
Security Management Process .....	3
<b><u>TECHNICAL</u></b>	
Information Access Management .....	4
Unique User Identification .....	4
<b><u>PHYSICAL SECURITY</u></b>	
Team Member Security .....	4
Background Checks .....	5
Drug Screen .....	6
Security Awareness and Training .....	6
Security and Compliance Training .....	7
Security Specific Training .....	7
Facility Security Summary .....	8
Visitor Procedures .....	8
Restricted Access to Restricted Areas .....	9
Overhead Doors .....	9
Windows .....	10
Fencing .....	10
Lighting .....	10
Exterior Trash Containers .....	10
Alarm System .....	10
CCTV Monitoring System .....	10
Repairs and Maintenance .....	11
Fire Protection .....	11
<b><u>SERVICE PROCESS</u></b>	
<b><i>CUSTOMER SECURITY REPRESENTATIVE</i></b>	
Safety .....	11
Licensing Requirements .....	11
Vehicle Insurance Cards .....	11
Vehicle Safety .....	11
Vehicle Security .....	11
Vehicle Accident Procedures .....	12
Containers .....	12
Communications .....	12
Service Types .....	13
Start of Day Procedures .....	13
At the Customer Site .....	13
After Taking Possession of CCM .....	14
CSR Security Matters .....	14
<b><u>PLANT OPERATIONS</u></b>	
Pre-Destruction .....	14
Destruction Timeframe .....	14
Destruction Process .....	15
Witnessed Destruction .....	15
Maintenance .....	15
Contingency Plan .....	15
Post Destruction .....	16
Facility End of Shift Closing .....	16
Quality Control .....	16
Security Incident Procedures .....	16
Disaster Recovery Plan .....	17

## **Security and Compliance Program**

The Shred-it Security and Compliance Program outlines the steps taken at Shred-it to ensure compliance with safeguarding customer information. Shred-it, acting as a service provider, is required to implement appropriate measures designed to meet the objectives of the safeguarding guidelines.

Shred-it has developed the Security and Compliance Program to document the required guidelines for service providers to implement a written security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the service provider and the nature and scope of its activities. The program is designed to ensure the security and confidentiality of customer information, protect against unanticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. As a service provider, Shred-it must assess risks to customer information and implement appropriate policies, procedures and training to manage and control these risks. Customer information is defined as any record, in paper or other form, containing non-public personal information of a customer. Shred-it's business operation model is to provide information security to our customers and therefore treats all customer information, in all formats, as protected personal information. The personal identifiable information is considered in our chain of custody from the pick up at the customer location and throughout the life of the document.

The following administrative, technical and physical safeguards are identified as part of the Security and Compliance Program.

### **ADMINISTRATIVE**

#### **Security Management Process**

An overall information security management process is necessary to establish policy, provide oversight, and administer operational aspects of the Shred-it Security and Compliance Program. The process functions in a proactive, risk-appropriate manner and establishes the framework for safeguarding protected personal information. An information security policy commits Shred-it to safeguard protected personal information, to establish goals, and to assign responsibility. Supporting policy statements and procedures facilitate the prevention, detection, containment, and correction of security breaches.

The Security Team is responsible for security oversight and operational aspects of safeguarding customer personal information. Shred-it maintains security policies that identify and communicate security responsibilities of Team Members who access, or manage access, to protected personal information.



Shred-it has zero tolerance for compromising protected personal information. The Security Incident Reporting Policy notes that all Team Members are expected to follow the security protocols and abide by and fully comply with all of Shred-it's security policies and procedures. Shred-it will appropriately discipline and sanction Team Members for any violation of the security policies and procedures, will investigate and mitigate security violations and incidents in a timely manner, and will not intimidate or retaliate against any Team Members or individual who reports a security violation or incident. Sanctions against Team Members that do not comply with, or violate security policies and procedures shall be commensurate with the gravity of the violation. The sanctions shall include, but are not limited to, re-training, verbal and written warnings and termination.

## **TECHNICAL**

### **Information Access Management**

Shred-it maintains policies and procedures for granting access to protected personal information. Shred-it has established policies and procedures to assign, implement, revoke and modify access to all information systems. Proper controls over the user access to computer systems and data are maintained at all times. The system includes a technical means to control information access and access is terminated upon removal from the employment systems.

### **Unique User Identification**

Shred-it must be able to uniquely identify and track users or Team Members for the purpose of access control to all networks, systems, and applications that contain protected personal information. To monitor access to the networks, systems and applications which contain protected personal information, Team Members must be provided a unique user identification name. When requesting access to any network, system, or application that accesses, transmits, receives, or stores protected personal information, a user or Team Member must supply an assigned unique user identification name and a secure password. Team Members must not write down or allow other Team Members to use their unique identification name and password. It is the responsibility of all Team Members to ensure that their assigned user identification name and password are appropriately protected and only used for legitimate access to networks, systems, or applications. If Team Members believe their user identification name and password have been comprised, they must report that as a security incident.

## **PHYSICAL SECURITY**

### **Team Member Security Summary**

Shred-it has a Team Member security clearance process to determine administratively that Team Members are trustworthy before giving them access to personally identifiable information (PII). Awareness training on these policies and procedures is required both for those who are cleared for and given access and for those who have incidental access.

Any person that comes into a facility is an Access Team Member, a Non-Access Team Member or a Visitor (including vendors). Access Team Members must have all the proper documentation, security training and testing completed upon hire and updated annually before they will have access to all areas of the facility. Non-Access Team Members are limited to only areas that do not have customer confidential material (CCM). All visitors, maintenance and vendor personnel are required to sign a Confidentiality Agreement and be escorted at all times when in an area containing PII.

Shred-it maintains documentation regarding the levels of access granted to each Team Member, program and procedure. Shred-it periodically reviews access levels including when the status of the Team Member changes.

Shred-it conducts background checks on all applicants for pre-employment, including residence, employment, and drug testing (where permitted) whenever there is access to PII. All Shred-it Team Members with access to CCM are subject to an annual background and random drug test (where permitted). In regions where random drug testing may not be permitted, all supervisors and managers would be required to complete a Substance Abuse & Reasonable Suspicion training. All Team Members are required to sign Confidentiality Agreements at hire and annually thereafter.

### **Background Checks**

- All Team Members with access to customer material will complete a consent and authorization form for the purpose of conducting pre-hire and annual background checks.
- Federal District Court (7 years felony and misdemeanor based on residency history revealed from social security number trace – where permitted)
- Statewide Criminal – where available (7 years felony and misdemeanor based on residency history revealed from social security number trace – where permitted)
- County Criminal (7 years felony and misdemeanor based on residency history revealed from social security number trace – where permitted)
- Social Security Trace and Validation (reveals all addresses on file for the Team Member and validates the issuance of the social security number to the Team Member and date of issuance – where permitted)
- National Sex Offender Search (verified through name, social security number and date of birth – where permitted)
- Prohibited Parties Check (Office of Foreign Asset Control (OFAC), Specially Designated Nationals, Terrorists, Narcotics Traffickers, Blocked Persons and Vessels, Debarred Parties, Denied Persons List, Entity List, and Unverified List – where permitted)

- Background checks will be completed by Shred-it approved third party vendor and all results will be reviewed by Shred-it management and Human Resources to ensure compliance with Shred-it Policy, National Association of Information Destruction (NAID) standards, and customer requirements
- Background checks that do not meet Shred-it policy, NAID standards, or customer requirements will be reviewed by the Human Resources Compliance Department
- If the Human Resources Compliance Department determines that background checks do not meet Shred-it policy, NAID Standards, and customer requirements, this may result in the Team Member's termination of employment

### **Drug Screens**

- All Team Members with access to customer material will complete a consent and authorization form for the purpose of conducting a drug screen pre-hire and randomly (where permitted)
- Drug screens will be completed by Shred-it approved third party vendors and all results will be reviewed by Shred-it management to ensure compliance with Shred-it policy, NAID standards, and customer requirements
- Refusal to submit to the drug screening will result in immediate termination
- Positive test results, as determined by Human Resources Compliance Department will result in immediate termination
- Negative dilute test results, as determined by the HR Compliance, will result in a second drug screen being administered. Two consecutive negative dilute test results, as determined by HR Compliance, will result in immediate termination
- Drug screens that do not yield a negative result for any other reason, as determined by HR Compliance, will result in a second drug screen being administered. Two consecutive tests that do not yield a negative result for any other reason, as determined by HR Compliance, will result in immediate termination

### **Security Awareness and Training**

Security training is provided for all employees who access PII. This training includes overall security awareness, periodic reminders, virus awareness, password management, and user-specific topics necessary for individual workstation security. The facility is responsible for the tracking of annual security awareness training.

Topics include:

- Protecting personally identifiable information
- Reporting security incidents
- Managing individual passwords

- Types of confidential information
- Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA) and Fair and Accurate Credit Transactions Act (FACTA)
- Payment Card Industry (PCI) Compliance
- Code of Conduct and Business Ethics

Shred-it requires additional security awareness training for Access Team Members that addresses, at a minimum:

- Monthly Compliance Self-Audits/Inspections (physical security access, alarm tests, uniforms, badges and key cards)
- Monthly review of security policies
- Annual review and signature of Team Member Confidentiality Agreement
- Annual review and acknowledgement of Security Incident Reporting Policy

### **Security Specific Training**

- All Access Team Members shall be trained for compliance with Security and Operating Policies and Procedures within 5 days of their start date. Training shall be based on the most current version of Security and Operating Policies & Procedures.
- Until training and satisfactory background check has been completed, new Team Members shall be treated as Non-Access.
- Team Members shall be made aware that consumers are provided protection against unauthorized disclosure and use of CCM that is in the possession of others. Protections are afforded through GLBA, HIPAA Privacy Rules, and FACTA as well as through a variety of other federal and state laws. There shall be no instances in which CCM shall be disclosed to anyone, unless specifically required by law.
- Team Members re-training shall be required in the event of any of the following:
  - Significant changes in or additions to privacy laws and/or policies
  - Significant changes in NAID Certification requirements
  - Team Members violation of a Security Policy
  - Security Breach or more than one security incident involving the same Team Members
  - At the discretion of management
- All Access Team Members shall be required to review all Security and Operating Policies and Procedures and to sign – Operations and Security Policy Acknowledgement annually. The District Operations Manager (DOM) shall verify completion of Operations and Security Policy Acknowledgement and successfully completed Security Training Assessment.

- All facilities are required to complete weekly service and production security meetings for the purpose of brief training sessions and reminders on Shred-it security rules.
  - Training topics should include items covered in security policies, NAID, HIPAA and industry information.

### **Facility Security Summary:**

Shred-it maintains policies and procedures to limit physical access to its facilities while ensuring that properly authorized access is allowed. This ensures that access to facilities used to house PII is appropriately controlled and that procedures are properly documented to safeguard all facilities, systems, and equipment from unauthorized physical access, tampering, or theft. The Facility Security Policy provides guidelines to control and validate Team Members' access to all facilities used to house protected information. The policy also provides procedures to control, validate, and document visitor access to any facility. This procedure applies to vendors, repair personnel, and other non-workforce members.

Shred-it facilities shall ensure the utmost in security by meeting or exceeding certification standards established by NAID. Additionally, facility security shall be sufficient to meet applicable state and federal privacy regulations such as HIPAA and GLBA. In order to meet these requirements, the following are the minimum expectations for any facility that processes or retains CCM.

**Visitor Procedures:** All visitors must sign the Visitor Log which requires them to show a government issued ID and sign a Confidentiality Agreement stating they will abide by all the facility's procedures. If the visitor is an official inspector or third party auditor, they must first show their credentials documentation when signing the Visitor Log and Confidentiality Agreement, then be escorted to a conference room until executive leadership is contacted. If the visitor is entering the Restricted Area, their phone should be kept in the Non-Restricted Area. The visitor must also be briefed by Team Members on the facility's Environmental and Health & Safety protocol.

Each facility will maintain a Visitor Log for 12 months. The Visitor Log should include date, time, name of visitor, what is the purpose of their visit, which Team Member will be escorting, confidentiality agreement number and visitor badge ID#. Confidentiality Agreement and Visitor Code of Conduct are valid for and shall be maintained for 12 months.

All Team Members must prominently wear their Shred-it identification badge while performing Shred-it duties on or off the facility premises. All damaged, outdated and terminated Team Member badges will be destroyed through the shredding process.

Visitors shall conspicuously wear a visitor badge at all times while on Shred-it premises. Badges shall not be issued to a visitor until after the Visitor Log entry and signing of Confidentiality and

Visitor Code of Conduct Agreement have been completed. Badges shall be retrieved upon exit of the premises. No visitor, regardless of the regularity of their visits, shall be allowed to retain their visitor badge. Should any individuals be found in a Restricted Area or on premise that does not have a visitor badge, the person shall be immediately escorted to the office Non-Restricted Area, and the Facility Authorized Team Member shall be contacted to resolve the matter and follow visitor sign in procedures.

All visitors shall be escorted and kept under the direct visual supervision of an Access Team Member at all times while in a Restricted Area. An exception may be granted to emergency personnel only when responding to an emergency.

Restricted Area - while in a Restricted Area, visitors may NOT:

- Bring anything into or out of the area (i.e. brief cases, bags, notebooks, purses, etc.) except to carry tools or other equipment that may be needed to conduct repairs. No cell phones with cameras will be allowed into a Restricted Area. Auditors may take audit forms and pertinent audit documentation into and out; however, nothing that may constitute CCM or that originated in a Restricted Area may be taken out. All forms, papers and other materials from a Restricted Area shall be subject to the inspection by the Facility Authorized Team Member prior to exit of the Restricted Area. An exception may be granted to emergency personnel only when responding to an emergency and only for such items that may be required to properly respond to the emergency situation.
- Observe operations including the unloading of containers, conveyor system, shredded paper, or bales of paper, etc. from closer than a 10' distance. Exceptions include witnessed destruction in which a customer is witnessing the destruction of CCM that originated from their business, safety or regulatory audits Occupational Safety and Health Administration (OSHA) audits, repair or maintenance performed by visitors.

**Access to Restricted Areas:** Access to any Restricted Area shall be limited to Access Team Members and appropriately escorted Visitors through the use of card/electronic access or combination door locks. All Restricted Area doors shall be self-closing and auto-locking. Access numbers/cards and combinations shall not be distributed to anyone other than Access Team Members. Access numbers/cards, keys, combinations or other methods of gaining access to CCM or areas containing CCM shall be immediately retrieved from any terminated Team Members to whom these items were issued.

**Roll-up Doors:** Roll-up doors shall remain closed and locked at all times when not in use. These are secured with padlocks after hours. Adjustable dock plates must meet with the roll-up door (when closed) to prohibit access between the plate and door. When opened, the doors must be physically guarded or continuously supervised to prevent unauthorized access. If not continuously supervised, doors shall be affixed with a full open height security gate with a mesh size no greater than 2 square inches (gate must reach from the floor to the open height of the door, with no openings at either the floor or door height level). Screen mesh applied to accordion style gates is acceptable.

**Windows:** Windows shall remain locked at all times during when facility is unoccupied.. Windows shall also be visually secured to prevent the ability to view any Restricted Area or CCM. Windows may be opened to allow air flow during plant operation, as long as they are screened to prevent paper loss and visual security is maintained.

**Fencing:** If allowed by local regulations or leaseholder, facilities shall have secure perimeter fencing of the maximum allowable height up to 12' high and not more than 2" mesh. Fencing shall start at grade level and reach to full height without break. Internal fencing or walls used to create a Restricted Area and/or separation from another operation shall extend to the ceiling. If fencing does not go to the ceiling it shall have a motion sensor alarm and Closed Circuit Television (CCTV) inside and over the perimeter of the Restricted Area to detect if individuals have climbed over or come through a section of the secured fence/wall.

**Lighting:** Outside lighting shall be set to be on from dusk to dawn. Inside lighting shall be sufficient for CCTV to record activity with clarity.

**Exterior Trash Containers:** Exterior trash containers are fully locked or equivalently secured with access limited to the Facility Manager or their designee. Trash containers may be opened to receive office/shop trash and to be emptied by trash haulers. An alternate to locking is storage of the containers in the Restricted Area. Placing CCM or documents (shredded or unshredded) in a trash dumpster is not allowed under any circumstances. No paper shall be baled without first being shredded.

**Alarm System:** All facilities that contain CCM have an actively monitored security system in place. Security systems must be:

- Activated at all times when the facility is not manned
- Actively monitored such that the local authority having jurisdiction and an Access Individual will be contacted immediately (within industry standards or local code) by representatives from a third-party monitoring company on notification of an alarm
- Activated or deactivated only by Access Team Members only unless the facility is mobile only and no unshred CCM is received or housed
- Maintained to prevent false alarms. There should be a test by the monitoring company at least monthly to ensure the system is in good working order. Notification of such test shall be provided and retained by the location for 12 months

**CCTV Monitoring System:** All facilities that contain CCM have an operating CCTV system that:

- Monitors all points of ingress and egress into Restricted Areas (including enclosures, cages, shipping containers, etc.)
- Provides sufficient image clarity as to readily enable identification of individuals accessing Restricted Areas and the nature of their activities
- System must maintain a stored record of all images for a minimum of 90 days

- The stored record must be secured from theft or vandalism by being locked inside a lockable cage or lockable cabinet. Accordingly, it should only be accessible by management Team Members
- All processing areas must have coverage to a minimum of entry and exit portals
- The system utilizes a hard drive and/or cloud based back-up system versus compact discs, VCR tapes, or other
- All non-compliant safety and/or security actions taken by Team Members viewed on the CCTV system must be documented and appropriate disciplinary action taken

**Repairs and Maintenance:** Any and all repairs or modifications to the physical components of a Shred-it facility (including but not limited to alarms, CCTV and Access Controls) shall be recorded with downtime information submitted on a weekly basis.

Operational security maintenance checks shall be completed on a weekly and monthly basis by the FM or their designee. These checks are designed to verify proper functioning of the facility alarm and CCTV systems, as well as proper visitor procedures and other security items.

**Fire Protection:** Locations shall maintain compliance with applicable local fire codes. A fire protection assessment and service shall be conducted at least annually.

### **SERVICE PROCESS**

**NAID AAA Certification:** NAID AAA Certification standards set forth certain criteria specific to the Customer Security Representative (CSR).

**Safety:** CSRs shall at all times wear proper personal protective equipment while handling any CCM. These include but are not be limited to safety glasses, gloves, hats, ear protection, etc.

**Licensing Requirements:** A CSR must possess a current, valid driver's license which meets all state and federal requirements for the class of vehicle they will operate. The CSR must immediately notify their supervisor if the license status changes. CSRs shall keep their license and medical card current and in their possession while operating a Shred-it vehicle.

**Vehicle Insurance Cards:** Prior to driving any Shred-it vehicle, CSRs shall ensure that Shred-it insurance cards are in the vehicle. The CSR must immediately inform their supervisor and follow their directions for resolution if there is no insurance card in the vehicle.

**Vehicle Safety:** All CSRs shall exercise extreme caution in all phases of vehicle operation. No Team Member shall place themselves or others at risk for any reason.

### **Vehicle Security:**

- Except in the case of an emergency, no unauthorized person shall be permitted access to the cab, body, box, payload or tail-lift of any vehicle. No unauthorized person shall be transported as a passenger at any time except in case of an emergency.



- All vehicles used for transfer or destruction of CCM shall be fully lockable. Cabs, boxes, and any storage areas must remain locked at all times when not attended by a Shred-it Access Individual.
- All un-shredded CCM shall be securely contained during transport to the facility.
- All Collection vehicles will have a corporate approved audible alarm system or a high security padlock on the rear to ensure the security of the customer material inside the truck.

**Vehicle Accident Procedures:**

- When a Stericycle/Shred-it truck is involved in an accident while transporting CCM, the driver must remain with the vehicle and immediately notify facility management of the facility receiving the material for further instruction. CCM may not be left unattended.
- If the truck is inoperable, the facility will send a second truck to transfer materials safely and securely back to the warehouse for final destruction.
- Facility Management is required to file the Accident Reporting for Claims Management and enter the accident into SEMS.

**Containers:** All containers used to transport customer confidential material (CCM) must have operable locks. Containers must remain locked at all times during which they contain CCM unless attended directly by an Access Individual. Once emptied, containers shall be completely free from un-shredded material. All security containers must be checked by the location/warehouse Team Members when emptied. All security containers must be checked again prior to loading on the collection trucks and checked again prior to servicing at the customer site.

**Communications:** All CSRs and helpers shall have fully operating two-way communication devices in their possession at all times. This includes driving to and from customer sites and during the collection or destruction process. Exception is made only for customer environments in which the possession and/or use of two-way communication devices is prohibited (some hospitals, clinic buildings, etc.).

- Handheld or other wireless electronic devices are prohibited to be used while operating a moving vehicle. These items are considered “additional equipment and accessories” and decrease the safe operation of the vehicle.
- Vehicle operators are required to operate wireless phones in a “hands free” mode where both hands can remain on the wheel or required to safely pull off the road. The Company has more strict requirements for DOT regulated drivers to include a strict prohibition of any wireless communication device unless the driver is legally parked in an appropriate safe location. Texting is not allowed while operating a moving vehicle.

## **SERVICE TYPES**

- **On-site destruction** shall take place fully while at the customer site using a mobile shred truck. CSRs shall ensure all CCM is fully destroyed prior to leaving the customer site.
- **Off-site destruction** allows Shred-it to collect the materials from the customer site and transfer it back to the secure facility where the final destruction takes place using state of the art document shredding equipment.

**Start of Day Procedures:** CSRs shall comply with the following in preparing for their daily route.

- Must wear a uniform and display Photo I.D. Badge ensuring the customer can see it at all times.
- CSRs shall:
  - Review their schedule for services, start of day instructions and special instructions. CSRs are expected to resolve any questions with their supervisor prior to beginning their route.
  - Ensure their truck is loaded with security containers, pallets or any other items that may be required to execute the assigned services.
  - Ensure that all supplies needed are on their truck. For example: straps, shrink-wrap, blank work orders, locks, city maps, etc.
  - Request the assistance of a helper if needed.

### **At the Customer Site**

CSRs shall be courteous, professional, and polite and shall conduct themselves with appropriate interaction with customer personnel. CSRs are expected to provide superior service with a minimum level of distraction to customer operations.

If a customer makes a reasonable, policy compliant request, CSR shall comply. If the request is unusual but does not seriously delay the route or violate policy, CSR should accommodate the request and notify their supervisor. If a customer makes a request that is unreasonable, delays the route, compromises security, violates policy or is otherwise inappropriate, CSR shall not comply and shall notify their supervisor immediately. The supervisor shall advise CSR on how to proceed.

If a customer expresses any complaint, the CSR shall listen to and document the matter and offer to convey the information to the Facility Manager (FM). CSR shall also invite the customer to convey their comments to the FM. The CSR shall also communicate the customer's concerns to their supervisor.

### **After taking possession of CCM:**

- No container may be left unattended outside of the customer's facility.
- Containers that remain in the customer's facility but will not be physically attended shall be locked.
- Containers that are physically attended by a CSR may be unlocked during the collection process. Containers must be locked whenever unattended and always during transfer to and from the vehicle.
- No person, including the customer, shall be allowed to examine or retrieve materials once taken into possession. If a person claims to have the right to look through the materials or retrieve something from a locked container, the CSR should determine if the request is from the authorized contact and they must contact their supervisor.
- Once in possession, the CCM will be continuously attended or physically secured from unauthorized access.
- Under no circumstances shall any Team Member discard any un-shredded paper, product, or other material into any unsecured area.

Service orders shall be properly completed for services provided and may contain any customer concerns or comments (missing locks, moved or missing containers, key requests, etc.).

**CSR Security Matters:** CSRs are required to attempt to secure all CCM and immediately report any incident where customer confidential information was compromised to their supervisor.

## **PLANT OPERATIONS – OFFSITE DESTRUCTION**

### **NAID Certification Standards for Destruction of CCM**

NAID Certification standards set forth certain criteria for operational security and plant-based operations. This section outlines those items specific to plant operations.

**Pre-Destruction:** All CCM received from routine service will enter the destruction process upon arrival at the facility. Incoming service containers will be completely emptied, cleaned and rotated back into service. Facility Team Members must check all service containers to ensure they are completely empty of CCM.

**Destruction Timeframe:** All CCM from routine service shall be destroyed within three business days of receipt. An exception may be made for acts of God, breakdowns, written customer instructions to retain the media for a longer period or other circumstances beyond Shred-it's control. Destruction of CCM from customer purges must take place within the requirements as defined by the facility NAID Certification type. In any case in which an exception is made, security of materials shall be maintained.

**Destruction Process:** Destruction processes shall comply with NAID Certification standards for maximum particle size of the media type destroyed. NAID requirements for particle size of cross cut or pierce and tear – ¾" x 2.5" length (19mm x 63mm).

- Paper or printed media:
  - ✓ Mobile Shred truck: Shredtech and ShredFast truck types: ¾" x 2.5" length (19mm x 63mm). Size may vary for non-paper CCM.
  - ✓ SMS Truck: 1 ½" x 5/8" (38mm x 16mm). Size may vary for non-paper CCM.
  - ✓ Plant-based Equipment –Rotary grinder – 2" diameter screen
- Micro media: Microfilm and Microfiche must be reduced to 1/8" or less in width. A location may not accept micro media or must send it out for incineration if it cannot meet this requirement.
- Hard drives: Hard drives shall be destroyed using the shearing method or hydraulic punch to ensure that the hard drive is rendered irreparably un-readable. Any location destroying Hard Drives shall be NAID Certified for this service.

**Witnessed Destruction:** Only the FM or their designee may authorize an appointment for witnessed destruction. Customer scheduling needs will be accommodated on a best efforts basis. CCM may be delivered to the facility either by a CSR or by the customer. If delivered by the CSR, the materials shall be securely stored until the customer representative arrives. The Facility Security Policy outlines proper security measures for all visitors and contains the Confidentiality and Visitor Code of Conduct Agreement which must be signed by all visitors. Upon compliance with all proper security measures, the witness will be escorted to the witnessing area. No other CCM may be readily visible. The destruction process shall be conducted as close to the time of the customer's arrival as possible.

**Maintenance:** The FM shall ensure that all equipment is properly maintained, including the performance of any required or recommended preventative maintenance procedures and the performance of any needed repairs.

**Contingency Plan:** In the event of equipment breakdown such that the time for repair is expected to be greater than 48 hours, the Facility Manager shall immediately notify the Regional Vice President and trigger a local contingency plan per the following parameters:

- Collection of CCM may continue so long as it is stored in a Restricted Area.
- On-site shredding trucks may be utilized for shredding within the Restricted Area provided that proper ventilation for exhaust is maintained.
- Materials may be taken to another Shred-it location for processing provided that transportation of materials is made in a secure vehicle.
- Should insufficient Restricted Area space be available for the time required for repair, and other contingency actions unavailable, additional security containers may be delivered to customers with notification of any temporary schedule change.

**Post Destruction:** All recycling must only be sent to approved recycling vendors. Any deviations to this must be reviewed and approved through the exception process. In no cases, shall shredded paper be utilized for any other purpose (animal bedding, package fill, etc.) than recycling.

**Facility End of Shift Closing:**

- Production Team Members shall sweep the entire exposed floor and pass the sweepings through the destruction process.
- The FM or their designee shall dismiss Team Members. At this time, Team Members shall return any company-related items (including all keys) and necessary paperwork that were used or completed.
- At the end of each day the FM or their designee shall perform a visual quality control and security inspection.

**Quality Control:**

- Process Control – All destroyed CCM shall be verified to comply with the standards set forth in “Destruction Process”. Examinations shall be made by the FM or their designee. Should any non-compliant CCM be found, the destruction process shall be stopped, root cause identified, and corrective action taken prior to restarting the plant operation.
- Visual Inspection – The FM or their designee shall complete a visual inspection of the facility at the beginning and end of each shift, ensuring that:
  - There are no breaches in security.
  - The areas surrounding the plant are free from shredded and un-shredded paper.
  - The shredded material (paper and non-paper) size is in compliance with NAID Certification standards.
  - Collection trucks have been completely emptied and are properly locked.
  - Unlocked containers have been completely emptied.
  - All non-shredded CCM is properly stored in a Restricted Area.
  - Any discovery that may result in a security weakness is properly remedied immediately or within a reasonable timeframe if immediate remedy is not possible. This must be reported immediately to the Security Team.

**Security Incident Procedures**

- A Security incident occurs when there is either loss or breach of company confidential or proprietary data/information. Loss of information/data may take either paper/hard copy or electronic form.
- All Shred-it Team Members, regardless of job description, have the responsibility to take all reasonable and safe means necessary to ensure the security of the confidential material at all times. This includes summoning of additional assistance, police or local authorities to assist or secure an area, the vehicle, the facility or any other reasonable

measures which do not compromise safety of Team Member or the security of confidential materials.

- All Shred-it Team Members that knowingly or unknowingly cause, initiate, or participate in any violation of security policy or procedure or have knowledge of any actual, potential or threatened security policy or procedure violation, shall immediately report such knowledge to the District Operations Manager/Facility Manager or their supervisor.
- Any incident will be reported electronically through SEMS, an online portal and be promptly reported to their immediate Supervisor, District Operations Manager/Facility Manager, Regional Vice President and Security Team.
- A conference between the DOM/FM, RVP and a member of the Security Team shall be held as soon as possible following receipt of notice to discuss the investigation results, disciplinary action, any requirements to retrain or change policy and to notify the customer.
- Customer notification will include the details collected during the investigation and must include any retraining of Team Members. The customer notification will include any further action or communication for follow up until both parties can close the case. All customer notification will either take the form of a phone call or in writing.
- All Security Incident/breach reports will be reviewed in detail by the Security Team which will determine if changes to policies or procedures could have prevented the incident and/or should be made to prevent future occurrences. Policy and/or procedural changes recommended will be presented to the Security Working Group for approval.
- All incidents are fully investigated by the location, the Security Team, the RVP and the appropriate HR Representative to provide final determination. All security matters are reported weekly to the Senior Vice President – SCS Operations US and Canada.
- Shred-it provides an Ethics and Compliance Hot Line procedure (1-800-451-5340) for receiving and addressing complaints regarding the practices or the actions of Shred-it Team Members and temporary workers. Shred-it prohibits all forms of retribution against any individual who reports actual or suspected violations of regulations, or policies. Shred-it Team Members will not discharge, demote, suspend, threaten, harass, or in any manner, discriminate against any Team Member in terms and conditions of employment based upon any actions of such Team Member with respect to good faith reporting.
- Each Team Member has a responsibility to comply with the laws and behave in an honest and ethical manner. Violating regulations, Shred-it policies, or failing to report such violations can result in serious disciplinary action up to and including termination. In addition, violators could be subject to civil and criminal charges by outside regulatory agencies. Shred-it has a policy of progressive discipline for infractions committed by Team Members, except where immediate termination is identified as the discipline.

#### **DISASTER RECOVERY PLAN**

- Shred-it has policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain protected personal information.

- Shred-it requires each location to maintain a contingency plan/disaster recovery plan for implementation in the event of an emergency, disaster, or other occurrence (i.e. fire, vandalism, system failure, or natural disaster). All facilities are required to update and test their Emergency Action Plans annually.
- Shred-it maintains a contingency plan for responding to system emergencies involving systems that contain protected personal information. Shred-it performs periodic backups of data, has facilities for continuing critical operations in the event of an emergency, and has disaster recovery procedures in place for such systems.