

**REQUEST FOR PROPOSAL #R10-180 FOR:
OFFICE & CLASSROOM COLLABORATION
SOLUTIONS**

January 28, 2022

Section Two :
Proposal Submission, Questionnaire and
Required Forms

Proposal Form Checklist3

PROPOSAL FORM 1: ATTACHMENT B – PRICING.....4

PROPOSAL FORM 2: QUESTIONNAIRE & EVALUATION CRITERIA.....5

PROPOSAL FORM 3: CERTIFICATIONS AND LICENSES 23

PROPOSAL FORM 4: CLEAN AIR WATER ACT.....24

PROPOSAL FORM 5: DEBARMENT NOTICE 25

PROPOSAL FORM 6: LOBBYING CERTIFICATION.....26

PROPOSAL FORM 7: CONTRACTOR CERTIFICATION REQUIREMENTS.....27

PROPOSAL FORM 8: ANTITRUST CERTIFICATION STATEMENTS28

PROPOSAL FORM 9: IMPLEMENTATION OF HOUSE BILL 1295.....29

PROPOSAL FORM 10: BOYCOTT CERTIFICATION AND TERRORIST STATE CERTIFICATION.....30

PROPOSAL FORM 11: RESIDENT CERTIFICATION31

PROPOSAL FORM 12: FEDERAL FUNDS CERIFICATION FORM..... 32

PROPOSAL FORM 13: ADDITIONAL ARIZONA CONTRACTOR REQUIREMENTS.....38

PROPOSAL FORM 14: OWNERSHIP DISCLOSURE FORM (N.J.S. 52:25-24.2).....40

PROPOSAL FORM 15: NON-COLLUSION AFFIDAVIT 41

PROPOSAL FORM 16: AFFIRMATIVE ACTION AFFIDAVIT (P.L. 1975, C.127).....42

PROPOSAL FORM 17: C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM.....45

PROPOSAL FORM 18: STOCKHOLDER DISCLOSURE CERTIFICATION50

PROPOSAL FORM 19: GENERAL TERMS AND CONDITIONS ACCEPTANCE FORM.....51

PROPOSAL FORM 20: EQUALIS GROUP ADMINISTRATION AGREEMENT..... 52

PROPOSAL FORM 21: OPEN RECORDS POLICY ACKNOWLEDGEMENT AND ACCEPTANCE..... 53

PROPOSAL FORM 22: VENDOR CONTRACT AND SIGNATURE FORM.....54

Proposal Form Checklist

The following documents must be submitted with the Proposal

The below documents can be found in Section 2; Proposal Submission and Required Bid Forms and must be submitted with the proposal. Please note Proposal Form 1 is a separate attachment (attachment B)

PROPOSAL PRICING: Attachment B is provided separately in a Microsoft Excel file and is required to complete your price proposal.

PROPOSAL FORM 1: ATTACHMENT B - PRICING

QUESTIONNAIRE & EVALUATION CRITERIA :

PROPOSAL FORM 2: QUESTIONNAIRE & EVALUATION CRITERIA

OTHER REQUIRED PROPOSAL FORMS:

PROPOSAL FORM 3: CERTIFICATIONS AND LICENSES

PROPOSAL FORM 4: CLEAN AIR AND WATER ACT

PROPOSAL FORM 5: DEBARMENT NOTICE

PROPOSAL FORM 6: LOBBYING CERTIFICATION

PROPOSAL FORM 7: CONTRACTOR CERTIFICATION REQUIREMENTS

PROPOSAL FORM 8: ANTITRUST CERTIFICATION STATEMENTS

PROPOSAL FORM 9: IMPLEMENTATION OF HOUSE BILL 1295

PROPOSAL FORM 10: BOYCOTT CERTIFICATION AND TERRORIST STATE CERTIFICATION

PROPOSAL FORM 11: RESIDENT CERTIFICATION

PROPOSAL FORM 12: FEDERAL FUNDS CERTIFICATION FORM

PROPOSAL FORM 13: ADDITIONAL ARIZONA CONTRACTOR REQUIREMENTS

PROPOSAL FORM 14: OWNERSHIP DISCLOSURE FORM (N.J.S. 52:25 -24.2)

PROPOSAL FORM 15: NON-COLLUSION AFFIDAVIT

PROPOSAL FORM 16: AFFIRMATIVE ACTION AFFIDAVIT (P.L. 1975, C.127)

PROPOSAL FORM 17: C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

PROPOSAL FORM 18: STOCKHOLDER DISCLOSURE CERTIFICATION

PROPOSAL FORM 19: GENERAL TERMS AND CONDITIONS ACCEPTANCE FORM

PROPOSAL FORM 20: EQUALIS GROUP ADMINISTRATION AGREEMENT

PROPOSAL FORM 21: OPEN RECORDS POLICY ACKNOWLEDGEMENT AND ACCEPTANCE

PROPOSAL FORM 22: VENDOR CONTRACT AND SIGNATURE FORM

(The rest of this page is intentionally left blank)

PROPOSAL FORM 1: ATTACHMENT B – PRICING

Pricing should be entered in the attachment B Excel form provided in this RFP packet. Please reference Section 1, Part B, Instructions to Proposers, for more information on how to complete pricing.

(The rest of this page is intentionally left blank)

PROPOSAL FORM 2: QUESTIONNAIRE & EVALUATION CRITERIA

Instructions:

Respondents should incorporate their questionnaire responses directly into the green cells below. Failure to provide responses in this format may result in the proposal being deemed as non-responsive at the sole discretion of Region 10.

Respondents may incorporate additional documents as part of their response which may be utilized by Region 10 as part of the evaluation. Additional documents must be consolidated as part of this Section 2 at the end of your response.

Region 10 has associated the evaluation criteria with the question that most closely aligns with that respective evaluation criteria. Region 10 reserves the right at its sole discretion to base its evaluation and specific evaluation criteria on any part of the respondent’s proposal.

Evaluation Criteria	Question	Answer
Basic Information		
	<i>What is your company's official registered name?</i>	One Diversified, LLC
	<i>What is the mailing address of your company's headquarters?</i>	37 Market Street Kenilworth, New Jersey 07033
	<i>Who is the main contact for any questions and notifications concerning this RFP response, including notification of award? Provide name, title, email address, and phone number.</i>	Tracie Lee, Business Development Representative tlee@onediversified.com (770) 855-7022
Products/Pricing (30 Points)		
Coverage of products and services	No answer is required. Region 10 will utilize your overall response and the products/services provided in Attachment B to make this determination	
Ability of offered products and services to meet	No answer is required. Region 10 will utilize your overall response and the products/services provided in Attachment B to make this determination	

the needs requested in the scope		
Pricing for all available products and services, including warranties if applicable	<i>Does the respondent agree to offer all future product and services at prices that are proportionate to contract pricing offered herein?</i>	Yes.
	<i>Does pricing submitted include the required administrative fee?</i>	Yes.
	<i>Do you offer any other promotions or incentives for customers? If yes, please describe.</i>	Yes, our manufacturer partners offer special pricing incentives for registered projects, large purchases, and special one-time purchase incentives. These incentives will be passed on to members.
Ability of Customers to verify that they received contract pricing	<i>Were all products/lines/services and pricing being made available under this contract provided in the attachment B and/or Appendix B, pricing sections?</i>	Yes.
	<i>Outline your pricing strategy provided in Attachment B. If utilizing a list price, please indicate where agencies can find the list and your methodology for determining that list price.</i>	We are offering a discount from Manufacturers Suggested Retail Price (MSRP). MSRP price sheets are made available to perspective customers and dealers by the manufacturers. Diversified would be happy to assist with MSRP price sheet request by members.
Payment methods	<i>Define your invoicing process and methods of payments you will accept. Please include the overall process for agencies to make payments</i>	Each member's credit worthiness will be determined upon account set-up. Standard terms for approved members would be as follows. Purchases less than \$25,000.00 are invoiced upon completion or delivery with standard net thirty (30) terms. Purchases over \$25,000.00 50% deposit, 30% progress payment, 20% final payment. Terms can be negotiated prior to order placement based on member purchasing policies and credit worthiness.

Other factors relevant to this section as submitted by the Respondent	No answer is required. Region 10 will utilize your overall response and the products/services provided in Attachment B to make this determination
---	---

Performance Capability (25 Points)

Ability to deliver, design, and install products and services	<p><i>Please outline your products and services being offered, including the features and benefits and how they address the scope being requested herein. Please be specific; your answer to this question, along with products/services provided in your pricing file will be used to evaluate your offering.</i></p>	<p>Diversified was formed in 1993 as a full-service systems and media technology integration company, originally addressing the technical needs of the broadcast, audio-visual, IT and RF market segments. However, as the market needs continued to grow and evolve, so did Diversified’s service offerings. Over the years, the company made a series of strategic investments and acquisitions that not only expanded their portfolio of expertise but also extended their geographic footprint to better serve a growing client base.</p> <p>With the enhanced capabilities, Diversified emerged as an industry leading technology solutions provider delivering innovative digital media, collaborative, broadcasting, electronic security, and OTT solutions to a global clientele across a wide array of markets including financial, media & entertainment, enterprise, energy, higher education, technology, healthcare, hospitality, government, and more. As an engineering-centric organization, our specialized teams of technical experts partner with clients to design custom solutions that enhance their operations, increase productivity, and help drive ROI.</p> <p>Today Diversified has 55+ offices serving Fortune 500 clients around the world and is widely recognized for thought leadership and strategic enterprise implementation. From initial design consultation to deployment to managed services, Diversified is a trusted technology partner. As one of the largest system integration firms in the country, Diversified enjoys direct buying relationships with most of the leading broadcast, AV and security manufacturers. In addition to the following list manufactures included in our response Diversified will provide a system integration services that can encompass the project life cycle from start to completion.</p>
---	--	---

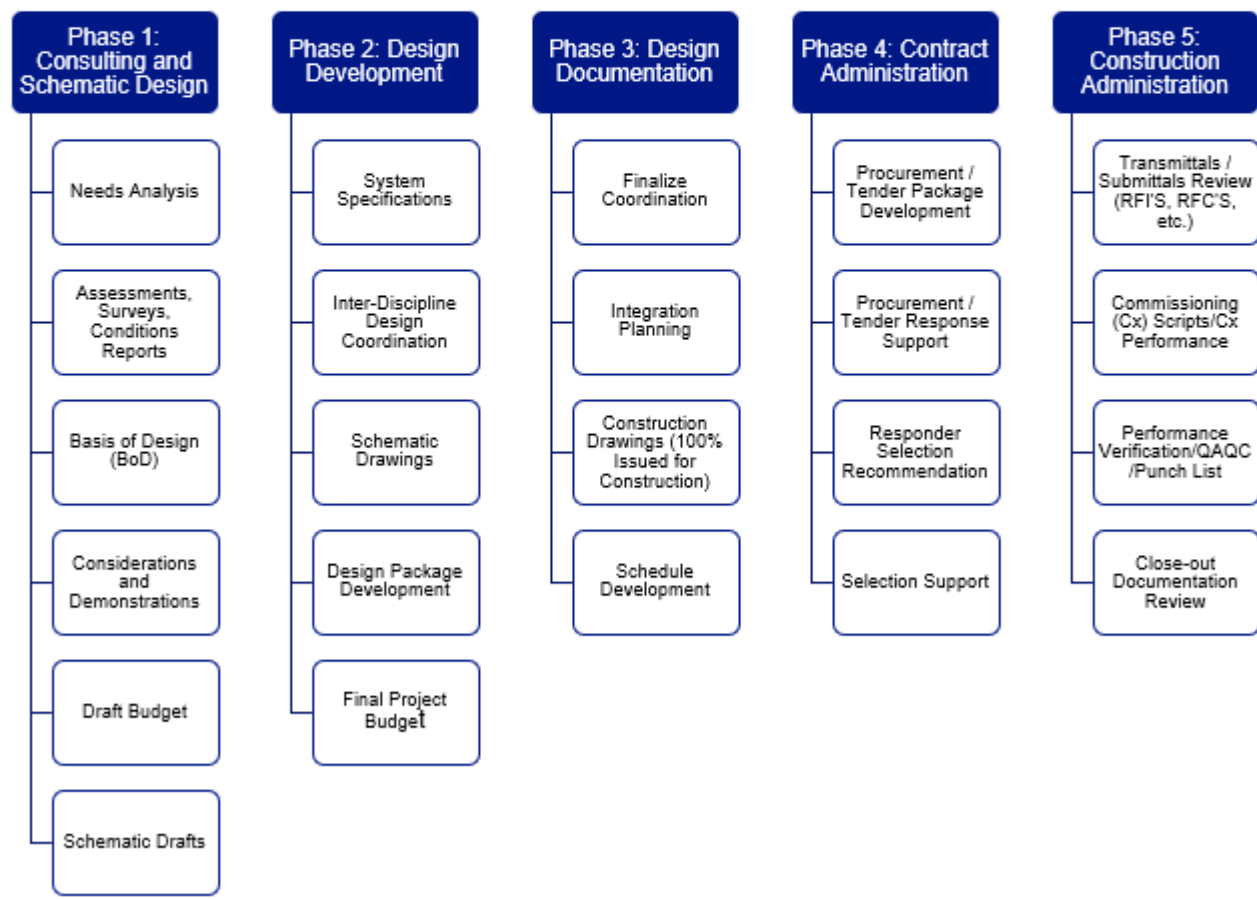
Please outline your design services and how you work with clients to develop a collaboration space design.

TECHNOLOGIES DESIGN SERVICES PROCESS (AVE)

Diversified's design services management approach ensures schedule adhesion, effective communication, flexible methods for sharing deliverables documentation.

Prior to moving on to a subsequent phase, a client will review and approve submittals from the current phase.

A multi-phase approach verifies the design is progressing toward the intended result and is critical to ensure the final design meets the functional expectations.



	<p><i>States Covered - Respondent must indicate any and all states or geographies where products and services are being offered. If your services are limited to a certain area, please be specific on the area your services are provided.</i></p>	<p>As our name suggests, we are truly diversified, with a deep understanding of the multi-faceted and interconnected needs of facilities technology. Diversified has more than 25 years of experience providing consulting, design, procurement, integration, project management and managed support services. Diversified is a national and global technical solutions provider, serving all 50 states, with headquarters in Kenilworth, NJ and fabrication and operation facilities in more than 55 locations around the globe.</p>
	<p><i>List the number and location of offices, or service centers for all states being proposed in solicitation</i></p>	<ol style="list-style-type: none"> 1.) Kenilworth, New Jersey (headquarters) 2.) Norcross, Georgia 3.) Orlando, Florida 4.) Pensacola, Florida 5.) Birmingham, Alabama 6.) Pleasanton, California 7.) Anaheim, California 8.) Santa Clara, California 9.) San Diego, California 10.) San Francisco, California 11.) Bentonville, Arkansas 12.) Chicago, Illinois 13.) Columbia, Maryland 14.) Boston, Massachusetts 15.) Indianapolis, Indiana 16.) Rochester, New York 17.) Charlotte, North Carolina 18.) Raleigh, North Carolina 19.) Portland, Oregon 20.) Philadelphia, Pennsylvania 21.) Memphis, Tennessee 22.) Nashville, Tennessee 23.) Austin, Texas 24.) Dallas, Texas 25.) Houston, Texas 26.) Sterling, Virginia 27.) Seattle, Washington
<p>History of meeting the delivery, installation, and</p>	<p><i>Outline the typical installation process, anticipated timelines and any ongoing</i></p>	<p>Build Project Approach</p>

maintenance timelines

maintenance that may be required.

Diversified follows a comprehensive procedure to ensure accurate and timely delivery of large-scale integrated technology systems. The procedure, which is divided into 9 distinct phases, places a strong emphasis on verification and preparation as these tasks are essential to ensuring a successful outcome.

Procedural Phase Descriptions:



1. Design Review = the submittal and/or review process composed of reviewing project scope and verifying that the components and systems to be installed, and the methods/details of installation, are consistent with the design intent and systems specifications and functionality.

2. Staging and Site-Preparation = staging and site-preparation are two distinct and concurrent processes. Staging is the process of completing an in-house set of tasks; interconnect, configure, update, program and test as many system capabilities/components as appropriate, in an attempt to discover early issues and minimize on-site time. Site-preparation is the process of performing site conditions assessments and surveys, attending construction and trades coordination meetings, and completing preliminary rough-in work. Both processes are crucial to delivering quality systems on time and ready for use.

3. Installation = the main installation effort; encompasses equipment delivery, passive infrastructure installation (cabling and racks and contracted raceways), active infrastructure installation (equipment hardware), terminations and testing reports production.

4. Device Configuration = the process of adjusting initial device settings required for proper operation of each component. Typically includes level settings, operational modes, addressing, EDID settings, etc. May include initial software file upload/config as needed.

		<p>5. Self-verification Testing = the process of testing each analysis system/tool to ensure it can accurately measure the intended system parameter.</p> <p>6. Systems Pre-verification Testing = the process of verifying, prior to optimization, that the components have been installed properly, devices are operating properly, and the environmental conditions are appropriate for the installed systems and components.</p> <p>7. Optimization and Software = the process of loading software files and performing device configuration, calibration, alignment and adjustments to optimize the performance of the system and components for the particular parameters and stated design objectives.</p> <p>8. Systems Post-verification Testing = the process of verifying, following optimization, the performance of the systems against the stated design objectives.</p> <p>9. Training and Acceptance = the final project stage, involving close-out document delivery, on-site training, and owner acceptance of the provided systems and services.</p>
Response to emergency orders and maintenance repair/requests	<i>Describe the type of emergency orders or requests your organization typically receives and how you respond to those requests</i>	Diversified has the ability to quickly respond to non-standard requests. We closely communicate with customers to inquire about timelines. If needed, depending on the size and scope, we can respond to a quote request within 24-48 hours. Depending on availability, product orders can be expedited with overnight delivery. Extra costs may incur to the customer. Upon expedited shipment, tracking information can be provided. Emergency site visits can be scheduled depending on the scope of the situation, travel distance and availability of technicians. DOA or Defective equipment can be expedited based upon the manufacturer warranty program. Diversify will respond to all DOA equipment requests within 24 hours. Customer communication and response times are important to our on-going partnership. Diversified will respond quickly to all urgent matters.
Return and restocking policy and applicable fees	<i>Please describe your company's return and restocking policy, including any commitments necessary for services and fees for agencies to end services early.</i>	Diversified follows the return policies of each manufacturer. On behalf of the customer, Diversified will always try to negotiate and or eliminate restock fees. For product purchases, Diversified has a dedicated RMA team. Our RMA team will acknowledge and respond within 24 hours of a request for return. Equipment warranties are determined by the manufacturer. Diversified can work with customers to provide extended warranties or services programs to maintain standards and up-time.

Customer service/problem resolution	<i>Describe your company's Customer Service Department (hours of operation, how you resolve issues, number of service centers, etc.).</i>	<ol style="list-style-type: none"> 1. The Diversified Global Service Center will provide unlimited Help Desk Tier 1 phone and email response during normal working hours 8:00 AM-5:00 PM Monday-Friday (local time) by the Diversified Global Service Center. 2. Unlimited Help Desk Tier 2 technical support will be provided via phone and email during normal working hours 8:00 AM-5:00 PM Monday-Friday (local time) by the Diversified Global Service Center. 3. Service requests received by phone or email will be responded to within fifteen (15) minutes from receipt of the emailed or phoned request. 4. If a reported Service issue is not resolved by the Help Desk, an on-site visit will be scheduled as necessary at an agreed upon time within standard business hours (8:00 AM-5:00 PM Monday-Friday local time zone). The Client shall give Diversified access to all covered rooms and/or equipment at the agreed scheduled time.
-------------------------------------	---	---

Financial condition of vendor	<i>Demonstrate your financial strength and stability with meaningful data. This could include, but is not limited to, such items as financial statements, SEC filings, credit & bond ratings, letters of credit, and detailed reference letters</i>	<p style="text-align: center;">Corporate Profile</p> <table border="1" style="width: 100%;"> <tr> <td>Legal Entity Name:</td> <td>Distinct Holdings, Inc.</td> </tr> <tr> <td>Type of organization:</td> <td>Corporation</td> </tr> <tr> <td>Business Name:</td> <td>One Diversified, LLC (dba Diversified)</td> </tr> <tr> <td>Corporate Headquarters</td> <td>37 Market Street Kenilworth, New Jersey 07033 (908) 245-4833 (908) 245-0011 (Fax)</td> </tr> <tr> <td>Website:</td> <td>www.diversifiedus.com</td> </tr> <tr> <td>Corporate Case Studies:</td> <td>https://onediversified.com/projects/</td> </tr> <tr> <td>Year Established:</td> <td>1993</td> </tr> <tr> <td>Number of Employees</td> <td>2400</td> </tr> <tr> <td>Federal Tax ID:</td> <td>42-1617340</td> </tr> <tr> <td>DUNS:</td> <td>14-414-5443</td> </tr> <tr> <td>DUNS Rating:</td> <td>4A2</td> </tr> <tr> <td>Cage Code:</td> <td>3T0D9</td> </tr> </table>	Legal Entity Name:	Distinct Holdings, Inc.	Type of organization:	Corporation	Business Name:	One Diversified, LLC (dba Diversified)	Corporate Headquarters	37 Market Street Kenilworth, New Jersey 07033 (908) 245-4833 (908) 245-0011 (Fax)	Website:	www.diversifiedus.com	Corporate Case Studies:	https://onediversified.com/projects/	Year Established:	1993	Number of Employees	2400	Federal Tax ID:	42-1617340	DUNS:	14-414-5443	DUNS Rating:	4A2	Cage Code:	3T0D9
Legal Entity Name:	Distinct Holdings, Inc.																									
Type of organization:	Corporation																									
Business Name:	One Diversified, LLC (dba Diversified)																									
Corporate Headquarters	37 Market Street Kenilworth, New Jersey 07033 (908) 245-4833 (908) 245-0011 (Fax)																									
Website:	www.diversifiedus.com																									
Corporate Case Studies:	https://onediversified.com/projects/																									
Year Established:	1993																									
Number of Employees	2400																									
Federal Tax ID:	42-1617340																									
DUNS:	14-414-5443																									
DUNS Rating:	4A2																									
Cage Code:	3T0D9																									

		NAICS:	238210, 334112, 334220, 334290, 334310, 334419, 541330, 541511, 541512, 541519, 541618, 541990, 811213										
		Contractor License	LOCATION LICENSURE										
		3-Year Revenue History:	<table border="0"> <tr> <td>2021</td> <td>\$ 1,000,000,000.00</td> </tr> <tr> <td>2020</td> <td>\$ 900,000,000.</td> </tr> <tr> <td>2019</td> <td>\$ 950,000,000.</td> </tr> <tr> <td>2018</td> <td>\$ 750,000,000.</td> </tr> <tr> <td>2017</td> <td>\$ 650,000,000.</td> </tr> </table> <p>Note: Diversified can provide audited financial reports, as required, upon completion of Diversified's Financial Confidentiality Agreement.</p>	2021	\$ 1,000,000,000.00	2020	\$ 900,000,000.	2019	\$ 950,000,000.	2018	\$ 750,000,000.	2017	\$ 650,000,000.
2021	\$ 1,000,000,000.00												
2020	\$ 900,000,000.												
2019	\$ 950,000,000.												
2018	\$ 750,000,000.												
2017	\$ 650,000,000.												
	What was your annual sales volume over last three (3) years?		<table border="0"> <tr> <td>2021</td> <td>\$ 1,000,000,000.00</td> </tr> <tr> <td>2020</td> <td>\$ 900,000,000.</td> </tr> <tr> <td>2019</td> <td>\$ 950,000,000.</td> </tr> </table>	2021	\$ 1,000,000,000.00	2020	\$ 900,000,000.	2019	\$ 950,000,000.				
2021	\$ 1,000,000,000.00												
2020	\$ 900,000,000.												
2019	\$ 950,000,000.												
Capabilities related to ordering, estimation, reporting, and overall website ease-of-use	Provide relevant information regarding your estimation, ordering, and overall implementation.	Diversified has dedicated teams to process all orders with accuracy and efficiency. Our ordering systems are designed to meet client deadlines and delivery on accuracy. Diversified has a tracking and reporting system that can be customized for contracts. The Diversified website highlights industry solutions, case studies, services, specialties, and insights. We do not offer E-Commerce through our website.											
Training & Implementation	Describe training or support you provide to help agencies understand how to utilize the spaces and technology equipment being installed.	1. Diversified includes one on-site demonstration and training for system hardware and software with the Customer End-User personnel. If additional sessions and/or time are required, Diversified will provide additional pricing as requested.											
Security protocols	Describe security protocols in place, including cybersecurity and the safe transmission of data	Please see attachments.											
Integration with other platforms	Describe any integrations your organization can	Diversified is a technology solution provider. We provide solutions that work across the breath of customer's technology footprints.											

	<i>provide with other platforms or systems.</i>	
Other factors relevant to this section as submitted by the Respondent	<i>Describe the capacity of your company to provide management reports, i.e. consolidated billing by location, time and attendance reports, etc. for each eligible agency</i>	Diversified has the ability to provide management reports to eligible agencies. Reporting can include billing statements and time and attendance reporting as required with advance notice from member agencies.

Provide your safety record, safety rating, EMR and worker's compensation rate where available.

Historical OSHA Data

Corporate Statistics and Rates	2020	2019	2018	2017	2016	2015
Total Employee Exposure Hours	3,178,896	3,885,272	3,225,250	2,364,769	1,087,101	919,360
Average Total Number of Employees	1,686	1,902	1,786	1,137	523	442
Total Recordable Injury Rate (TRIR)	1.07	0.86	1.48	1.86	1.10	2.61
Days Away, Restricted or Transferred Rate (DARTR)	0.50	0.36	0.43	0.34	0.60	1.10
Days Away Rate (DAR)	0.25	0.26	0.12	0.34	0.60	1.10

OSHA Form 300A Data

Total Number of all Recordable Cases	17	17	24	22	6	12
Number of Medical Treatment Only Cases	9	10	17	18	3	7

Lost Workday Statistics

Number of Cases	4	5	2	4	1	2
Number of Lost Workdays	269	246	19	46	8	82

Restricted or Transferred Statistics

Number of Cases	4	2	5	0	2	3
Number of Restricted Workdays	17	17	78	110	26	9

Fatalities Statistics

Number of Cases	0	0	0	0	0	0
Number of Fatalities	0	0	0	0	0	0

Qualification and Experience (25 Points)

Respondent reputation in the marketplace

Provide a link to your company's website

www.diversifiedus.com

Please provide a brief history of your company, including the year it was established.

Diversified was formed in 1993 as a full-service systems and media technology integration company, originally addressing the technical needs of the broadcast, audio-visual, IT and RF market segments. However, as the market needs continued to grow and evolve, so did Diversified's service offerings. Over the years, the company made a series of strategic investments and acquisitions that not only expanded their portfolio of expertise but also extended their geographic footprint to better serve a growing client base.

Past relationship with Region 10 ESC and/or Region 10 ESC members	<i>Have you worked with Region 10 in the past? If so, what was the timeframe for that work?</i>	No.
Experience and qualification of key employees	<i>Please provide contact information and resumes for the person(s) who will be responsible for the following areas. Region 10 requests contacts to cover the following: * Executive Support * Account Manager * Contract Manager * Marketing * Billing, reporting & Accounts Payable</i>	David Berndt, Vice President (Executive Sponsor) dberndt@diversifiedus.com (615) 294-6699 Tracie L. Lee, Business Development Representative (Account Manager & Contract Manager) tlee@onediversified.com (770) 855-7022 Anna DeMuro, Supervisor Accounts Payable andemuro@diversifiedus.com (770) 441-5218 Rina Ebert, Chief Marketing Officer rebert@onediversified.com (917) 570-2559
Past experience working with the public sector	<i>What are your overall public sector sales, excluding Federal Government, for last three (3) years?</i>	Diversified has overall public sector sales in excess of \$50M over the last three years.
	<i>What is your strategy to increase market share in the public sector?</i>	Diversified has dedicated teams to process all orders with accuracy and efficiency. Our ordering systems are designed to meet client deadlines and delivery on accuracy. Diversified has a tracking and reporting system that can be customized for contracts. The Diversified website highlights industry solutions, case studies, services, specialties and insights. We do not offer E-commerce through our website.
Past litigation, bankruptcy, reorganization, state investigations of entity or current officers and directors	<i>Provide information regarding whether your firm, either presently or in the past, has been involved in any litigation, bankruptcy, or reorganization.</i>	None.
Minimum of 5 public sector customer references relating to the products and services within this RFP	<i>Provide a minimum of five (5) customer references for product and/or services of similar scope dating within the past 3 years. Please try to provide references for K12, Higher</i>	References UC Merced University of California Merced Jodon Bellofatto Office of Information Technology Enhanced Spaces, Lead Analyst 5200 North Lake Road, Merced Ca 95343 Phone: 209-228-4400 Email jbellofatto@ucmerced.edu UC Davis University of California Davis Health System

	<p><i>Education, City/County and State entities. Provide the entity; contact name & title; city & state; phone number; years serviced; description of services; and annual volume</i></p>	<p>Chris Floyd AV-IT Engineer 4 - Supervisor Education Building 4610 X St. Suite 1206 Sacramento, CA. 95817 email: crfloyd@ucdavis.edu phone 916.734.4550</p> <p>University of Tennessee Michael T. Berger 865-974-0599 mberger@utk.edu 0%-45% based on Manufacturer</p> <p>Michael T. Berger IT Manager, Office of Information Technology Communications: Engineering Services Suite 61 Communications Building 1345 Circle Park Drive Knoxville, TN 37996-0311 Phone: 865-974-0599 Cell: 865-806-0782</p> <p>University of Memphis Beau Staples 901.678.3535 bstaples@memphis.edu 0%-45% based on Manufacturer</p> <p>Beau Staples Local Tech Support Provider III Smart Tech Services ITS Desktop and Smart Technologies Support 107 Admin Building Memphis, TN 38152 901.678.3535 email: bstaples@memphis.edu</p> <p>Shoreline Community College Randy Gottfried 206-546-5831 rgottfried@shoreline.edu 0%-45% based on Manufacturer</p> <p>Randy Gottfried Director, Classroom Support Shoreline Community College Shoreline, WA 98133 rgottfried@shoreline.edu 206-546-5831</p> <p><u>Butte College</u> Scott Gordon Butte College Multimedia Electronic Engineer, Senior 530-879-4074 GordonSc@butte.edu</p>
--	---	--

<p>Certifications in the Industry</p>	<p><i>Provide a copy of all current licenses, registrations and certifications issued by federal, state and local agencies, and any other licenses, registrations or certifications from any other governmental entity with jurisdiction, allowing Respondent to perform the covered services including, but not limited to licenses, registrations or certifications. M/WBE, HUB, DVBE, small and disadvantaged business certifications and other diverse business certifications, as well as manufacturer certifications for sales and service must be included if applicable</i></p>	<p>Diversified is licensed to sell in all fifty states. Diversified also has applicable licenses to perform low-voltage installation in all states and jurisdictions that we have physical offices in and required by law.</p> <p>Diversified is a certified reseller for all manufacturers pricing is being provided for.</p> <p>Business licenses, contractor licenses and manufacturer certifications will be made available to interested members as needed. We have provided a sample of licenses that we hold.</p>
<p>Company profile and capabilities</p>	<p><i>What best describes your position in the distribution channel? (Manufacturer, Authorized Distributor, Value-Add Reseller, Other</i></p>	<p>Diversified is a Value-Added Reseller and System Integrator.</p>
<p>Other factors relevant to this section as submitted by the Respondent</p>	<p><i>If your company is a privately held organization, please indicate if the company is owned or operated by anyone who has been convicted of a felony.</i></p>	<p>No Executives with One Diversified, LLC have been convicted of a felony.</p>

	<p><i>If yes, a detailed explanation of the names and conviction is required.</i></p>	
<p>Provide a copy of all current licenses, registrations and certifications issued by federal, state and local agencies, and any other licenses, registrations or certifications from any other governmental entity with jurisdiction, allowing Respondent to perform the covered services. These will be provided in the space provided in Form 6. No answer is required here.</p>		

MWBE Status and/or Program Capabilities (10 Points)

<p>MWBE status, subcontractor plan, and/or joint venture program</p>	<p><i>Please indicate whether you hold any diversity certifications, including, but not limited to MWBE, SBE, DBE, DVBE, HUB, or HUBZone</i></p>	<p>Diversified partners with <i>MWBE, SBE, DBE, DVBE, HUB, or HUBZone</i> on a case-by-case basis.</p>
	<p><i>Do you currently have a diversity program in place, such as a Mentor Protégé Program or subcontractor program? If you have a diversity program, please describe it and indicate whether you plan to offer your program or partnership through Equalis Group?</i></p>	<p>Diversified is an Equal Opportunity Employer fully committed to providing and engaging and fulfilling environment. We are dedicated to providing equality of opportunity in all areas of employment and business including, but not limited to gender, race, nationality, age, disability, sexual orientation or religion.</p> <p style="text-align: center;">Diversity. Equity. Inclusion.</p> <p>We've all heard these words before, perhaps more frequently of recent than we have in a while. These words recognize systemic differences in experience. Experiences that have likely had a resounding effect on many of our lives. These words also represent an opportunity for betterment – an opportunity Diversified is committed to realizing to its full potential for the advancement of our employees internally as well as the communities we serve, externally.</p> <p style="text-align: center;">Our Commitment to Better</p> <p>Diversified highlight's employee commitment in an annual affirmation and has developed internal diversity, equity and inclusion (DEI) as well as supplier diversity programs to extend them.</p> <p style="text-align: center;">All employees participate in <i>Respect in the Workplace</i> training to create awareness and establish consistent expectations across the organization.</p> <p style="text-align: center;">Three of the seven individuals on our executive leadership team are members of underrepresented groups and thus form the basis of our "Lead by Example" philosophy.</p> <p style="text-align: center;">They ensure that Diversified's PeopleTeam monitors relevant indicators of the company's progress on DEI issues. Policies are annually reviewed and assistance to managers and employees on DEI issues is provided.</p>

Please attach any certifications you have as part of your response to Form 6.

<p>Good faith efforts to involve MWBE subcontractors in response</p>	<p><i>Did your company contact MWBEs or minority chambers of commerce by telephone, written correspondence, or trade associations at least one week before the due date of this RFP to provide information relevant to this opportunity and to determine whether any MWBEs were interested in subcontracting and/or joint ventures?</i></p>	<p>No. Diversified has on-going relationships with MWBE's, and HUB's. We typically engage with these partners when projects develop that require their participation.</p>
<p>Demonstrated ongoing MWBE program</p>	<p><i>Outline your subcontractor strategy and efforts your organization takes to include MWBE subcontractors in future work, including but not limited to efforts to reach out to individual MWBE businesses, minority chambers of commerce, and other minority business and trade associations.</i></p>	<p>Diversified has on-going partnerships with MWBE's and HUB's that support MWBE and HUB requirements for contracted business.</p>
<p>Commitment to Service Equalis Group Members (10 Points)</p>		
<p>Marketing plan, capability, and commitment</p>	<p><i>Detail how your organization plans to market and promote this contract upon award, including how this contract will fit into your organization's current go-to-market strategy in the public sector.</i></p>	<p>If awarded, Diversified may choose to add this contract to its existing contracts and programs landing page for website visitors to clearly identify Diversified as a qualified provider. Upon addition to this page, Diversified would promote the contract via press release, social media and targeted email campaigns to reach new and existing customers within the eligible markets.</p> <p>Additional sales collateral may be developed including, but not limited to, presentation slides and one sheets. This collateral would be used by our sales teams to better educate existing clients and prospects, as well as our marketing teams in our account-based marketing efforts.</p> <p>Once projects are completed that leverage the contract, Diversified may pursue additional project related promotions--with client approval--including, but not limited to, case studies, press releases, video testimonials and award entries that may reference the contract benefits provided.</p>

	<p><i>Detail how your organization will train your sales force and customer service representatives on this contract to ensure that they can competently and consistently present the contract to public agency customers and answer any questions they might have concerning it.</i></p>	<p>In order to properly equip the company's sales team on how to best promote the contract, Diversified will develop and provide the necessary training resources including, but not limited to, email scripts and presentation materials in addition to other customer facing collateral. Targeted marketing to existing customers through our account-based marketing program will further help to promote the contract and provide the foundation for sales engagements.</p> <p>During Diversified's monthly sales meetings, sales leadership will provide additional insight on the contract as well as highlight success stories from high performing sales team members to further encourage contract promotion and successful tactics with existing clients and prospects.</p>
	<p><i>Acknowledge that your organization agrees to provide its company logo(s) to Region 10 ESC and Equalis Group and agrees to provide permission for reproduction of such logo in marketing communications and promotions</i></p>	<p>Yes.</p>
<p>Ability to manage a cooperative contract</p>	<p><i>Describe the capacity of your company to report monthly sales through this agreement to Equalis Group.</i></p>	<p>We will provide monthly sales to Equalis Group as stated and agreed to in the agreement (contract).</p>
	<p><i>Identify any contracts with other cooperative or government group purchasing organizations of which your company is currently a part of:</i></p>	<p>The Interlocal Purchasing System (TIPS) State of Georgia Alabama Community College System (ACCS) University of Wisconsin The University of Washington State of Washington University of North Carolina North Carolina State University University of Kentucky</p>

		<p>Ontario Education Collaborative Marketplace Middle Tennessee State University OMNIA Partners Group (OMNIA) Mississippi Department of Information Technology Services Organization for Educational Technology and Curriculum (OETC) University of California</p>
<p>Commitment to supporting agencies to utilize the contract</p>	<p><i>If awarded a contract, how would you approach agencies in regards to this contract? Please indicate how this would work for both new customers to your organization, as well as existing.</i></p>	<p>If awarded the contract, Diversified would leverage social media as well as targeted email marketing to reach both existing customers and new prospects. As part of Diversified’s social media strategy, we not only post to our main page but also encourage our sales social media power users to promote directly to their pages to further enhance the exposure.</p> <p>Targeted marketing to existing customers through our account-based marketing program will further help to promote the contract and encourage them to contact their Diversified representative to learn more. There would also be the option to potentially purchase market specific email lists to reach additional prospects.</p>
<p>Other factors relevant to this section as submitted by the Respondent</p>	<p><i>Provide the number of sales representatives which will work on this contract and where the sales representatives are located.</i></p>	<p>Diversified has a nation-wide presence with thirty sales representatives on the team. If awarded this contract Equalis Group will be an additional contract vehicle that the Higher Education/Public sector team members could utilize with current and future customers.</p>

PROPOSAL FORM 3: CERTIFICATIONS AND LICENSES

Provide a copy of all current licenses, registrations and certifications issued by federal, state and local agencies, and any other licenses, registrations or certifications from any other governmental entity with jurisdiction, allowing Respondent to perform the covered services including, but not limited to licenses, registrations or certifications. M/WBE, HUB, DVBE, small and disadvantaged business certifications and other diverse business certifications, as well as manufacturer certifications for sales and service must be included if applicable. (PLEASE SEE ATTACHMENT.)

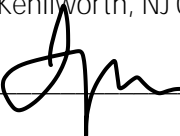
PROPOSAL FORM 4: CLEAN AIR WATER ACT

I, the Vendor, am in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the Enforcement.

Potential Vendor: One Diversified, LLC

Title of Authorized Representative: Tracie Lee, Business Development Representative

Mailing Address: 37 Market Street Kenilworth, NJ 07033

Signature: Tracie L. Lee 

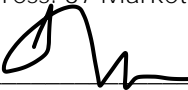
PROPOSAL FORM 5: DEBARMENT NOTICE

I, the Vendor, certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, "Debarment and Suspension", as described in the Federal Register and Rules and Regulations.

Potential Vendor: One Diversified, LLC

Title of Authorized Representative: Tracie Lee, Business Development Representative

Mailing Address: 37 Market Street Kenilworth, NJ 07033

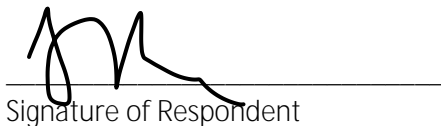
Signature:  _____

PROPOSAL FORM 6: 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 \$10,000 and not more than \$100,000 for each such failure.

The undersigned certifies, to the best of his/her knowledge and belief, 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 \$100,000 in Federal funds at all appropriate tiers and that all sub-recipients shall certify and disclose accordingly.



Signature of Respondent

March 9, 2022
Date

PROPOSAL FORM 7: CONTRACTOR CERTIFICATION REQUIREMENTS

Contractor's Employment Eligibility

By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statutes of the states it will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The Respondent complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.


Contractor shall comply with governing board policy of the Region 10 ESC Participating entities in which work is being performed.

Fingerprint & Criminal Background Checks

If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

The Respondent shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed.



Signature of Respondent

March 9, 2022
Date

PROPOSAL FORM 8: ANTITRUST CERTIFICATION STATEMENTS
(Tex. Government Code § 2155.005)

I affirm under penalty of perjury of the laws of the State of Texas that:

- (1) I am duly authorized to execute this contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;
- (2) In connection with this proposal, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;
- (3) In connection with this proposal, neither I nor any representative of the Company has violated any federal antitrust law; and
- (4) Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this proposal to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.


VENDOR One Diversified, LLC

ADDRESS: 4 Market Street
Kenilworth, New Jersey 07033

PHONE _____

FAX _____

RESPONDANT



Signature

David Berndt

Printed Name

Vice President

Position with Company

AUTHORIZING OFFICIAL

Signature

Printed Name

Position with Company

PROPOSAL FORM 9: IMPLEMENTATION OF HOUSE BILL 1295

Certificate of Interested Parties (Form 1295):

In 2015, the Texas Legislature adopted House Bill 1295, which added section 2252.908 of the Government Code. The law states that a governmental entity or state agency may not enter into certain contracts with a business entity unless the business entity submits a disclosure of interested parties to the governmental entity or state agency at the time the business entity submits the signed contract to the governmental entity or state agency. The law applies only to a contract of a governmental entity or state agency that either (1) requires an action or vote by the governing body of the entity or agency before the contract may be signed or (2) has a value of at least \$1 million. The disclosure requirement applies to a contract entered into on or after January 1, 2016.

The Texas Ethics Commission was required to adopt rules necessary to implement that law, prescribe the disclosure of interested parties form, and post a copy of the form on the commission's website. The commission adopted the Certificate of Interested Parties form (Form 1295) on October 5, 2015. The commission also adopted new rules (Chapter 46) on November 30, 2015, to implement the law. The commission does not have any additional authority to enforce or interpret House Bill 1295.

Filing Process:

Starting on January 1, 2016, the commission will make available on its website a new filing application that must be used to file Form 1295. A business entity must use the application to enter the required information on Form 1295 and print a copy of the completed form, which will include a certification of filing that will contain a unique certification number. An authorized agent of the business entity must sign the printed copy of the form and have the form notarized. The completed Form 1295 with the certification of filing must be filed with the governmental body or state agency with which the business entity is entering into the contract.

The governmental entity or state agency must notify the commission, using the commission's filing application, of the receipt of the filed Form 1295 with the certification of filing not later than the 30th day after the date the contract binds all parties to the contract. The commission will post the completed Form 1295 to its website within seven business days after receiving notice from the governmental entity or state agency.

Information regarding how to use the filing application will be available on this site starting on January 1, 2016. https://www.ethics.state.tx.us/whatsnew/elf_info_form1295.htm

PROPOSAL FORM 10: BOYCOTT CERTIFICATION AND TERRORIST STATE CERTIFICATION

BOYCOTT CERTIFICATION

Respondents 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.

Does vendor agree? _____
(Initials of Authorized Representative)

TERRORIST STATE CERTIFICATION

In accordance with Texas Government Code, Chapter 2252, Subchapter F, REGION 10 ESC is prohibited from entering into a contract with a company that is identified on a list prepared and maintained by the Texas Comptroller or the State Pension Review Board under Texas Government Code Sections 806.051, 807.051, or 2252.153. By execution of any agreement, the respondent certifies to REGION 10 ESC that it is not a listed company under any of those Texas Government Code provisions. Responders must voluntarily and knowingly acknowledge and agree that any agreement shall be null and void should facts arise leading the REGION 10 ESC to believe that the respondent was a listed company at the time of this procurement.

Does vendor agree? _____
(Initials of Authorized Representative)

PROPOSAL FORM 11: RESIDENT CERTIFICATION

This Certification Section must be completed and submitted before a proposal can be awarded to your company. This information may be placed in an envelope labeled "Proprietary" and is not subject to public view. In order for a proposal to be considered, the following information must be provided. Failure to complete may result in rejection of the proposal:

As defined by Texas House Bill 602, a "nonresident Bidder" means a Bidder whose principal place of business is not in Texas, but excludes a contractor whose ultimate parent company or majority owner has its principal place of business in Texas.

Texas or Non-Texas Resident

I certify that my company is a "resident Bidder"

X I certify that my company qualifies as a "nonresident Bidder"

If you qualify as a "nonresident Bidder," you must furnish the following information:

What is your resident state? (The state your principal place of business is located.)

One Diversified, LLC 37 Market Street Kenilworth, New Jersey 07033

Company

Name

Address

City

State

Zip

PROPOSAL FORM 12: FEDERAL FUNDS CERIFICATION FORM

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 Vendors submitting proposals must complete this Federal Funds Certification Form regarding Vendor'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 participating agencies for their use while considering their purchasing options when using federal grant funds. Participating agencies may also require Vendors 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, Vendor should certify Vendor's agreement and ability to comply, where applicable, by having Vendor's authorized representative complete and initial the applicable lines after each section and sign the acknowledgment at the end of this form. If a vendor fails to complete any item in this form, Region 10 ESC will consider the Vendor'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 Vendor using federal funds.

1. Vendor Violation or Breach of Contract Terms:

Contracts for more than the simplified acquisition threshold currently set at \$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 contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Any Contract award will be subject to Region 10 ESC General Terms and Conditions, as well as any additional terms and conditions in any Purchase Order, participating agency ancillary contract, or Member Construction Contract agreed upon by Vendor and the participating agency which must be consistent with and protect the participating agency at least to the same extent as the Region 10 ESC 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 Vendor violation and breach of contract terms.

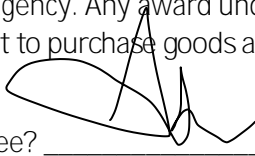
Does vendor agree? Yes, TLL.

(Initials of Authorized Representative)

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 \$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. Offeror 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 vendor agree? _____

(Initials of Authorized Representative)

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. Vendor 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 Vendor agrees that it shall comply with such provision.



Does vendor agree? _____

(Initials of Authorized Representative)

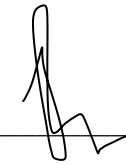
4. Davis-Bacon Act:

When required by Federal program legislation, Vendor agrees that, for all participating agency prime construction contracts/purchases in excess of \$2,000, Vendor 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, Vendor 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, Vendor 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. Vendor agrees that, for any purchase to which this requirement applies, the award of the purchase to the Vendor is conditioned upon Vendor's acceptance of the wage determination.

Vendor 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 contractor 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 vendor agree? _____

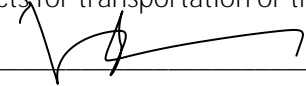


(Initials of Authorized Representative)

5. Contract Work Hours and Safety Standards Act:

Where applicable, for all participating agency contracts or purchases in excess of \$100,000 that involve the employment of mechanics or laborers, Vendor 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, Vendor is required to compute the wages of every mechanic and laborer on the basis of a standard work week of 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 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 vendor agree? _____



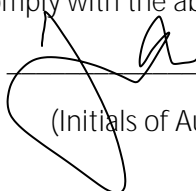
(Initials of Authorized Representative)

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.

Vendor agrees to comply with the above requirements when applicable.

Does vendor agree? _____



(Initials of Authorized Representative)

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 \$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, Vendor 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 vendor agree? _____



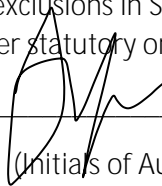
(Initials of Authorized Representative)

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.

Vendor certifies that Vendor 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. Vendor further agrees to immediately notify the Cooperative and all participating agencies with pending purchases or seeking to purchase from Vendor if Vendor 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 vendor agree? _____

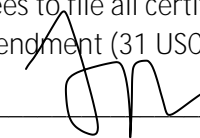


(Initials of Authorized Representative)

9. Byrd Anti-Lobbying Amendment:

Byrd Anti-Lobbying Amendment (31 USC 1352) -- Vendors that apply or bid for an award exceeding \$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, Vendor agrees to file all certifications and disclosures required by, and otherwise comply with, the Byrd Anti-Lobbying Amendment (31 USC 1352).

Does vendor agree? _____



(Initials of Authorized Representative)

10. Procurement of Recovered Materials:

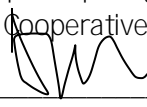
For participating agency purchases utilizing Federal funds, Vendor agrees to comply with Section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act where applicable and provide such information and certifications as a participating agency may require to confirm 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 \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$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 vendor agree? 
(Initials of Authorized Representative)

11. Profit as a Separate Element of Price:

For purchases using federal funds in excess of \$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, Vendor agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Vendor agrees that the total price, including profit, charged by Vendor to the participating agency shall not exceed the awarded pricing, including any applicable discount, under Vendor's Cooperative Contract.

Does vendor agree? 
(Initials of Authorized Representative)

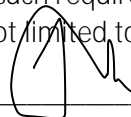
12. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

Vendor agrees that recipients and subrecipients are prohibited from obligating or expending loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system from companies described in Public Law 115-232, section 889. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country are also prohibited.

Does vendor agree? 
(Initials of Authorized Representative)

13. General Compliance and Cooperation with Participating Agencies:

In addition to the foregoing specific requirements, Vendor agrees, in accepting any Purchase Order from a participating agency, it shall make a good faith effort to work with participating agencies 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 vendor agree? 
(Initials of Authorized Representative)

14. Applicability to Subcontractors

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

Does vendor agree? 

(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.

One Diversified LLC

Company Name



Signature of Authorized Company Official

David Berndt

Printed Name

Vice President

Title

3/10/2022

Date

PROPOSAL FORM 13: ADDITIONAL ARIZONA CONTRACTOR REQUIREMENTS

AZ Compliance with Federal and state requirements: Contractor agrees when working on any federally assisted projects with more than \$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. Contractor agrees to post wage rates at the work site and submit a copy of their payroll to the member for their files. Contractor must retain records for three years to allow the federal grantor agency access to these records, upon demand. Contractor 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, contractor 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, Contractor 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" Region 10 ESC reserves the right to cancel or suspend the use of any contract for violations of immigration laws and regulations. Region 10 ESC and its members reserve the right to inspect the papers of any contractor or subcontract employee who works under this contract to ensure compliance with the warranty above.

AZ Contractor Employee Work Eligibility: By entering into this contract, contractor 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. Region 10 ESC and/or Region 10 ESC members may request verification of compliance from any contractor or sub contractor performing work under this contract. Region 10 ESC and Region 10 ESC members reserve the right to confirm compliance. In the event that Region 10 ESC or Region 10 ESC members suspect or find that any contractor or subcontractor is not in compliance, Region 10 ESC 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 contractor. All cost associated with any legal action will be the responsibility of the contractor.

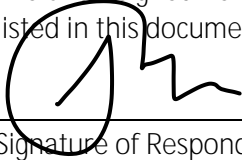
AZ Non-Compliance: All federally assisted contracts to members that exceed \$10,000.00 may be terminated by the federal grantee for noncompliance by contractor. In projects that are not federally funded, Respondent must agree to meet any federal, state or local requirements as necessary. In addition, 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, contractor 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. Contractor 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 Region 10 ESC member's discretion. Contractor 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, Region 10 ESC and Region 10 ESC members are prohibited from purchasing from a company that is in violation of the Export Administration Act. By entering into the contract, contractor 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.



March 9, 2022

Signature of Respondent

Date

PROPOSAL FORM 15: NON-COLLUSION AFFIDAVIT

Company Name:

Street:

City, State, Zip Code:

State of New Jersey

County of _____

I, David Berndt of the Washville
Name City

in the County of Davidson, State of Tennessee of full age, being duly sworn according to law on my oath depose and say that:

I am the Vice President of the firm of Diversified
Title Company Name

the Respondent making the Proposal for the goods, services or public work specified under the Harrison Township Board of Education 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 Harrison Township Board of Education 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

Diversified
Company Name

[Signature]
Authorized Signature & Title

Subscribed and sworn before me

this 1st day of March, 2022

Angela H. Smith

Notary Public of New Jersey

My commission expires

, 20 ANGELA G. SMITH
Notary Public, State of Alabama
Alabama State At Large
My Commission Expires
June 23, 2022

SEAL

PROPOSAL FORM 16: AFFIRMATIVE ACTION AFFIDAVIT (P.L. 1975, C.127)
Company Name: One Diversified, LLC
Street: 37 Market Street
City, State, Zip Code: Kenilworth, New Jersey 07033

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)

Vendors must submit with proposal:

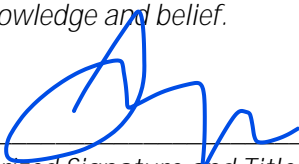
1. A photo copy of their Federal Letter of Affirmative Action Plan Approval _____
OR
2. A photo copy of their Certificate of Employee Information Report _____
OR
3. A complete Affirmative Action Employee Information Report (AA302) _____ **Please see attached.**

Public Work – Over \$50,000 Total Project Cost:

A. No approved Federal or New Jersey Affirmative Action Plan. We will complete Report Form _____
AA201-A upon receipt from the Harrison Township Board of Education

B. 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.



Authorized Signature and Title

March 9, 2022

Date

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

PROCUREMENT, PROFESSIONAL AND SERVICE CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor 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 contractor 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 contractor 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 contractor or subcontractor, where applicable will, in all solicitations or advertisement for employees placed by or on behalf of the contractor, 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 contractor 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 contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor 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 contractor 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 contractor 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 contractor 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 contractor 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 contractor 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

Global Sourcing Director

PROPOSAL FORM 17: C. 271 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 contractors. What follows are instructions on the use of form local units can provide to contractors 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 is available in Local Finance Notice 2006-1 (https://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html).

1. The disclosure is required for all contracts in excess of \$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 contractor 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 contractor and on file at least 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 contractor 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 contractors be provided a list of the affected agencies. This will assist contractors 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 https://www.state.nj.us/dca/divisions/dlgs/programs/pay_2_play.html 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 contractors 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 "Contractor 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 contractor also complete a "Stockholder Disclosure Certification." This will assist the local unit in its obligation to ensure that contractor did not make any prohibited contributions to the committees listed on the Business Entity Disclosure Certification in the 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 Contractor Instructions. NOTE: This section is not applicable to Boards of Education.

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Contractor Instructions

Business entities (contractors) 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 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

1. any State, county, or municipal committee of a political party
2. any legislative leadership committee*
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:
 1. of the public entity awarding the contract
 2. of that county in which that public entity is located
 3. of another public entity within that county
 4. 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 \$300 per election cycle that were made during the 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:

5. individuals with an "interest" ownership or control of more than 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
6. all principals, partners, officers, or directors of the business entity or their spouses
7. any subsidiaries directly or indirectly controlled by the business entity
8. 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 contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor'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 contractor's submission and is disclosable to the public under the Open Public Records Act. The contractor 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.

* 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

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 A COUNTY-BASED, CUSTOMIZABLE FORM.

PROPOSAL FORM 18: STOCKHOLDER DISCLOSURE CERTIFICATION

Name of Business:

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

OR

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

Check the box that represents the type of business organization:

Partnership

Sole Proprietorship

Limited Liability

Limited Partnership

Partnership

Corporation

XLimited Liability



Subchapter S

Corporation

Corporation

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

Stockholders:

Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:
Subscribed and sworn before me this <u>1st</u> day of <u>March</u> , 20 <u>22</u> .	 (Affiant)
(Notary Public) 	<u>David Berndt</u> Vice President (Print name & title of affiant)
My Commission expires: <u>ANGELA G. SMITH</u> <u>Notary Public, State of Alabama</u> <u>Alabama State At Large</u> <u>My Commission Expires</u> <u>June 23, 2022</u>	(Corporate Seal)

PROPOSAL FORM 19: GENERAL TERMS AND CONDITIONS ACCEPTANCE FORM

Signature on the Vendor Contract Signature form certifies complete acceptance of the General Terms and Conditions in this solicitation, except as noted below (additional pages may be attached, if necessary).

Check one of the following responses to the General Terms and Conditions:

- We take no exceptions/deviations to the general terms and conditions

(Note: If none are listed below, it is understood that no exceptions/deviations are taken.)

We take the following exceptions/deviations to the general terms and conditions. All exceptions/deviations must be clearly explained. Reference the corresponding general terms and conditions that you are taking exceptions/deviations to. Clearly state if you are adding additions terms and conditions to the general terms and conditions. Provide details on your exceptions/deviations below:

(Note: Unacceptable exceptions shall remove your proposal from consideration for award. Region 10 ESC shall be the sole judge on the acceptance of exceptions/deviations and the decision shall be final.)

PROPOSAL FORM 20: EQUALIS GROUP ADMINISTRATION AGREEMENT

Requirements for Master Agreement To be administered by Equalis Group

Attachment A, Equalis Group Administrative Agreement is used in administering Master Agreements with Region 10 and is preferred by Equalis Group. Redlined copies of this agreement should not be submitted with the response. Should a respondent be recommended for award, this agreement will be negotiated and executed between Equalis Group and the respondent. Respondents must select one of the following options for submitting their response.

- Respondent agrees to all terms and conditions outlined in each of the Administration Agreement.
- Respondent wishes to negotiate directly with Equalis Group on terms and conditions outlined in the Administration Agreement. Negotiations will commence after sealed Proposals are opened and Region 10 has determined the respondent met all requirements in their response and may be eligible for award.

PROPOSAL FORM 21: OPEN RECORDS POLICY ACKNOWLEDGEMENT AND ACCEPTANCE
OPEN RECORDS POLICY ACKNOWLEDGMENT AND ACCEPTANCE

Be advised that all information and documents submitted will be subject to the Public Information Act requirements governed by Chapter 552 of the Texas Government Code.

Because contracts are awarded by a Texas governmental entity, all responses submitted are subject to release as public information after contracts are executed. If a Respondent believes that its response, or parts of its response, may be exempted from disclosure to the public, the Respondent must specify page-by-page and line-by-line the parts of the response, which it believes, are exempted from disclosure. In addition, the Respondent must specify which exception(s) are applicable and provide detailed reasons to substantiate the exception(s). Respondent must provide this information on the "Acknowledgement and Acceptance to Region 10 ESC's Public Information Act Policy" form found on the next page of this solicitation. Any information that is unmarked will be considered public information and released, if requested under the Public Information Act.

The determination of whether information is confidential and not subject to disclosure is the duty of the Office of Attorney General (OAG). Region 10 ESC must provide the OAG with the information requested in order for the OAG to render an opinion. In such circumstances, Respondent will be notified in writing that the material has been requested and delivered to the OAG. Respondent will have an opportunity to make arguments to the OAG in writing regarding the exception(s) to the TPIA that permit the information to be withheld from public disclosure. Respondents are advised that such arguments to the OAG must be specific and well-reasoned--vague and general claims to confidentiality by the Respondent are generally not acceptable to the OAG. Once the OAG opinion is received by Region 10 ESC, Region 10 ESC must comply with the opinions of the OAG. Region 10 ESC assumes no responsibility for asserting legal arguments on behalf of any Respondent. Respondents are advised to consult with their legal counsel concerning disclosure issues resulting from this procurement process and to take precautions to safeguard trade secrets and other proprietary information.

After completion of award, these documents will be available for public inspection.

Signature below certifies complete acceptance of Region 10 ESC's Open Records Policy, except as noted below (additional pages may be attached, if necessary). Check one of the following responses to the Acknowledgment and Acceptance of Region 10 ESC's Open Records Policy below:

We acknowledge Region 10 ESC's Public Information Act policy and declare that no information submitted with this proposal, or any part of our proposal, is exempt from disclosure under the Public Information Act.
(Note: All information believed to be a trade secret or proprietary must be listed below. It is further understood that failure to identify such information, in strict accordance with the instructions below, will result in that information being considered public information and released, if requested under the Public Information Act.)

We declare the following information to be a trade secret or proprietary and exempt from disclosure under the Public Information Act.
(Note: Respondent must specify page-by-page and line-by-line the parts of the response, which it believes, are exempt. In addition, Respondent must specify which exception(s) are applicable and provide detailed reasons to substantiate the exception(s).)

March 9, 2022

Date

Business Development Representative


Authorized Signature & Title

PROPOSAL FORM 22: VENDOR CONTRACT AND SIGNATURE FORM

The undersigned hereby proposes and agrees to furnish goods and/or services in strict compliance with the terms, specifications and conditions at the prices proposed within response unless noted in writing. The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this proposal in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said proposal have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

VENDORS MUST SUBMIT THIS FORM COMPLETED AND SIGNED WITH THEIR RESPONSE TO BE CONSIDERED

Company name One Diversified, LLC
Address 37 Market Street
City/State/Zip Kenilworth, New Jersey 07033
Telephone No. (866) 447-1004
Fax No.
Email address tlee@onediversified.com
Printed name Tracie L. Lee
Position with company Business Development Representative
Authorized signature

Term of contract March 1, 2022 to February 28, 2025

Unless otherwise stated, all contracts are for a period of three (3) years with an option to renew annually for an additional two (2) years if agreed to by Region 10 ESC. Vendor shall honor all administrative fees for any sales made based on the contract whether renewed or not.


Jana Melsheimer (Apr 20, 2022 10:30 CDT)
Region 10 ESC Authorized Agent

4/20/22
Date

Dr.. Jana Melsheimer
Print Name

Equalis Group Contract Number R10-1130B



Did you sign the vendor contract and signature form? If not, your Proposal will be rejected.

Region 10 will negotiate any exceptions and both parties will agree upon which exceptions will be accepted or altered before the Region 10 board votes to accept or reject the proposals.

DIVERSIFIED

Cryptography Policy

Version 1.00
March 9, 2020



Kenilworth, NJ

Contents

1	Purpose.....	3
2	Scope.....	3
3	Definitions.....	3
4	Controls.....	4
5	Policy	4
5.1	Secret Key Encryption Keys	4
5.2	Public Key Encryption Keys	5
5.3	Loss and Theft.....	5



1 Purpose

The Diversified Security Policy establishes requirements for the use of encryption techniques to protect sensitive data both at rest and in transit. This policy defines the controls and related procedures for the various areas where encryption and other cryptographic techniques are employed.

2 Scope

Cryptographic controls can be used to achieve multiple cybersecurity objectives. These include:

- **Confidentiality:** using encryption of information to protect sensitive or critical information, either during transmission or while at rest
- **Integrity/authenticity:** using digital signature certificates or message authentication codes to verify authenticity or integrity of stored or transmitted sensitive or critical information
- **Non-repudiation:** using cryptographic techniques to provide evidence of the occurrence of an event or action
- **Authentication:** using cryptographic techniques to authenticate users and other system entities requesting access or transacting with system users, entities and

3 Definitions

- **Cryptography:** a method of storing and transmitting data in a form that only those it is intended for can read and process.
- **Encryption:** the process of converting data from plain text to a form that is not readable to unauthorized parties, known as cipher-text.
- **Key:** the input that controls the process of encryption and decryption. There are both secret and public keys used in cryptography.
- **Digital Certificate:** An electronic document that is used to verify the identity of the certificate holder when conducting electronic transactions. SSL certificates are a common example that have identifying data about a server on the Internet as well as the owning authority's public encryption key.
- **Digital Signature Certificate:** a type of digital certificate that proves that the sender of a message or owner of a document is authentic, and the integrity of the message or document is intact. A digital signature certificate uses asymmetric cryptography and is not a scanned version of someone's handwritten signature or a computer-generated handwritten signature (a.k.a. an electronic signature).
- **SSH Keys:** A public/private key pair used for authenticating to SSH servers and establishing a secure network connection.



4 Controls

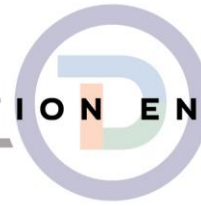
- Approved encryption methods for data at rest
 - Data in some locations requires that the storage of sensitive data be encrypted.
- Encryption methods for data in motion
 - The transfer of sensitive data is required to be done via a secure channel, which is an encrypted network connection.
 - Various methods of encryption are available and generally built-into the application. The user should be aware of the data connection being used to transmit sensitive data and if encryption is enabled for that connection.
- Encryption is required for
 - The transport of sensitive files (SSL or SCP usage to encrypt sensitive data for network file access of unencrypted files).
 - Access to sensitive data via a web site, web application or mobile app. Encryption is required for accessing sensitive data from anything with a web interface, including mobile devices (i.e. use of HTTPS to encrypt sensitive data).
 - All network traffic for remote access to the virtual desktop environment.
 - Transport of sensitive data that is part of a database query or web service call (examples SQL query to retrieve or send data from database or a web service call to retrieve or send data from a cloud application).
- Encryption of Email
 - Sensitive data is not permitted to be sent via normal email. The use of encryption is required for any email containing sensitive information or attachments.
- Use and management of SSH keys
 - Create a key-pair by running: `ssh-keygen -t rsa -C "your_email"`
- Use and management of SSL digital certificates
 - Diversified production web servers (or devices with a web interface) that support secure (HTTPS) connections must have an SSL certificate installed.

5 Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

5.1 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be



encrypted using an RSA key of at least 2048 bits. This is implemented using standard openssl libraries when using both SSH and HTTPS, which ensures proper key-exchange and storage.

5.2 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it is issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

5.3 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to the current staff, which must then apply proper actions that will be required regarding revocation of certificates or public-private key pairs.

DIVERSIFIED

Information Security Policy

Version 1.50
March 30 2021



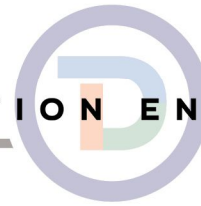
Kenilworth, NJ

Contents

1	Document Scope	2
2	Information Security Principles and Standards.....	3
3	Security Guidelines	3
3.1	Policies	3
3.2	Administrative and Technical Control Guidelines	4
3.2.1	IT Acceptable Use.....	4
3.2.2	Information Management.....	6
3.2.3	Access Management	8
3.2.4	Asset Management.....	12
3.2.5	Configuration Management	13
3.2.6	Information System Lifecycle.....	15
3.2.7	Encryption.....	16
3.2.8	Logging & Monitoring.....	17
3.2.9	Network Security	18
3.2.10	Platform Security	20
3.2.11	Physical Security.....	21
3.2.12	Risk Assessments.....	23
3.2.13	Security Awareness.....	24
3.2.14	External Party Management.....	24
3.2.15	Disaster Recovery and Business Continuity	25
3.2.16	Incident Management.....	27
4	Appendix A: Glossary of Terms	30

1 Document Scope

This is the Security Policy Statement of DIVERSIFIED. The document will define the steps to protect the confidentiality, integrity and availability of Diversified's information assets. The standards set forth in this document are intended as guidelines and best practices to secure Diversified's information assets and are not intended to create legal standards. Its purpose is to provide general strategy and guidelines for administrative and technical security controls. The standards and guidelines set forth in this document are applicable to all Diversified users, employees, vendors, contractors, external parties and all others with access to information and equipment owned or managed by Diversified.



2 Information Security Principles and Standards

Information security is, at its core, the preservation of the following properties of information:

Confidentiality – Protection of information against unauthorized disclosure throughout its lifecycle.

Integrity – Protection of the accuracy and completeness of information.

Availability – Protection of the accessibility of information when required.

Safeguarding the Confidentiality, Integrity and Availability of Information assets should be a priority at Diversified.

Like most organizations, Diversified relies heavily on information (Information Assets) to achieve its organizational goal. Diversified is committed to protecting the confidentiality, integrity, and availability of its Information Assets in order to accomplish this. Information security should be a consideration in all Diversified operations and activities, to protect Information Assets in a manner that reduces risk while enabling and supporting all aspects of Diversified functions.

3 Security Guidelines

3.1 Policies

Diversified has created the following Policies to protect their information assets from unauthorized access, modification and destruction.

- Access Management Policy
- Asset Management Policy
- Business Continuity and Disaster Recovery Policy
- Backup and Recovery Policy
- Change Management Policy
- Configuration Management Policy
- Encryption
- External Party Management Policy
- Information Management Policy
- Information Security Incident Management Policy
- Information System Lifecycle Policy
- IT Acceptable Use Policy
- Logging & Monitoring Policy
- Network Security Policy

Physical Security Policy
Platform Security Policy
Risk Assessment Policy

3.2 Administrative and Technical Control Guidelines

The following controls and best practices should be in place to protect Diversified's information assets from unauthorized access, modification and destruction.

3.2.1 IT Acceptable Use

3.2.1.1 Overview

IT Acceptable Use sets out the principles and procedures applicable to the acceptable use of Information Technology equipment, services, facilities, and electronic communications, including email, instant messaging, digital faxing, removable storage devices, data exchange, wireless technology, mobile computing, and other similar facilities and services of Diversified.

3.2.1.2 Activities that should be required

All Users should:

1. Properly use and protect all Diversified Information Assets based on classification, including, but not limited to, proper labeling, handling, access, storage, transmission, and destruction. Classification-specific guidelines are detailed in the Information Management Policy.
2. Use Diversified Information Assets for business purposes only, and in a professional manner. (Occasional limited personal use is permitted at the sole discretion of management. Such use should be minimized and should not interfere with the work of the User or the business of the Diversified.)
3. Limit the use of Removable Media for storing and/or transporting Diversified Information classified For Internal Use Only.
4. Notify Information Technology management promptly when an Information Asset is lost, stolen, or disclosed in a manner inconsistent with its classification.
5. Obtain proper authorization for any of the following activities:
 - a. Removal of Information Assets or other Diversified equipment from any Diversified Facility.
 - b. Access to another employee's files, email, voicemail, or other stored Information.
 - c. Intercepting any network communications (reading messages/file contents, rerouting packets, packet sniffing, etc.).
 - d. Installation of any software.
 - e. Transmission of Diversified Information, in any fashion, to any third party.
 - f. Use of any software not previously approved.

- g. Sending of electronic messages (email, instant messages, SMS messages, etc.) to a large number of recipients.
- h. Use of social media platforms for official communications on behalf of the Diversified, including, but not limited to, use of the Diversified's logo, graphics, trademarks, trade names, or corporate slogans in any online media or forum.
- i. Audio or video recording of other employees in the workplace.
- 6. Take reasonable measures to prevent unauthorized individuals from accessing Diversified Information Security Assets, including via a Mobile Device.
- 7. Comply with the social media policy set forth in the Diversified Compliance Plan when reading, writing, or otherwise contributing to any online social media platform, including but not limited to blogs, chat rooms, online message boards, social networking websites or profiles, and online discussion group.

3.2.1.3 Activities which are expressly prohibited

All Users shall not:

- 1. Utilize a Mobile Device while driving.
- 2. Use Information Assets for unauthorized purposes, including, but not limited to:
 - a. Gaining unauthorized access to, damaging, altering, or disrupting the Diversified's or other systems.
 - b. Using or disclosing another employee's password.
 - c. Enabling unauthorized third parties to gain access to or use Diversified Information Assets.
 - d. Unreasonably jeopardizing the security of the Diversified's Information Assets.
 - e. Connecting unauthorized hardware directly to the Diversified network or Information Assets, including, but not limited to, computers, modems and wireless access points.
 - f. Using unauthorized or unlicensed software, including, but not limited to, data sharing applications and remote control applications.
 - g. Introducing malicious code into any Diversified Information Asset or Facility.
 - h. Using Diversified Information Assets in any violation of state or federal laws or regulations.
 - i. Making unauthorized and infringing copies of material protected under copyright law or making that material available to others for such copying. This includes use of data sharing programs.
 - j. Using Diversified Information Assets for illegal or unethical activities or any purposes related to activities prohibited by the Employee handbook, except when part of authorized monitoring and reporting within the Security Monitoring and Reporting Process.
 - k. Transmitting, accessing, or receiving offensive, harassing, sexually suggestive, or otherwise inappropriate material.
- 3. Disclose Diversified Information in a manner inconsistent with its classification.

4. Copy and/or transport Protected or Confidential Information to Removable Media without authorization from management (other than backup tapes managed by an Information Backup and Restore Process).
5. Circumvent, or attempt to circumvent, any personnel, process, or technical security controls.

3.2.2 Information Management

3.2.2.1 Overview

This control provides standards and guidelines for the ownership and classification of Diversified information assets. Assignment of an owner and a classification to information allows for the definition of exactly how that information should be managed and protected and makes those guidelines clear to all users.

3.2.2.2 Information Ownership

All Information Assets should have an assigned and recorded Data Custodian (Information), System Custodian (Information Systems), and Application Custodian (applications, where applicable). For example, in the case of financial data stored in a financial application, a designated individual or subgroup in the Finance Department is the Data Custodian; designated individuals(s) or subgroup(s) in the Information Technology Department are the System Custodian and Application Custodian. The System Custodian and the Application Custodian may or may not be the same individual or group. The Information Classification Process should be used to execute this guideline.

3.2.2.3 Information Classification

All Diversified Information should be assigned, by its Data Owner or Data Custodian, a classification in respect to its confidentiality, integrity, and availability. Possible classifications are shown in bold below.

1. Protected - Data with significant access restrictions due to legal, regulatory, or contractual obligations; this classification applies across the entire Diversified organization. The following Information is automatically classified as Protected:
 - a. Cardholder data as defined by the PCI DSS.
 - b. Patient health information (PHI) as defined by the HIPAA Security Rule and Privacy Rule.
 - c. Personally-identifiable information (PII), including personnel data.

- d. Controller Unclassified Information or Covered Defense Information that is marked and provided to Diversified or data is created by Diversified that fits the defined criteria of these information categories
- e. Any other regulated data for which high confidentiality is required by law.
- 2. Confidential - Data considered sensitive by the business unit or a client; this classification may be discretionary, subject to review and policy changes. This classification should be applied to sensitive internal information which is to be known only to a small and well-defined group of people. Diversified-specific examples include, but are not limited to, financial data and internal-use software applications developed by Diversified.
- 3. Internal Use Only Data that is semi-confidential, is accessed within one or more departments, and is not to be shared with the general public. This classification is discretionary and is often defined by functional requirements. This classification should be applied by default to all other Diversified Information but should be restricted to departments. Diversified-specific examples include, but are not limited to: internal Policies, Processes, and Procedures; internal meeting minutes, and facilities records.
- 4. Public - Data that is available to both Users and the general public; this classification is also discretionary subject to review and policy changes. This classification should generally be applied to all Information that can be shared with the general public without risk to the Diversified. Diversified-specific examples include, but are not limited to, approved press releases and public Web site content.

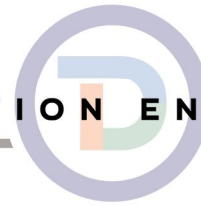
3.2.2.4 Information Labeling

Once the Information is classified, System and Application Owners (or their custodians) should implement the labels and resulting controls within their systems. In addition, this will drive guidelines for unique storage, transmission, protection, handling, and destruction of classified and/or protected information. The Information Classification Process should be used to execute this guideline.

3.2.2.5 Information Loss

Information loss is defined as the transfer of classified information from a computer, data center or user to unauthorized parties. Information can be accomplished by several methods including, but not limited to:

1. Email
2. Data transfer using removable storage devices
3. Photography, Screenshots
4. Cloud File Storage Upload/transfer
5. Social Media
6. Verbal or Audible disclosure



System and Application Owners are required to implement technical and systematic controls within their systems for preventing and monitoring for Information Loss. To determine what information should be prevented from transmission and what information should be monitored, System and Application owners should refer to the Information classification guidelines. The information loss should be prevented in the following fashions:

1. System and information access should be controlled using the Access Management Policy (3.2.3)
2. Protected and Confidential data should be transmitted and stored using approved Encryption methods.
3. Technical controls should be in place to prevent violations of these Information Loss guidelines.
4. Storage of Protected, Confidential, or Internal Use Only information on non-Diversified controlled environments including devices maintained by a third party with whom Diversified does not have a contractual agreement, is prohibited.
5. Any violations or suspicious actions should be monitored and flagged for further investigation. The following questions can help determination of incident.
 - a. How is the information classified?
 - b. Is the information source authorized to view and transmit the information?
 - c. Is the information destination authorized to view the information?
6. All Information Loss alerts should be sent and logged in OneDesk for Information Security Team investigation.
7. All Information Loss alerts should be reviewed continuously on a 24/7/365 basis.
8. Any alerts that require further investigation should be immediately escalated to the Information Security Team Review Team.
9. If further action is required, please refer to the Incident Management Policy (3.2.16)
10. This process will be reviewed on a quarterly basis for efficacy.

3.2.3 Access Management

3.2.3.1 Overview

The objective of access control is to ensure authorized access and prevent unauthorized access to Information Assets.

3.2.3.2 Access Request and Revocation

1. All access requests should be initiated centrally through a centralized process.
2. Upon termination, all access should be revoked for any terminated users. All termination requests should initiate through a centralized process, which will review all access request tickets to relay the appropriate revocation requests and retrieve allocated hardware.

3.2.3.3 Administrative Access

Standard users should not have local administrative access to their own workstations and laptops. System administration privileges should only be granted to authorize users after security review.

3.2.3.4 Segregation Rules

1. Segregation of duties between development/test and production environments should be enforced.
2. Application and system development staff should not have standing access to production systems. This should only occur in emergency situations via an established standard Firewall procedure.
3. Segregation of duties between technical staff and those individuals who are responsible for performing business related functions should be enforced.
4. Segregation of duties to ensure that individuals responsible for assigning access to information systems are not themselves end users of those systems should be enforced.

3.2.3.5 Least Privilege Rules

1. Default access controls for all systems should be 'no access.'
2. Limit access to system components and protected data to only those individuals whose job requires such access.
3. Restrict External Party access to content/production areas unless required for their job function.
4. Ensure Users only have access to their own data and digital information assets.
5. Enable vendor accounts used for remote access only during the time period needed.

3.2.3.6 Access Review

1. IT Management and Executive Management should review Users' access rights at quarterly intervals. These reviews should be documented and submitted to the Information Security Office.
2. Disabled accounts (or inactive) user accounts should be removed at least every 90 days

3.2.3.7 Standard User Accounts and Passwords

1. All users should have a unique ID.
2. Passwords should be at least eight (8) characters long.
3. Should include at least three of the following four (4) categories: uppercase letters, lowercase letters, numbers, and special characters (punctuation marks and symbols).
4. Should not include words that can be found in a dictionary.
5. Should not be comprised of an obvious keyboard sequence (i.e., QWERTY).
6. Should not include "guessable" data such as personal information (birthdays, addresses, phone numbers, locations, favorite teams, pets, etc.) or part or all of a Diversified name.
7. Should expire at least every ninety (90) days.

8. Should not be the same as any of the previous eight passwords used for that account or within the last 90 days.
9. Render all passwords unreadable during transmission and storage on all system components using strong cryptography
10. Individuals should not use group, shared, or generic accounts and passwords or similar authentication methods.
11. System accounts should have a designated owner
12. Default passwords for any installed software, hardware or technology platform should be changed immediately after installation.
13. Initial/Temporary password should be unique and random and comply with all other password complexity rules.
14. Initial/Temporary password should be changed at first logon.
15. Systems and applications should never send protected information including Passwords/PINs in clear text across the network.
16. A session time-out mechanism, which forces a user to re-authenticate their user ID should activate after 15 minutes (or less) of inactivity by a user's interface device (e.g., keyboard, mouse, or touch screen), should be in place.
17. This policy applies to all user accounts and password in use for application, systems, and devices.
18. A user must first authenticate on to a system before they may change any password they have permission to change.

3.2.3.8 Privileged Accounts

1. Administrator and root level system accounts should be strictly controlled. Administrators should be granted only the minimum level of privilege necessary for their specific duties.
2. Privileged Account access actions should be logged and monitored.
3. Administrative privileges should be removed when no longer needed

3.2.3.9 Non-Interactive Service Accounts

1. Should have a Unique ID.
2. Should be at least fifteen (15) characters long.
3. Should include at least three of the following four (4) categories: uppercase letters, lowercase letters, numbers, and special characters (punctuation marks and symbols).
4. Should not include words that can be found in a dictionary
5. Should not be comprised of an obvious keyboard sequence (i.e., QWERTY).
6. Should not include "guessable" data such as personal information (birthdays, addresses, phone numbers, locations, favorite teams, pets, etc.) or part or all of a Diversified name.
7. Should expire at least every 180 days. Expiration should be set to trigger in February and August so that passwords do not expire during the Diversified season.
8. Should never be reused.

3.2.3.10 Non-Permanent Personnel Account for Troubleshooting

1. Should comply with Standard User Accounts and Passwords policy
2. Account should be disabled or removed after each use

3.2.3.11 Lockout and Session Inactivity

1. All accounts should lock automatically after no more than five (5) failed login attempts and remain locked until a System Owner unlocks it.
2. Any user session idle for more than fifteen (15) minutes should lock or disconnect and require re-authentication, except for connections to continuous-monitoring systems. Such systems should employ additional physical and technical security controls to limit access.
3. Non-laptop Mobile Devices should have their screens lock after no more than five (5) minutes of inactivity, with password required to unlock.
4. Laptops should have their screens lock after no more than ten (10) minutes of inactivity, with password required to unlock.

3.2.3.12 Remote Access

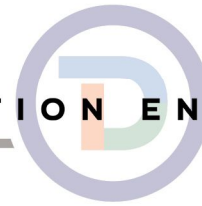
1. All accounts should lock automatically after no more than five (5) failed login attempts and remain locked until a System Owner unlocks it.
2. Any user session idle for more than fifteen (15) minutes should lock or disconnect and require re-authentication

3.2.3.13 Authentication Methods

All authentication methods should use industry-accepted encryption methods such as Kerberos and SAML.

3.2.3.14 Network Access Control

1. The network and infrastructure should be protected by a Network Access Control platform. That platform should perform the following functions:
 - a. Scan Network for Non-Domain Authenticated Devices
 - b. Scan Network for Devices out of compliance. Factors for compliance should be:
 - i. Windows Updates
 - ii. Anti-Virus Software installed
 - iii. Approved Software installed
 - iv. No Peer to Peer Software installed
 - v. Device has no Malware
 - vi. Device can be classified
 - c. Remove rogue devices from the network, place them in quarantine.
 - d. Notify Network Administrators and Information Security Team if a rogue device is discovered.
 - e. Capture network information about each device, including MAC address, IP address, Port number, Switch, hostname etc.
 - f. Utilize 802.1x or other method/protocol to perform device level authentication
 - g. Perform cyber threat management and information generation.



- h. Promote compliant devices to the network VLAN/subnet
2. Network Access control should be utilized to provide corporate VLAN access for approved and compliant devices based upon multi-factor authentication. (Domain authenticated, MAC address authenticated)
3. Network Access Control should verify security of equipment and compliance before allowing access to the corporate network.
4. Devices that do not meet security standards, present security risks, are infected by malware or are at risk for infection should be prevented from having network access.
5. Any new devices that are allowed access to the network, should be submitted to the ticketing system for review of the device and the request. Approval is required from the Network Engineering team and the information security team.
6. Any non-compliant incidents or events should be captured and reviewed by Information security team. This should be done on a 365x7x24 basis.
7. Any non-compliant or non-authenticated devices will be immediately removed from the network. This should be done on a 365x7x24 basis.

3.2.4 Asset Management

3.2.4.1 Overview

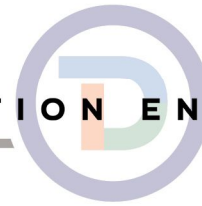
This Control addresses baseline guidelines for lifecycle management and physical inventory management of IT hardware and software assets (assets) purchased, licensed and/or leased by Diversified.

3.2.4.2 Asset Management

1. All IT assets should have an asset owner. An IT asset owner is accountable for determining, implementing, and maintaining adequate security for his/her IT assets.
2. Asset management should utilize a lifecycle methodology that manages asset procurement, deployment, operations, and end of life.
3. Asset management is responsible for maintaining vendor list for their respected assets.
4. Before deploying information assets to External Parties, those entities should read and sign confidentiality agreements.

3.2.4.3 Asset Identification

1. All hardware assets used by information technology should be identified, tagged, and tracked as they are assigned to personnel.
2. Labeling of assets should include owner, contact information and purpose.
3. All Blank Media should be tagged and tracked



4. All software inventory should be identified and tracked.
5. License requirements for software and other proprietary software assets should be tracked and met.
6. Perform a quarterly inventory count.

3.2.4.4 Asset Storage or Relocation

1. Store elements targeted for recycling/destruction in a secure location/container and store client assets in a restricted and secure area.
2. Backup media should be stored in a secure location at all times.
3. Data on an asset relocated to a new location should be reviewed to ensure its classification is properly protected during the movement and in all locations outside its primary location or it should be properly sanitized prior to any movement.

3.2.4.5 Asset Reclamation

1. All terminated users should have their assets reclaimed and processed for recycling or disposal.
2. All retrieved media should be routinely checked for protected data and scrubbed.

3.2.4.6 Asset Disposal

1. All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
2. Destroy media when it is no longer needed for business or legal reasons. Require that rejected, damaged, and obsolete stock are erased, degaussed, shredded, or physically destroyed before disposal.

3.2.5 Configuration Management

3.2.5.1 Patch Management & Security Patches

1. Ensure that all Applications, Systems, and Network Appliances are protected from known vulnerabilities by having the latest vendor-supplied security patches. Security patches should be reviewed every 30 days by the technology teams.
2. Implement a patch management process.
3. Applications, Systems, and Network Appliances should be at the same supported version levels for configuration management consistency.

3.2.5.2 Security Configuration Management

1. Configure system security parameters to prevent misuse. Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.
2. Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
3. Always change vendor-supplied defaults before installing a system on the network, including passwords, SNMP community strings, and elimination of unnecessary accounts.

4. Any unauthorized software should be removed from production systems.
5. Utilities, compilers, assemblers or other utilities that create object code should not be installed on production computer systems.
6. Activities of maintenance personnel without the required access authorization shall be supervised at all times by an individual with the required access authorizations.

3.2.5.3 Remote Access Controls

1. Remote access should incorporate two-factor authentication
2. For Protected Information accessed remotely, prohibit copy, move, and storage of such data onto local hard drives.
3. Remote access connection rules should be implemented to restrict access to required nodes and networks.
4. As a rule, management networks (subnets utilized for managing critical infrastructure resources) should not be accessible via remote access without security approval.
5. Activation of remote-access technologies for vendors and business partners only when needed by vendors.
6. Directly connected networks such as business to business connections must be initiated through a formal change control and be approved by information security or senior management.
7. Access to the Diversified Internal Network is restricted to Diversified Managed devices that meet or exceed the company security standard.
8. Approval is required by Diversified IT Security for any encrypted protocol communications that cannot be authenticated via a proxy device

3.2.5.4 Change Control

1. All elements of the production system and application environment should be subject to change control.
2. New or not yet approved technology should not be installed unless it follows approved change control procedures and is approved by management. This includes, but is not limited to, installing operating systems, routers, wireless devices, etc. All changes to the production environment should be documented, tested, approved and scheduled. Documentation should include back out procedures.
3. Formalized testing criteria should be defined and proposed changes to production systems should be tested against those criteria. The test criteria should include security requirements and all network connections and changes to the firewall and router configurations before deploying dependent systems.
4. A change control process and procedure should be utilized for all changes to system components. This includes change notification through an RFC (Request for Change) ticket and approval from the change advisory board (CAB).
5. There should be documented procedures for introducing unscheduled or emergency changes to the environment; these should be kept to minimum.

6. All changes to production systems should include steps to back out or undo implemented changes.
7. A start time and duration of change window should be defined for all change control requests.
8. Emergency changes can be requested of the change advisory board for any system change needed for a production system outside its maintenance window or prior to the defined notification process.
9. Emergency changes should be reviewed within 24 hours of completion.
10. All Changes should be reviewed as part of the Bi-Weekly IT Security Meeting.

3.2.6 Information System Lifecycle

3.2.6.1 Overview

This control sets forth standards and guidelines for the secure development, implementation, and management of all Diversified Information Assets that are information systems and software. Proper application of technical and process-based security controls to Information Assets at all stages of use is essential to ensure the Information Asset is adequately protected.

3.2.6.2 Development Environment

1. Development should be controlled utilizing a software development lifecycle (SDLC) for application development as defined by the IT Engineering Department.
2. This SDLC should include business requirements translations, SDLC change control processes, iterative or non-iterative development phases, and testing criteria. Testing criteria examples would be functional and non-functional testing, load (stress) testing, user acceptance testing, and security testing.
3. Security should be monitored and integrated within the development processes in respect to business requirements and security testing.
4. Development, test and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.
5. The use of live production data for development testing is prohibited. In cases where production data is needed for testing, the data should be desensitized and approved by Information security.
6. All source code is stored in a Code Repository with access controlled by user permissions.
7. All source code is versioned and all changes/updates to the code are tracked in the repository.
8. Developers are allowed either read or read-write access to the code based on job function and code can only be checked out onto Diversified owned device.

3.2.6.3 Secure Coding Practices and Techniques

1. Comply with all security requirements and approved software deployment. Review and comply with the security operations requirements.

2. Develop applications based on secure coding guidelines. Review custom code prior to release to production or customers in order to identify any potential coding vulnerability. When possible, utilize automated code checking software in addition to peer review.
3. Remove custom application accounts, user IDs, and passwords before applications become active.
4. When importing a database from production, all unnecessary production data should be deleted. All Protected Information from production should be deleted.
5. IT systems should not be coded to contain back doors that circumvent the authorized access control mechanisms

3.2.7 Encryption

3.2.7.1 Overview

This Control addresses baseline guidelines for applying cryptographic solutions to Diversified's information.

3.2.7.2 Block and Stream Encryption

1. All encryption implemented in production should leverage strong encryption within the infrastructure on which the encryption is implemented.
2. The following algorithms are approved for use in production:
 - a. Encryption: AES (128, 192, or 256 bits) and 3DES
 - b. Key establishment: RSA (1024 bits minimum, 2048 or higher recommended) and Diffie-Hellman
 - c. Digital signatures: RSA and DSA (1024 bits minimum, 2048 or higher recommended)
 - d. Hash algorithms: SHA-2 or higher
 - e. Data integrity: HMAC and CMAC
 - f. Wireless: Wi-Fi Protected Access (WPA) version 2
3. All Web servers supporting HTTPS (SSL) should support SSL version 3 and TLS 1.2. Certificate Hashes should be configured for SHA-2 or higher.
4. All email systems should use Transport Layer Security (TLS 1.2 or higher) wherever possible.
5. All management access and remote desktop access should be configured to only support strong crypto packs.
6. Only SSH version 3 and Open SSH 5.2 are to be utilized when SSH protocols are used.
7. Send decryption symmetric keys or passwords using an out-of-band communication protocols or PGP protocols. The Information Security Office should be consulted.
8. Protected data should be encrypted in storage and transmission and never be sent unprotected by end-user messaging technologies.

3.2.7.3 Key Management

1. A key management process should be in place to support the organization's use of cryptographic certificate techniques.
2. External-facing sites should utilize recognized Internet Certificate Authorities (such as VeriSign) for all SSL connections. All purchased certificates should be reviewed with current industry standards and updated if required regardless of certificate expiration date. Certificate review should be done yearly by the Information Security Office.
3. Internal sites can utilize external certificate authorities or an internal PKI infrastructure. If an internal PKI infrastructure is utilized, the same yearly review of certificates should be conducted by the Information Security Office.
4. If utilized, an internal PKI infrastructure should be composed of a minimum of two servers, a root certificate server and a certificate issuing server. The root certificate server should not be integrated into Active Directory and be kept offline when not used. The issuing certificate server should be integrated into Active directory with restrictive controls. This will allow the utilization of Active directory recovery agents and IPsec encryption for domain controller traffic.
5. Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of protected data.
6. Key management process should be designed so that no single person has full knowledge of Certificate Authority keys or encryption master keys. This should be achieved by separation of duties or dual control or by other appropriate means (e.g. by storing the keys in tamper proof modules).

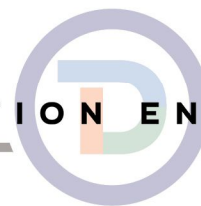
3.2.7.4 File and Drive Encryption

1. Encrypt laptop hard drives using minimum of AES 128-bit encryption.
2. Encrypt protected data within directories utilizing enterprise EFS technologies leveraging a PKI infrastructure. Using EFS in this manner will ensure integrity and confidentiality controls and protect against data disclosure and misuse.
3. Mobile Devices (mobile phones, smartphones and tablets) should support local encryption controls.

3.2.8 Logging & Monitoring

3.2.8.1 Overview

All information assets should, according to asset criticality, generate audit logs regarding user activities, administrator activities, exceptions, system faults, and information security events. Such logs, which are Diversified Information Assets themselves, should be transmitted to a secured central logging facility.



3.2.8.2 Audit Logs, Review and Alerts

1. All Diversified production systems that handle sensitive or critical Diversified data should generate logs.
2. Network traffic, both internal and external, should be logged and monitored for unusual activity
3. Audit logs should record user activities, exceptions, and information security events. These logs should be kept for a minimum of 90 days online and one year offline to assist in future investigations. Logs should record for source of access, accessing user, date and time of access, success or failure, what was accessed and source computer name.
4. Results of the monitoring activities should be reviewed regularly. Logs for all system components should be reviewed daily and include those servers that perform security functions.
5. Alerts from logs should be configured by selecting meaningful security and performance logs, setting relevant thresholds for triggering alerts to reduce "excessive alerts". These logs and thresholds should be reviewed yearly or as required.
6. Monitoring systems such as IDS/IPS systems should be configured to send alerts to individuals authorized to respond to those alerts.
7. IDS/IPS Systems should be updated at least every (7) days to ensure current vulnerabilities and exploits are being monitored

3.2.8.3 Audit Security

1. All system logs should be securely transmitted and collected, protected and appropriately archived.
2. Secure audit trails so they cannot be altered, allowing only system controls (non-interactive system accounts) to modify those logs.
3. Backup locations of all logs should have appropriate ACL controls and encryption controls.

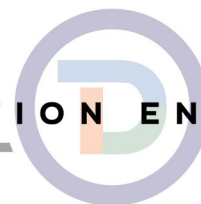
3.2.8.4 Security Testing

1. There should be an Annual Internal and External vulnerability scanning process that encompasses all networks and systems.
2. Significant changes to critical application and network with internet connectivity should require penetration tests with (12) months of initial change

3.2.9 Network Security

3.2.9.1 Overview

Network Security controls should be established that ensure and maintain confidentiality, integrity and availability of Diversified's network. Network and system security controls should be implemented as appropriate based on classification of the Information Assets being protected.



3.2.9.2 Network and System Documentation

1. A current network diagram with all connections to Protected Information, including any wireless networks, should be documented. This should include documentation and business justification for use of all services, protocols, and ports allowed.
2. Current documentation describing groups, roles, and responsibilities for logical management of network components should be maintained.
3. All connections between public and Diversified networks should be expressly authorized and registered.

3.2.9.3 DMZ

1. Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. Place externally-accessible servers within the DMZ.
2. Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content/production network.
3. All DMZ traffic should be monitored for unusual activity

3.2.9.4 Firewall

1. ICSA certified firewalls should be utilized at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. Firewall configurations should be used to restrict connections between untrusted networks and any system components in the data environment. This is to prohibit direct public access between the Internet and any system component in the protected environment.
2. Firewall rule sets and router rule sets should be reviewed at least every six months.
3. Deny all protocols by default and enable only specific permitted secure protocols. Restrict inbound and outbound traffic to that which is necessary. Document all access.
4. Internet access should be tracked at a minimum by user, sites visited and time.

3.2.9.5 Router/Switches

Port level access control should be implemented. All unused network ports should be disabled.

3.2.9.6 IDS/IPS

Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all network traffic at the perimeter of the data environment as well as inside of the data environment

3.2.9.7 Time Clocks

Time-synchronization technology (NTP) should be utilized to synchronize all critical system clocks.

3.2.9.8 Wireless

1. Wireless infrastructure should be implemented only by authorized personnel, should be fully documented and adhere to the wireless security standards.

2. Wireless infrastructure should encrypt all information while it is in transit over a wireless network.
3. Wireless implementations should incorporate the use of client-based authentication and should not use pre-shared keys where possible. If pre-shared keys are used, they should meet the same requirements as non-interactive service accounts (see section 1.3).
4. Wireless SSIDs should not identify the Diversified as the owner.

3.2.9.9 Security Banner

1. Prior to authentication, all systems should display an approved notification message that appears on the user's screen before granting access; Notification messages should be consistent with all applicable laws
2. Banners should include the following statements:
 - a. Unauthorized use is prohibited
 - b. Violators may be subject to civil and criminal prosecution
 - c. Use of the System is monitored and all access is logged
 - d. Usage of the system indicates consent to logging and monitoring

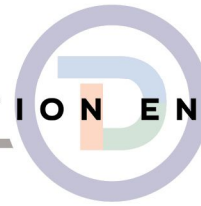
3.2.10 Platform Security

3.2.10.1 Overview

Operating systems of servers, databases, and all other systems should be properly configured and maintained in order to ensure the protection of information on those resources. IT Personnel should ensure that the computing environment is secure, patches are up to date and the machines are operated in a way to minimize the chance of a security breach. All servers, laptops and desktops should have end point security protections implemented to minimize risk of malware infections.

3.2.10.2 Malware and Host Base Firewalls

1. DMG pushes definition updates to the test devices for assessment before they are pushed to production. Those updates are observed by the trained Network Operations Center technicians who update the ticketing system with any issues. If no issues are observed or detected in the monitoring system, the updates are approved for production by the System Engineer.
2. Deploy anti-virus software on all systems. Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
3. A centralized anti-malware system should be implemented with quarantine controls, centralized client updating controls, and signature definition deployment processes.
4. Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet. This should also include application control functionality and host-based intrusion detection capabilities (HIDS).



5. Host-based firewall rule sets and malware detection processes should be reviewed at least every six months. All exceptions should receive security approval before implementation.
6. A standard security configuration for firewalls and anti-malware software should be defined for workstations and servers.

3.2 10.3 System Placement Controls

1. Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.
2. Segment systems dedicated to transfer files from systems that store or process content and from the non-production network
3. Sensitive systems should have a dedicated (isolated) computing environment. For example, the Root Certificate server for PKI.
4. All Productions systems should be scanned for vulnerabilities on a regular basis.

3.2 10.4 Back-up Controls

1. IT Operations should create backup copies of all data assets on a regular basis, based on business requirements. It should determine the frequency, operation time and storage locations based on the requirements for recovery in case of system or disk outage, or a disaster.
2. Backup/Copies of data should be accorded the same level of security and controls as the original data Store media backups in a secure location, preferably an off-site facility. Secure backups of network infrastructure devices to a centrally secured server.
3. All backup media should be encrypted.

3.2 10.5 Mobile devices

In addition to the standard controls, Mobile Devices that are not owned by Diversified and are used to connect to a Diversified Information Asset and store such data should comply with the listed controls for accessing information assets and have the capability of being "remotely wiped."

3.2.11 Physical Security

3.2 11.1 Overview

This control addresses threats to critical IT resources that result from unauthorized access to facilities owned or leased by Diversified including offices, data centers and similar facilities that are used to house such resources.

3.2 11.2 Physical Access

1. Visitor tags should be utilized to easily distinguish between onsite personnel, vendors, and visitors, especially in areas where Protected Information is accessible.

2. Employee tags should have photo identification that is validated and required to be visible at all times.
3. A visitor log should be maintained in order to keep a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law. Validate that the user is who he or she claims to be (request review of driver license).
4. Visitors should not be provided with electronic access to content/production areas.
5. All lost tags should be immediately reported.

3.2 11.3 Physical Controls

1. Information assets should be physically and logically secured and safeguarded at all times (e.g., locked doors, locked cabinets, fire suppression, and security guards, password protected, encrypted, access controls, etc.)
2. Equipment rooms housing servers, routers, communication lines, etc., should be secure from unauthorized access.
3. Access to equipment rooms housing servers, routers, gateways, consoles, communication lines, etc., should be logged and routinely reviewed.
4. Implement electronic access throughout each Facility to cover all entry/exit points. Lock all entry/exit points at all times if the Facility does not have a segregated access-controlled area beyond reception.
5. Install a centralized, audible alarm system that covers all entry/exit points. Test the alarm system every six (6) months.
6. Review the list of users who can arm and disarm alarm systems annually. Each user who has access to the alarm system should be assigned a unique identifier.
7. Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store feeds for at least three months, unless otherwise restricted by law. Restrict physical and logical access to the CCTV console and to CCTV equipment
8. Store media backups in a secure location. Maintain strict control over the storage and accessibility of media.
9. Limit the distribution of master keys (physical) to authorized personnel. All master keys should be tagged and access to their keys should be documented. Master key access should be reviewed quarterly.

3.2 11.4 Emergency Management Controls

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. Install a power backup system.

3.2 11.5 Receiving and Shipping

1. Track and log asset shipping details including media sent by secured courier.

2. Validate assets leaving the Facility against a valid work/shipping order. Ship all assets in closed/sealed containers and, if sensitive, use tamper evidence tape or packaging seals (holograms).
3. Inspect delivered content upon receipt and compare to shipping documents. Inspect delivered content upon receipt and compare to shipping documents.

3.2.11.6 Physical Media Controls

1. Store media backups in a secure location. Maintain strict control over the storage and accessibility of media.
2. Ensure management approves any and all media that is moved from a secured area.

3.2.11.7 Offsite and Secure Area Controls

1. Equipment should be sited or protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access. Review of secure areas should be conducted yearly.
2. Control access to production areas by segregating the content/production area from other facility areas. Review access to restricted areas quarterly
3. Restrict physical access to publicly accessible network jacks. Enable port security if public access is required.
4. Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises

3.2.12 Risk Assessments

3.2.12.1 Overview

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. This includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.

3.2.12.2 Assessing Security Risks

1. Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. These risks should be maintained and tracked using a risk registry.
2. Review and assess a workflow that identifies, implements, and assesses the effectiveness of key controls.
3. All security recommendations should be categorized as risk acceptance, risk mitigation, risk transference, or risk avoidance. All recommendations should be formally acknowledged by the business owner.

3.2.12.3 Security Testing

1. Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

2. Run internal network vulnerability scans at least quarterly and after any significant change in the network. Run external vulnerability scans at least monthly and after any significant change in the network.
3. Perform external and internal penetration testing at least once a year.
4. Perform vulnerability and security testing of systems and applications before deployment to production systems.

3.2.13 Security Awareness

3.2.13.1 Overview

This control addresses the guideline for an Information Security Training and Awareness Program

3.2.13.2 Security Awareness

An Information security training process should be created.

1. All personnel should go through the security awareness program yearly and understand the importance of protected data security and security principles.
2. Users should acknowledge receipt and understanding of security policy.
3. Users should be tested after going through the security awareness program.
4. The security awareness program should be updated yearly.
5. A monthly security awareness email should be sent out to the organization and read by all Users.
6. Appropriate User awareness procedures should be implemented in respect to security incident escalation from employees and contractors.

3.2.14 External Party Management

3.2.14.1 Overview

External Parties doing business with the Diversified, such as contractors, consultants, vendors, suppliers, business partners, service providers, and sponsors. External Parties are a vital resource in the Diversified's quest to achieve its organizational goals but introduce additional risks to confidentiality, integrity, and availability of Diversified Information. The objective of this control is to properly address that risk by identifying, quantifying, and managing these risks throughout the lifecycle of each External Party relationship.

3.2.14.2 Confidentiality Agreements

All company personnel and External Party workers should be required to sign a confidentiality agreement or a non-disclosure agreement. All External Party workers who handle company content should sign confidentiality agreements.

3.2 14.3 Service Provider Agreements

Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of Protected Information the service providers possess, such as cardholder data.

3.2 14.4 Contracts and SLA Review

1. The Technology Management should ensure there is an established process for engaging service providers, including proper due diligence prior to engagement.
2. Technology Management should ensure that all relevant security controls, service definitions, and delivery levels are included in the External Party service delivery agreement and that they are implemented, operated, and maintained by the External Party. All security requirements should be included in External Party contracts, including provisions that allow the Diversified to monitor and check compliance to the required security controls.
3. The services, reports and records provided by the External Party should be regularly monitored and reviewed, and audits should be carried out regularly.

3.2 14.5 3rd Party requirements

1. A list of service providers should be maintained by asset management, business units, and vendor management.
2. All External Party workers should be bonded and insured where appropriate.
3. As a condition of gaining access to Diversified IT Systems, every third party should secure its own connected systems and network in a manner consistent with Diversified security requirements.
4. The establishment of a direct connection (e.g. VPN tunnels) between Diversified systems and computers at external organizations, vendors or customers via the Internet or any other public network, is prohibited unless this connection has first been risk assessed by Information Technology, and appropriate control mechanisms are employed.
5. Diversified will complete any required reviews to verify these requirements.

3.2.15 Disaster Recovery and Business Continuity

3.2 15.1 Overview

The purpose of this control is to set forth standards and guidelines for developing, implementing, and maintaining both business processes (business continuity) and technology processes (disaster recovery) that ensure the Diversified's continued operations during emergencies ("Crises") that adversely affect business services due to natural and/or manmade events

3.2 15.2 Business Impact Analysis

1. Diversified should develop and maintain a Business Impact Analysis Process to identify and document critical and important business processes, identify as many potential

events (Crises) as possible that can cause interruptions to those processes, and document and analyze the estimated probability, likelihood, and impact (including information security-related consequences) of each such event.

2. All Key departments should define their business critical activities, processes and technology applications
3. Results of the Business Impact Analysis should be reviewed and assigned to individuals with the necessary skills to ensure that gaps, potential threats and vulnerabilities are identified and assessed.
4. Any results of the Business Impact Analysis that required review and assignment should be followed up on with the group in within six months to ensure progress is made at addressing any outstanding issues.

3.2 15.3 Business Continuity

Each department/business unit should have its own Business Continuity Plan that defines business processes for response to each potential Crisis identified and analyzed in the Business Impact Analysis Process. Each Business Continuity Plan should include, but is not limited to:

1. Detailed contact information for all individuals responsible for management of any aspect of the Plan, including authorized third parties (emergency management personnel, local authorities, etc.).
2. BCP should address each department's plan in the event there is an unavailability of up to 50% of critical employees and/or third parties, during a large scale absentee scenario.
3. Responsible party should be trained on the BCP annually and should content active or passive test of their role as part of the annual testing prescribed in this control.
4. Critical business processes.
 - a. Procedures to restore those processes, including, but not limited to, communication plans, personnel responsibilities, and alternate locations.
 - b. Workaround procedures.
 - c. Description of the technology required for successful process restoration.
5. Plan review by each Department/Business Unit annually
6. Review and Approval by Senior Management annually or in conjunction with changes to underlying technology or processes.
7. The Business Continuity Plan should be tested no less than once every twelve (12) months and issues should be documented and addressed by appropriate individuals with skillset to remedy.

3.2 15.4 Disaster Recovery

The Information Technology Department should coordinate the development, maintenance, and testing of a centralized Disaster Recovery Plan that defines technology processes to support all of the Business Continuity Plans. The Disaster Recovery Plan should include, but is not limited to, the following:

1. Detailed contact information for all individuals responsible for management of any aspect of the Plan, including authorized third parties (emergency management personnel, local authorities, etc.).
2. Communication plans and personnel responsibilities.
3. Descriptions of alternate locations and their usage.
4. A list of Information Assets, prioritized by criticality based on the associated business processes.
5. For each Information Asset:
 - a. System and data restoration procedures, taking into account potential Crises previously identified.
 - b. Estimated time required for full restoration.
 - i. Ensure restoration time are in accordance with any contract requirements
 - c. The time at which non-operation or impaired operation of the Information Asset begins to have measurable impact to the Diversified's operations.
 - d. Specific testing plans, including a schedule, planning, and post-test review, to ensure the Disaster Recovery Plan is fully effective in meeting the needs of the Business Continuity Plans.
 - e. Plan review to be performed annually
 - f. The Disaster Recovery Plan should be tested no less than once every twelve (12) months
 - g. The DR Plan should ensure that RPO/RT0 are met.

3.2.16 Incident Management

3.2.16.1 Overview

The purpose of this control is for reporting and managing

- Security incidents affecting Diversified's information and IT systems
- Information Loss
- Outage of critical system
- Physical intrusion
- Near misses and information security concerns (including virus threats)

Everyone has an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security Business Impact Analysis.

3.2.16.2 Security incident Examples

An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of Diversified information in any format. Examples of information security incidents can include but are not limited to:

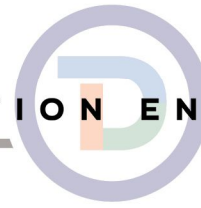
- The disclosure of confidential information to unauthorized individuals
- Loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored
- Inappropriate access controls allowing unauthorized use of information
- Suspected breach of the University IT and communications use policy
- Attempts to gain unauthorized access to computer systems, e, g hacking
- Records altered or deleted without authorization by the data "owner"
- Virus or other security attack on IT equipment systems or networks
- Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area
- Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information.
- Covert or unauthorized recording of meetings and presentations
- Issue that causes a Diversified Critical system to be offline to either Internal Diversified resources or external client resources

3.2.16.3 Reporting and Resolution of Incidents

1. All incidents or suspected incidents should be logged into the corporate incident tracking system or reported to Diversified Internal NOC
2. Diversified will notify any critical parties, including Clients about an incident
3. Incident tracking ticket should be escalated to Diversified Security Team for further review and response.
4. Any compromised system found should be immediately isolated from the corporate network
5. Root Cause Analysis should be generated to understand why issue occurred and recommend steps to prevent similar occurrences within 7 days of resolution of issue

3.2.16.4 Review Organization Response

1. At least annually, a test should be performed to assess the organization response to a supposed incident. (An actual or suspect incident response can be reviewed in lieu of performing a separate test)
2. Identify any deficiencies or areas in need of improvement
3. Determine risks associated with findings
4. Remediate any discovered vulnerabilities in accordance with the risk in a timely manner
5. Document test, findings, risks and remediation



4 Appendix A: Glossary of Terms

The following terms, as maintained in the Diversified Policy Document Template, may be used in this policy and other Diversified documents. If a definition below differs from the equivalent definition in the current version of the Diversified Policy Document Template, the definition in the Diversified Policy Document Template shall control. Terms marked with * are reprints from the source indicated in parentheses.

Access Control – The process of authorizing, enabling, disabling, and monitoring the ability of an individual, process, or service to access a defined physical or logical area, system, or service.

Application Custodian – The individual or group to which an Application Owner has legitimately designated some or all Application Owner responsibilities specific to a software application.

Application Owner – The individual or group to which specific management and operational responsibilities for a software application has been assigned.

Artifact - The remnants of an intruder attack or incident activity. This could be software used by intruder(s), a collection of tools, malicious code, logs, files, output from tools, or status of a system after an attack or intrusion.

Asset - Anything owned by the Diversified that has value to the Diversified.

Availability – The property of being accessible and usable upon demand by an authorized entity.

Business Continuity – The ability of an organization to continue operations, from a business process perspective, during and after Crises or events that adversely affect the organization’s ability to do so.

Change – Any modification to the configuration and/or operational status of an Information Asset in a test/staging or production environment, including, but not limited to:

- Any modification to hardware or software configuration of any kind.
- Installation or removal of software packages or updates.
- Hardware repair/replacement.
- Implementation of a new Information Asset or significant change to an existing Information Asset, using the Implementation phase of the Information System Lifecycle Process.

A modification to an environmental system (HVAC, water, electric, fire suppression, physical access, etc.) that directly or indirectly affects the operational status of an Information Asset.

Charter – A document issued by an authority establishing and defining an organization subsidiary to that authority. Most commonly used in the Diversified to establish and define committees.

Confidentiality– The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Crisis – An event that adversely affects business services due to natural and/or manmade events.

Data Custodian – The individual or group to which a Data Owner has legitimately designated some or all Data Owner responsibilities specific to a set of Information.

Data Owner – The individual or group to which specific management and operational responsibilities for a specific set of Information has been assigned.

Disaster Recovery – The ability of an organization to resume and/or continue operations, from a technology perspective, during and after Crises or events that adversely affect the organization’s ability to do so.

Diversified – Is the professional organization Diversified.

Document Owner – The individual who is directly responsible for the development, implementation, and maintenance of a document.

Event - An observable occurrence; an aspect of an investigation that can be verified and analyzed.

Evidence - Data on which to base proof or to establish a truth or falsehood.

External Party – An individual, group, or organization that is NOT a Diversified employee, group, or Diversified and has a relationship with the Diversified. An External Party may be, but is not limited to, a contractor, consultant, vendor, supplier, business partner, service provider, and/or sponsor. Includes “Customer” and “Vendor” as defined in the Diversified Contract Policy.

Forensic Analysis - Examination of material to determine its features and relationships in an effort to discover evidence that will be admissible in disciplinary or legal proceedings.

Guideline – A statement of something that should be done; a best practice but not a mandatory requirement. Usually includes the word “should.”

Information – Data that is endowed with meaning and Overview that is the property of the Diversified and is of value to the Diversified, including, but not limited to:

- Strategic information
- Business plans
- Financial data and information, including financial models and operating results
- New products or services
- Computer programs
- Mathematical proofs, derivations, and models
- Statistical methods and analyses
- Operational research models
- Passwords
- Payroll and compensation data
- Specific information (playbook contents, game and player statistics, video, etc.)

Information Asset – Diversified Information (as defined above) or a computerized system storing, transmitting, and/or processing same. Such systems may include, but are not limited to:

- Endpoints (desktop PC, laptops, tablets, and smartphones)
- Servers
- Networking infrastructure, such as routers, switches, and wireless access points
- Internal and external software applications, including email
- Operating systems
- Storage media, such as hard drives, USB flash drives, and writable CDs

This term may also be used for a collection of such systems performing a common function.

Information Classification – The assignment of a level of sensitivity to information that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as information is created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the Diversified.

Information Security – Preservation of confidentiality, integrity, and availability of information.

Information Security Governance - The process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.

Information Security Incident – A single or a series of unwanted information security events that have a significant probability of compromising business operations and threatening information security.

Information Security Management System (ISMS) – That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

Integrity – The property of safeguarding the accuracy and completeness of assets.

Mobile Code) - Software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is associated with a number of middleware services.

Mobile Device – A portable device (a cellular phone, smartphone, tablet, or similar device) that is used to access a Diversified Information Asset and/or store Diversified Information.

Payment Card – An instrument used in lieu of cash in the form of a credit, debit or charge card.

Payment Card Industry Data Security Standards (PCI DSS) – Data security standards developed by the major payment card companies (Visa, MasterCard, Discover, American Express and JCB) as a guideline to help organizations that process card payments prevent fraud, hacking and various other security vulnerabilities and threats.

Payment Application Data Security Standards (PA DSS) - Data security standards developed under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP) as a guideline for software vendors and other develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS

Payment Card Merchant - A department or other entity which processes payment card transactions.

Payment Gateway - Facilitates the transfer of payment card transaction information between a payment portal (such as a website) and the acquiring bank.

Policy – A document that articulates management’s vision and direction in a particular area by formally stating one or more Standards or Guidelines.

Privileged Access – The right to access and/or modify some or all administrative aspects of an Information Asset.

Procedure – A document containing step-by-step instructions for how to execute part or all of a Process.

Process – A document containing high-level instructions for how to put one or more Standards or Guidelines from a Policy into practice. Equivalent to “operating procedures” as defined in ISO 27001.

Standard – A statement of something that must be done; a mandatory non-negotiable requirement. Usually includes the word “must.”

System Custodian – The individual or group to which a System Owner has legitimately designated some or all System Owner responsibilities specific to the hardware and operating system of an information system.

System Owner – The individual or group to which specific management and operational responsibilities for the hardware and operating system of an information system has been assigned.

User – Any end user of an Diversified Information Asset, including, but not limited to, full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to an Information Asset.

Threat - A potential cause of an unwanted incident, which may result in harm to a system or the organization.

STATE OF ALABAMA



LICENSE NO.: S- 54068
TYPE: NEW

BID LIMIT:
AMOUNT:

State Licensing Board for General Contractors

THIS IS TO CERTIFY THAT

ONE DIVERSIFIED LLC

NORCROSS, GA. 30071

is hereby licensed a General Contractor in the State of Alabama and is authorized to perform the following type(s) of work:

SUBCONTRACTOR: LOW VOLTAGE

until May 31, 2020 when this Certificate expires.

Witness our hands and seal of the Board, dated Montgomery, Ala.,

19th day of June, 2019

SECRETARY-TREASURER

CHAIRMAN

Max N. Long

Alley Whaley

153088

State of Arkansas
Commercial Contractors Licensing Board

ONE DIVERSIFIED, LLC, D/B/A DIVERSIFIEDUS LLC
37 MARKET ST
KENILWORTH, NJ 07033

ONE DIVERSIFIED, LLC, D/B/A DIVERSIFIEDUS LLC

This is to Certify That

_____ is duly licensed under the provisions of Ark. Code Ann. § 17-25-101 et. seq. as amended and is entitled to practice Contracting in the State of Arkansas within the following classifications/specialties:

SPECIALTY

Communication, Computer or Sound Systems, Cabling

This contractor has an unlimited suggested bid limit.

from June 25, 2021 **until** June 30, 2022 **when this Certificate expires.**

Witness our hands of the Board, dated at North Little Rock, Arkansas:



[Handwritten Signature]

CHAIRMAN

[Handwritten Signature]

SECRETARY

June 25, 2021 - dsa

ARLINGTON COUNTY, VIRGINIA
2100 Clarendon Boulevard, Suite 200, Arlington, VA 22201

Business License Tax Certificate

ONE DIVERSIFIED LLC

Account #: BLC-1001167125-02

Trade Name:

Location Address:
2975 NORTHWOODS PARKWAY
NORCROSS, GA

Classification:
57.B, Specialized
64, Contractors



2020

Ingrid H. Morroy
COMMISSIONER OF REVENUE

Carla de la Pava
TREASURER

ROBERT TURNER
ONE DIVERSIFIED LLC
2975 NORTHWOODS PARKWAY
NORCROSS GA



CONTRACTORS STATE LICENSE BOARD

Pursuant to Chapter 9 of Division 3 of the Business and Professions Code
and the Rules and Regulations of the Contractors State License Board,
the Registrar of Contractors does hereby issue this license to:

ONE DIVERSIFIED LLC

License Number 1030361

to engage in the business or act in the capacity of a contractor in the following classifications:

C-7 - LOW VOLTAGE SYSTEMS

Witness my hand and seal this day,

October 23, 2019

Issued August 24, 2017

CERTIFIED COPY

Johnny Simpson, Board Chair

Handwritten signature of Johnny Simpson in black ink.

This license is the property of the Registrar of Contractors,
is not transferable, and shall be returned to the Registrar
upon demand when suspended, revoked, or invalidated
for any reason. It becomes void if not renewed.

David R. Fogt, Registrar of Contractors

Handwritten signature of David R. Fogt in black ink.



2" %3' , 55ž , 9f12* , 2

\$, * , 5ž , * , ~ , ž fl) '3fl~ 2fl15' 2<



STATE OF FLORIDA
DEPARTMENT OF BUSINESS AND PROFESSIONAL REGULATION
ELECTRICAL CONTRACTORS LICENSING BOARD

5ž fl~3/fl~ " . &5< fl&fl~ 52" . & , * 52 . ~ 5 , 2ž fl2fl" * "3~ fl25"1 "fV ~7 * / fl2~5ž fl
/2, 9"3" , * 3' , 1~ž . /5fl2 . 1 & , 2"/ . 35 . 57 5fl3

WEBER, STEVEN MARC

* fl~ "9fl23"1 "fV ~&&
/ flf12~ 2fl35~& . * fl
527 339" &&fl . &

LICENSE NUMBER: ES12001001

EXPIRATION DATE: AUGUST 31, 2020

· f >%L~\$#~ \$L~%o%o ~ S-L~>") # , ` \$!>&&B L~%oB, }



/ , ~ , " > " L ~ " p%h, Bÿ} L ~ " s ~ ~ \$N ~ }

5pS%&%, Ÿ~ \$L~%o " " " \$%~ ~ >£ N~ " ~ >~\$, ~L, "pL ~ " p>~ " pL ~ \$L~%d , "Ÿ%o " pS%h, Bÿ} L ~ "



**CONTRACTOR REGISTRATION
CERTIFICATE**

**STATE OF IOWA
DIVISION OF LABOR**

150 Des Moines St, Des Moines, IA 50309
Phone: 515-242-5871 | FAX: 515-725-2427

www.iowacontractor.gov | contractor.registration@iwd.iowa.gov

DATE ISSUED:
01/26/2022

DATE EXPIRES:
01/23/2023

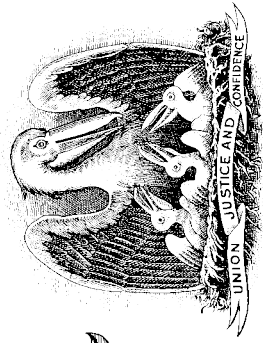
REGISTRATION NUMBER:
C132728

ONE DIVERSIFIED LLC
37 MARKET ST BLDG
KENILWORTH, NJ 07033

A handwritten signature in black ink that reads "Rod A. Roberts".

Rod A. Roberts, Labor Commissioner

State of Louisiana



State Licensing Board for Contractors

This is to Certify that:

ONE DIVERSIFIED, LLC
37 Market Street
Kenilworth, NJ 07033

is duly licensed and entitled to practice the following classifications

SPECIALTY: TELECOMMUNICATIONS (EXCLUDING PROPERTY PROTECTION AND LIFE SAFETY SYSTEMS)



Expiration Date March 28, 2024

License No 64840

Witness our hand and seal of the Board dated,
Baton Rouge, LA 14th **day of** December 2021

Will B. McCoy

Director

Lee Mallett

Chairman

Andy Hume

Treasurer

This License Is Not Transferable

90 County

State of Maryland License

03323578

03124343

14227392



ONE DIVERSIFIED LLC
2975 NORTHWOOD PKWY
NORCROSS GA 30071

ONE DIVERSIFIED LLC
2975 NORTHWOOD PKWY
NORCROSS GA 30071

18

CODE	UNIT	TYPE OF LICENSE	NO OF LIC	COST
66	060	OUT-OF-STATE CONTRACTOR	1	60.00

DATE OF ISSUE
MO DAY YR
05/02/2018

MONTHS PAID
12

ISSUING FEES	2.00		
TOTAL	62.00	AMOUNT PAID	62.00

**THIS LICENSE MUST BE PUBLICLY DISPLAYED
AND EXPIRES ON APRIL 30, 2019**

ISSUED BY

JULIE L. ENSOR, CLERK OF CIRCUIT COURT
P.O. Box 6754
TOWSON, MARYLAND 21285-6754 (410)887-2607

CBT

State of Mississippi

BOARD OF CONTRACTORS

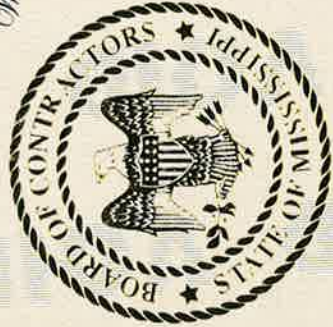
ONE DIVERSIFIED, LLC
37 MARKET STREET
KENILOWRTH, NJ 07033

ACTIVE

is duly registered and entitled to perform

INSTALLATION OF ELECTRONIC VIDEO EQUIP.

We have herewith set our hand and caused the Seal of the Mississippi Board of Contractors to be affixed this 9 day of Apr., 2021



CERTIFICATE OF RESPONSIBILITY

No. 14767-SC

Expires Apr. 9, 2022

Joel A. Canall,

CHAIRMAN OF THE BOARD



STATE OF NEVADA CONTRACTOR'S LICENSE

THIS IS TO CERTIFY THAT THE COMPANY OR PERSON LISTED BELOW IS
LICENSED IN THE STATE OF NEVADA FOR THE CLASSIFICATION(S) SHOWN

LICENSE#: **0082969** EXPIRES: **11/30/2023**

ONE DIVERSIFIED LLC
37 MARKET ST
KENILWORTH, NJ 07033

LIMIT: **Unlimited**
CLASS: **C-2D**

Southern Nevada Office
2310 Corporate Circle, Suite 200
Henderson, Nevada 89074
(702) 486-1100

Northern Nevada Office
5390 Kietzke Lane, Suite 102
Reno, Nevada 89511
(775) 688-1141

STATE CONTRACTORS BOARD

The Nevada State Contractors Board certifies that

ONE DIVERSIFIED LLC

Licensed since November 22, 2017

License No. **0082969**

Is duly licensed as a contractor in the following classification(s):

PRINCIPALS:

DISTINCT HOLDINGS INC, Managing
Member
ALFRED D'ALESSANDRO, Other
MICHAEL MCKEE, QI

C-2D Low Voltage

LIMIT: Unlimited
EXPIRES: 11/30/2023





Chair, Nevada State Contractors Board

State of North Dakota

SECRETARY OF STATE



CONTRACTOR LICENSE

NO: 000046103

CLASS: A

The undersigned, as Secretary of State of the state of North Dakota and Registrar of Contractors, certifies that **ONE DIVERSIFIED, LLC** whose address is in KENILWORTH, NJ, has filed in this office proper documents for a Contractor License valid until March 1, 2023, and has complied with all requirements of North Dakota Century Code, chapter 43-07.

ONE DIVERSIFIED, LLC is entitled to bid on and accept contracts as authorized by law under this license without limit as to the value of any single contract project.

Dated: January 11, 2022

A handwritten signature in black ink, reading "Alvin A. Jaeger".

Alvin A. Jaeger
Secretary of State

The North Dakota Secretary of State verifies that:

ONE DIVERSIFIED, LLC

is the holder of a North Dakota Class A Contractor License which is in force until March 1, 2023 unless sooner suspended or revoked as provided by NDCC 43-07.

License # 000046103

000222

ONE DIVERSIFIED LLC
37 MARKET ST
KENILWORTH NJ 07033

CONSTRUCTION CONTRACTORS BOARD
LICENSE CERTIFICATE

LICENSE NUMBER: 213697
EXPIRATION DATE: 01/19/2024
ENTITY TYPE: Limited Liability

CONSTRUCTION CONTRACTORS BOARD
LICENSE CERTIFICATE

ONE DIVERSIFIED LLC
37 MARKET ST
KENILWORTH NJ 07033



⇐ ⇐ ⇐ ⇐
POCKET CARD
⇐ ⇐ ⇐ ⇐

*fold and detach
along
perforation*

↓ ↓ ↓ ↓ ↓
LICENSE CARD
↓ ↓ ↓ ↓ ↓

STATE OF OREGON
CONSTRUCTION CONTRACTORS BOARD
LICENSE CERTIFICATE

This document certifies that:

ONE DIVERSIFIED LLC
37 MARKET ST
KENILWORTH NJ 07033



LICENSE NUMBER: 213697

EXPIRATION DATE: 01/19/2024

is licensed in accordance with Oregon Law as
Commercial Specialty Contractor Level 2

ENTITY TYPE: Limited Liability Company



Office of the Secretary of State

Certificate of Fact

The undersigned, as Secretary of State of Texas, does hereby certify that the document, Application for Registration for One Diversified, LLC, authorized under the name TIDiversified, LLC (file number 802512883), a GEORGIA, USA, Foreign Limited Liability Company (LLC), was filed in this office on August 03, 2016.

It is further certified that the entity status in Texas is in existence.

Delayed Effective date: August 04, 2016

In testimony whereof, I have hereunto signed my name officially and caused to be impressed hereon the Seal of State at my office in Austin, Texas on June 25, 2020.



A handwritten signature in black ink, appearing to read "Ruth R. Hughs".

Ruth R. Hughs
Secretary of State

COMMONWEALTH of VIRGINIA

Department of Professional and Occupational Regulation

9960 Mayland Drive, Suite 400, Richmond, VA 23233

Telephone: (804) 367-8500

EXPIRES ON

04-30-2022

NUMBER

2705152777



ONE DIVERSIFIED LLC
37 MARKET ST
KENILWORTH, NJ 07033

BOARD FOR CONTRACTORS
CLASS A CONTRACTOR
CLASSIFICATIONS ELE



Maury Brown
Maury Brown, Director

Status can be verified at <http://www.dpor.virginia.gov>

DPOR-LIC (02/2017)

(DETACH HERE)



COMMONWEALTH of VIRGINIA
Department of Professional and Occupational Regulation

CLASS A BOARD FOR CONTRACTORS
CONTRACTOR

CLASSIFICATIONS ELE
NUMBER: 2705152777 EXPIRES: 04-30-2022

ONE DIVERSIFIED LLC
37 MARKET ST
KENILWORTH, NJ 07033



(FOLD)

Status can be verified at <http://www.dpor.virginia.gov>

DPOR-PC (02/2017)

Department of Labor and Industries
PO Box 44450
Olympia, WA 98504-4450

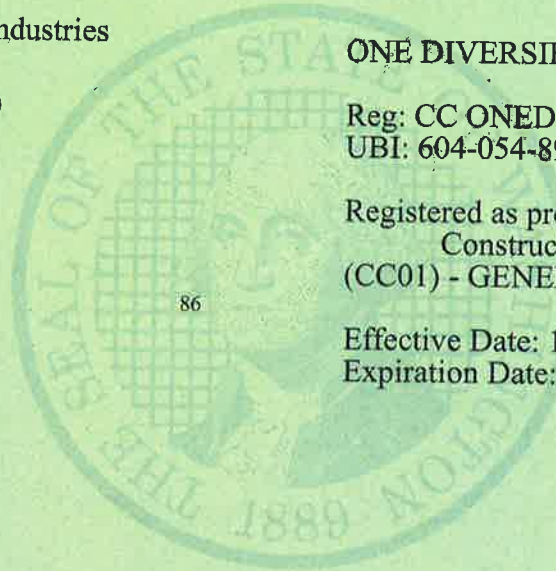
ONE DIVERSIFIED LLC
37 MARKET STREET
KENILWORTH NJ 07033

ONE DIVERSIFIED LLC

Reg: CC ONEDIDL839CG
UBI: 604-054-892

Registered as provided by Law as:
Construction Contractor
(CC01) - GENERAL

Effective Date: 11/2/2017
Expiration Date: 11/2/2021



PROPOSAL FORM 4: CLEAN AIR WATER ACT

I, the Vendor, am in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the Enforcement.

Potential Vendor: One Diversified, LLC

Title of Authorized Representative: Tracie Lee, Business Development Representative

Mailing Address: 37 Market Street Kenilworth, NJ 07033

Signature: _____

PROPOSAL FORM 5: DEBARMENT NOTICE

I, the Vendor, certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, "Debarment and Suspension", as described in the Federal Register and Rules and Regulations.

Potential Vendor: One Diversified, LLC

Title of Authorized Representative: Tracie Lee, Business Development Representative

Mailing Address: 37 Market Street Kenilworth, NJ 07033

Signature: _____

PROPOSAL FORM 6: 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 \$10,000 and not more than \$100,000 for each such failure.

The undersigned certifies, to the best of his/her knowledge and belief, 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 \$100,000 in Federal funds at all appropriate tiers and that all sub-recipients shall certify and disclose accordingly.

Signature of Respondent

March 9, 2022

Date

PROPOSAL FORM 7: CONTRACTOR CERTIFICATION REQUIREMENTS

Contractor's Employment Eligibility

By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statutes of the states it will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The Respondent complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.

Contractor shall comply with governing board policy of the Region 10 ESC Participating entities in which work is being performed.

Fingerprint & Criminal Background Checks

If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

The Respondent shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed.

Signature of Respondent

March 9, 2022
Date

**PROPOSAL FORM 8: ANTITRUST CERTIFICATION STATEMENTS
(Tex. Government Code § 2155.005)**

I affirm under penalty of perjury of the laws of the State of Texas that:

- (1) I am duly authorized to execute this contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;
- (2) In connection with this proposal, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;
- (3) In connection with this proposal, neither I nor any representative of the Company has violated any federal antitrust law; and
- (4) Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this proposal to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.

VENDOR One Diversified, LLC

**ADDRESS: 4 Market Street
Kenilworth, New Jersey 07033**

PHONE _____

FAX _____

RESPONDANT

Signature

Printed Name

Position with Company

AUTHORIZING OFFICIAL

Signature

Printed Name

Position with Company

PROPOSAL FORM 9: IMPLEMENTATION OF HOUSE BILL 1295

Certificate of Interested Parties (Form 1295):

In 2015, the Texas Legislature adopted House Bill 1295, which added section 2252.908 of the Government Code. The law states that a governmental entity or state agency may not enter into certain contracts with a business entity unless the business entity submits a disclosure of interested parties to the governmental entity or state agency at the time the business entity submits the signed contract to the governmental entity or state agency. The law applies only to a contract of a governmental entity or state agency that either (1) requires an action or vote by the governing body of the entity or agency before the contract may be signed or (2) has a value of at least \$1 million. The disclosure requirement applies to a contract entered into on or after January 1, 2016.

The Texas Ethics Commission was required to adopt rules necessary to implement that law, prescribe the disclosure of interested parties form, and post a copy of the form on the commission's website. The commission adopted the Certificate of Interested Parties form (Form 1295) on October 5, 2015. The commission also adopted new rules (Chapter 46) on November 30, 2015, to implement the law. The commission does not have any additional authority to enforce or interpret House Bill 1295.

Filing Process:

Starting on January 1, 2016, the commission will make available on its website a new filing application that must be used to file Form 1295. A business entity must use the application to enter the required information on Form 1295 and print a copy of the completed form, which will include a certification of filing that will contain a unique certification number. An authorized agent of the business entity must sign the printed copy of the form and have the form notarized. The completed Form 1295 with the certification of filing must be filed with the governmental body or state agency with which the business entity is entering into the contract.

The governmental entity or state agency must notify the commission, using the commission's filing application, of the receipt of the filed Form 1295 with the certification of filing not later than the 30th day after the date the contract binds all parties to the contract. The commission will post the completed Form 1295 to its website within seven business days after receiving notice from the governmental entity or state agency.

Information regarding how to use the filing application will be available on this site starting on January 1, 2016. https://www.ethics.state.tx.us/whatsnew/elf_info_form1295.htm

BOYCOTT CERTIFICATION

Respondents 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.

Does vendor agree? _____
(Initials of Authorized Representative)

TERRORIST STATE CERTIFICATION

In accordance with Texas Government Code, Chapter 2252, Subchapter F, REGION 10 ESC is prohibited from entering into a contract with a company that is identified on a list prepared and maintained by the Texas Comptroller or the State Pension Review Board under Texas Government Code Sections 806.051, 807.051, or 2252.153. By execution of any agreement, the respondent certifies to REGION 10 ESC that it is not a listed company under any of those Texas Government Code provisions. Responders must voluntarily and knowingly acknowledge and agree that any agreement shall be null and void should facts arise leading the REGION 10 ESC to believe that the respondent was a listed company at the time of this procurement.

Does vendor agree? _____
(Initials of Authorized Representative)

PROPOSAL FORM 11: RESIDENT CERTIFICATION

This Certification Section must be completed and submitted before a proposal can be awarded to your company. This information may be placed in an envelope labeled "Proprietary" and is not subject to public view. In order for a proposal to be considered, the following information must be provided. Failure to complete may result in rejection of the proposal:

As defined by Texas House Bill 602, a "nonresident Bidder" means a Bidder whose principal place of business is not in Texas, but excludes a contractor whose ultimate parent company or majority owner has its principal place of business in Texas.

Texas or Non-Texas Resident

- I certify that my company is a **"resident Bidder"**
- I certify that my company qualifies as a **"nonresident Bidder"**

If you qualify as a "nonresident Bidder," you must furnish the following information:

What is your resident state? (The state your principal place of business is located.)

One Diversified, LLC 37 Market Street Kenilworth, New Jersey 07033

Name	Address	Company
State		City
Zip		

PROPOSAL FORM 1 2: FEDERAL FUNDS CERIFICATION FORM

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 Vendors submitting proposals must complete this Federal Funds Certification Form regarding Vendor’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 participating agencies for their use while considering their purchasing options when using federal grant funds. Participating agencies may also require Vendors 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, Vendor should certify Vendor’s agreement and ability to comply, where applicable, by having Vendor’s authorized representative complete and initial the applicable lines after each section and sign the acknowledgment at the end of this form. If a vendor fails to complete any item in this form, Region 10 ESC will consider the Vendor’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 Vendor using federal funds.

1. Vendor Violation or Breach of Contract Terms:

Contracts for more than the simplified acquisition threshold currently set at \$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 contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

Any Contract award will be subject to Region 10 ESC General Terms and Conditions, as well as any additional terms and conditions in any Purchase Order, participating agency ancillary contract, or Member Construction Contract agreed upon by Vendor and the participating agency which must be consistent with and protect the participating agency at least to the same extent as the Region 10 ESC 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 Vendor violation and breach of contract terms.

Does vendor agree? Yes, TLL.

(Initials of Authorized Representative)

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 \$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. Offeror 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 vendor agree? _____

(Initials of Authorized Representative)

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. Vendor 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 Vendor agrees that it shall comply with such provision.

Does vendor agree? _____

(Initials of Authorized Representative)

4. Davis-Bacon Act:

When required by Federal program legislation, Vendor agrees that, for all participating agency prime construction contracts/purchases in excess of \$2,000, Vendor 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, Vendor 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, Vendor 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. Vendor agrees that, for any purchase to which this requirement applies, the award of the purchase to the Vendor is conditioned upon Vendor's acceptance of the wage determination.

Vendor 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 contractor 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 vendor agree? _____

(Initials of Authorized Representative)

5. Contract Work Hours and Safety Standards Act:

Where applicable, for all participating agency contracts or purchases in excess of \$100,000 that involve the employment of mechanics or laborers, Vendor 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, Vendor is required to compute the wages of every mechanic and laborer on the basis of a standard work week of 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 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 vendor agree? _____

(Initials of Authorized Representative)

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.

Vendor agrees to comply with the above requirements when applicable.

Does vendor agree? _____

(Initials of Authorized Representative)

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 \$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, Vendor 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 vendor agree? _____

(Initials of Authorized Representative)

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.

Vendor certifies that Vendor 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. Vendor further agrees to immediately notify the Cooperative and all participating agencies with pending purchases or seeking to purchase from Vendor if Vendor 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 vendor agree? _____

(Initials of Authorized Representative)

9. Byrd Anti-Lobbying Amendment:

Byrd Anti-Lobbying Amendment (31 USC 1352) -- Vendors that apply or bid for an award exceeding \$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, Vendor agrees to file all certifications and disclosures required by, and otherwise comply with, the Byrd Anti-Lobbying Amendment (31 USC 1352).

Does vendor agree? _____

(Initials of Authorized Representative)

10. Procurement of Recovered Materials:

For participating agency purchases utilizing Federal funds, Vendor 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 \$10,000 or the value of the quantity acquired during the preceding fiscal year exceeded \$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 vendor agree? _____

(Initials of Authorized Representative)

11. Profit as a Separate Element of Price:

For purchases using federal funds in excess of \$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, Vendor agrees to provide information and negotiate with the participating agency regarding profit as a separate element of the price for a particular purchase. However, Vendor agrees that the total price, including profit, charged by Vendor to the participating agency shall not exceed the awarded pricing, including any applicable discount, under Vendor’s Cooperative Contract.

Does vendor agree? _____

(Initials of Authorized Representative)

12. Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

Vendor agrees that recipients and subrecipients are prohibited from obligating or expending loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system from companies described in Public Law 115-232, section 889. Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country are also prohibited.

Does vendor agree? _____

(Initials of Authorized Representative)

13. General Compliance and Cooperation with Participating Agencies:

In addition to the foregoing specific requirements, Vendor agrees, in accepting any Purchase Order from a participating agency, it shall make a good faith effort to work with participating agencies 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 vendor agree? _____

(Initials of Authorized Representative)

14. Applicability to Subcontractors

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

Does vendor agree? _____

(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.

Company Name

Signature of Authorized Company Official

Printed Name

Title

Date

PROPOSAL FORM 13: ADDITIONAL ARIZONA CONTRACTOR REQUIREMENTS

AZ Compliance with Federal and state requirements: Contractor agrees when working on any federally assisted projects with more than \$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. Contractor agrees to post wage rates at the work site and submit a copy of their payroll to the member for their files. Contractor must retain records for three years to allow the federal grantor agency access to these records, upon demand. Contractor 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, contractor 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, Contractor 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" Region 10 ESC reserves the right to cancel or suspend the use of any contract for violations of immigration laws and regulations. Region 10 ESC and its members reserve the right to inspect the papers of any contractor or subcontract employee who works under this contract to ensure compliance with the warranty above.

AZ Contractor Employee Work Eligibility: By entering into this contract, contractor 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. Region 10 ESC and/or Region 10 ESC members may request verification of compliance from any contractor or sub contractor performing work under this contract. Region 10 ESC and Region 10 ESC members reserve the right to confirm compliance. In the event that Region 10 ESC or Region 10 ESC members suspect or find that any contractor or subcontractor is not in compliance, Region 10 ESC 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 contractor. All cost associated with any legal action will be the responsibility of the contractor.

AZ Non-Compliance: All federally assisted contracts to members that exceed \$10,000.00 may be terminated by the federal grantee for noncompliance by contractor. 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, contractor 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. Contractor 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 Region 10 ESC member's discretion. Contractor 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, Region 10 ESC and Region 10 ESC members are prohibited from purchasing from a company that is in violation of the Export Administration Act. By entering into the contract, contractor 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.

Signature of Respondent

Date

PROPOSAL FORM 1 4 : OWNERSHIP DISCLOSURE FORM (N.J.S. 52:25 -24.2)

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

Company Name: One Diversified, LLC

Street: 37 Market Street

City, State, Zip Code: Kenilworth, New Jersey 07033

Complete as appropriate:

I _____, certify that I am the sole owner of _____, 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:

I _____, a partner in _____, do hereby certify that the following is a list of all individual partners who own a 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% or more of that corporation's stock or the individual partners owning 10% or greater interest in that partnership.

OR:

I _____, an authorized representative of _____, 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% or more of the corporation's stock or the individual partners owning a 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
_____	_____	_____
_____	_____	_____
_____	_____	_____

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

Date

PROPOSAL FORM 15: NON-COLLUSION AFFIDAVIT

Company Name:

Street:

City, State, Zip Code:

State of New Jersey

County of _____

I, _____ of the _____
Name City

in the County of _____, State of _____ of full
age, being duly sworn according to law on my oath depose and say that:

I am the _____ of the firm of _____
Title Company Name

the Respondent making the Proposal for the goods, services or public work specified under the Harrison Township Board of Education 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 Harrison Township Board of Education 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

Company Name

Authorized Signature & Title

Subscribed and sworn before me

this _____ day of _____, 20____

Notary Public of New Jersey
My commission expires _____, 20____

SEAL

PROPOSAL FORM 1 6: AFFIRMATIVE ACTION AFFIDAVIT (P.L. 1975, C.127)

Company Name: One Diversified, LLC

Street: 37 Market Street

City, State, Zip Code: Kenilworth, New Jersey 07033

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)

Vendors must submit with proposal:

- 1. A photo copy of their Federal Letter of Affirmative Action Plan Approval _____
OR
- 2. A photo copy of their Certificate of Employee Information Report _____
OR
- 3. A complete Affirmative Action Employee Information Report (AA302) _____

Public Work – Over \$50,000 Total Project Cost:

A. No approved Federal or New Jersey Affirmative Action Plan. We will complete Report Form AA201-A upon receipt from the Harrison Township Board of Education _____

B. 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.

Authorized Signature and Title

Date

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

MANDATORY AFFIRMATIVE ACTION LANGUAGE

PROCUREMENT, PROFESSIONAL AND SERVICE CONTRACTS

During the performance of this contract, the contractor agrees as follows:

The contractor 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 contractor 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 contractor 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 contractor or subcontractor, where applicable will, in all solicitations or advertisement for employees placed by or on behalf of the contractor, 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 contractor 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 contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor 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 contractor 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 contractor 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 contractor 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 contractor 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 contractor 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

PROPOSAL FORM 17: C. 271 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 contractors.**

What follows are instructions on the use of form local units can provide to contractors 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 is available in Local Finance Notice 2006-1 (https://www.nj.gov/dca/divisions/dlgs/resources/lfns_2006.html).

1. The disclosure is required for all contracts in excess of \$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 contractor 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 contractor and** on file at least 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 contractor 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 contractors be provided a list of the affected agencies. This will assist contractors 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 https://www.state.nj.us/dca/divisions/dlgs/programs/pay_2_play.html 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 contractors 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 “Contractor 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 contractor also complete a “Stockholder Disclosure Certification.” This will assist the local unit in its obligation to ensure that contractor did not make any prohibited contributions to the committees listed on the Business Entity Disclosure Certification in the 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 Contractor Instructions. **NOTE: This section is not applicable to Boards of Education.**

C. 271 POLITICAL CONTRIBUTION DISCLOSURE FORM

Contractor Instructions

Business entities (contractors) 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 10 days prior to the award of such a contract, the contractor shall disclose contributions to:

1. any State, county, or municipal committee of a political party
2. any legislative leadership committee*
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:
 1. of the public entity awarding the contract
 2. of that county in which that public entity is located
 3. of another public entity within that county
 4. 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 \$300 per election cycle that were made during the 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:

5. individuals with an “interest” ownership or control of more than 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
6. all principals, partners, officers, or directors of the business entity or their spouses
7. any subsidiaries directly or indirectly controlled by the business entity
8. 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 contractor in identifying those public agencies whose elected official and/or candidate campaign committees are affected by the disclosure requirement. It is the contractor’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 contractor’s submission and is disclosable to the public under the Open Public Records Act. The contractor 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.

* 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.”

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 Clerk

Sheriff

{County Executive}

Surrogate

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 A COUNTY-BASED, CUSTOMIZABLE FORM.

PROPOSAL FORM 18: STOCKHOLDER DISCLOSURE CERTIFICATION

Name of Business:

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

OR

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

Check the box that represents the type of business organization:

Partnership

Sole Proprietorship

Limited Liability Partnership

Corporation

Limited Partnership

Limited Liability Corporation

Subchapter S Corporation

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

Stockholders:

Name:	Name:
Home Address:	Home Address:
Name:	Name:
Home Address:	Home Address:
Name:	Name:
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)

PROPOSAL FORM 19: GENERAL TERMS AND CONDITIONS ACCEPTANCE FORM

Signature on the Vendor Contract Signature form certifies complete acceptance of the General Terms and Conditions in this solicitation, except as noted below (additional pages may be attached, if necessary).

Check one of the following responses to the General Terms and Conditions:

We take no exceptions/deviations to the general terms and conditions

(Note: If none are listed below, it is understood that no exceptions/deviations are taken.)

We take the following exceptions/deviations to the general terms and conditions. All exceptions/deviations must be clearly explained. Reference the corresponding general terms and conditions that you are taking exceptions/deviations to. Clearly state if you are adding additions terms and conditions to the general terms and conditions. Provide details on your exceptions/deviations below:

(Note: Unacceptable exceptions shall remove your proposal from consideration for award. Region 10 ESC shall be the sole judge on the acceptance of exceptions/deviations and the decision shall be final.)

PROPOSAL FORM 20: EQUALIS GROUP ADMINISTRATION AGREEMENT

Requirements for Master Agreement To be administered by Equalis Group

Attachment A, Equalis Group Administrative Agreement is used in administering Master Agreements with Region 10 and is preferred by Equalis Group. Redlined copies of this agreement should not be submitted with the response. Should a respondent be recommended for award, this agreement will be negotiated and executed between Equalis Group and the respondent. **Respondents must select one of the following options for submitting their response.**

- Respondent agrees to all terms and conditions outlined in each of the Administration Agreement.
- Respondent wishes to negotiate directly with Equalis Group on terms and conditions outlined in the Administration Agreement. Negotiations will commence after sealed Proposals are opened and Region 10 has determined the respondent met all requirements in their response and may be eligible for award.

PROPOSAL FORM 21: OPEN RECORDS POLICY ACKNOWLEDGEMENT AND ACCEPTANCE
OPEN RECORDS POLICY ACKNOWLEDGMENT AND ACCEPTANCE

Be advised that all information and documents submitted will be subject to the Public Information Act requirements governed by Chapter 552 of the Texas Government Code.

Because contracts are awarded by a Texas governmental entity, all responses submitted are subject to release as public information after contracts are executed. If a Respondent believes that its response, or parts of its response, may be exempted from disclosure to the public, the Respondent must specify page-by-page and line-by-line the parts of the response, which it believes, are exempted from disclosure. In addition, the Respondent must specify which exception(s) are applicable and provide detailed reasons to substantiate the exception(s). Respondent must provide this information on the "Acknowledgement and Acceptance to Region 10 ESC's Public Information Act Policy" form found on the next page of this solicitation. Any information that is unmarked will be considered public information and released, if requested under the Public Information Act.

The determination of whether information is confidential and not subject to disclosure is the duty of the Office of Attorney General (OAG). Region 10 ESC must provide the OAG with the information requested in order for the OAG to render an opinion. In such circumstances, Respondent will be notified in writing that the material has been requested and delivered to the OAG. Respondent will have an opportunity to make arguments to the OAG in writing regarding the exception(s) to the TPIA that permit the information to be withheld from public disclosure. Respondents are advised that such arguments to the OAG must be specific and well-reasoned--vague and general claims to confidentiality by the Respondent are generally not acceptable to the OAG. Once the OAG opinion is received by Region 10 ESC, Region 10 ESC must comply with the opinions of the OAG. Region 10 ESC assumes no responsibility for asserting legal arguments on behalf of any Respondent. Respondents are advised to consult with their legal counsel concerning disclosure issues resulting from this procurement process and to take precautions to safeguard trade secrets and other proprietary information.

After completion of award, these documents will be available for public inspection.

Signature below certifies complete acceptance of Region 10 ESC's Open Records Policy, except as noted below (additional pages may be attached, if necessary). Check one of the following responses to the Acknowledgment and Acceptance of Region 10 ESC's Open Records Policy below:

We acknowledge Region 10 ESC's Public Information Act policy and declare that no information submitted with this proposal, or any part of our proposal, is exempt from disclosure under the Public Information Act.
(Note: All information believed to be a trade secret or proprietary must be listed below. It is further understood that failure to identify such information, in strict accordance with the instructions below, will result in that information being considered public information and released, if requested under the Public Information Act.)

We declare the following information to be a trade secret or proprietary and exempt from disclosure under the Public Information Act.
(Note: Respondent must specify page-by-page and line-by-line the parts of the response, which it believes, are exempt. In addition, Respondent must specify which exception(s) are applicable and provide detailed reasons to substantiate the exception(s).)

Date

Authorized Signature & Title

PROPOSAL FORM 22: VENDOR CONTRACT AND SIGNATURE FORM

The undersigned hereby proposes and agrees to furnish goods and/or services in strict compliance with the terms, specifications and conditions at the prices proposed within response unless noted in writing. The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this proposal in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said proposal have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

VENDORS MUST SUBMIT THIS FORM COMPLETED AND SIGNED WITH THEIR RESPONSE TO BE CONSIDERED

Company name _____

Address _____

City/State/Zip _____

Telephone No. _____

Fax No. _____

Email address _____

Printed name _____

Position with company _____

Authorized signature _____

Term of contract March 1, 2022 **to** February 28, 2025

Unless otherwise stated, all contracts are for a period of three (3) years with an option to renew annually for an additional two (2) years if agreed to by Region 10 ESC. Vendor shall honor all administrative fees for any sales made based on the contract whether renewed or not.

Region 10 ESC Authorized Agent

Date

Print Name

Equalis Group Contract Number _____



Did you sign the vendor contract and signature form? **If not, your Proposal will be rejected.**

Region 10 will negotiate any exceptions and both parties will agree upon which exceptions will be accepted or altered before the Region 10 board votes to accept or reject the proposals.

Equal Employment Opportunity Policy Statement

One Diversified LLC (Diversified) reaffirms its long-standing commitment to equality of opportunity in every aspect of employment. Equal Employment Opportunity (EEO) is not only a legal requirement under our nation's laws, but also a business imperative. EEO is a critical component of Diversified's effort to recruit, develop and retain the most qualified workforce.

It is the policy of Diversified that all employees and applicants for employment be afforded equal opportunities in employment without regard to race, color, sex (including pregnancy, sexual orientation, and gender identity including transgender status), national origin, religion, age (40 or over), genetic information, disability (mental and physical), or retaliation for engaging in an EEO-protected activity. As a part of its' EEO program, Diversified prohibits discrimination or harassment based on any of these categories. In addition, Diversified prohibits discrimination or harassment based on marital status, status as a parent and past, present or future military service. All employees must refrain from practicing or tolerating discrimination or harassment.

Diversified will take affirmative action to ensure that the EEO policy is implemented regarding advertising, application procedures, compensation, demotion, employment, fringe benefits, job assignment, job classification, layoff, leave, promotion, recruitment, rehire, social activities, training, termination, transfer, upgrade, and working conditions.

Any employee who believes they have been discriminated against must immediately report any incident to their manager and/or Business Partner.

Employees found to have taken actions that violate this policy and our country's EEO laws may be subject to corrective action up to and including termination.

All of us—executives, managers, supervisors, and employees—share in the responsibility of successfully incorporating Diversified's EEO policy into every aspect of our duties and complying with our country's EEO laws.

Sincerely,

A handwritten signature in black ink, appearing to read 'Fred D'Alessandro'.

Fred D'Alessandro

January 1, 2021