APPLICATION FOR EVALUATION OF GOOD FAITH EFFORTS

RLI / BID No.: GEN2120797P1

Project Name: Website Design and Hosting Services for CVB, Airport, and Seaport

Prime Contractor: Cemtrex Advanced Technologies DBA CemtrexLabs

Address: 276 Greenpoint Ave, Suite 208, BLDG 8, Brooklyn, NY 11222

Phone: +1 (631) 756-9116 x103

Email: lucky@cemtrex.com

The undersigned representative of the Prime Contractor attests that he/she has authority to bind the Prime Contractor and certifies that the Prime Contractor has made Good Faith Efforts, as defined in Section 1-81.5 of the Broward County Business Opportunity Act of 2012, as amended (the "Business Opportunity Act"), to meet the County Business Enterprise (CBE) goal established for this solicitation by contacting CBE-certified firms to serve as subcontractors for the Project. However, Prime Contractor has been unable to recruit enough CBE-certified firms to meet the CBE participation goal. Consistent with the requirements of the Business Opportunity Act, Prime Contractor hereby submits documentation (attached to this form) of its recruitment efforts, for evaluation by Broward County's Office of Economic and Small Business Development (OESBD), to determine whether Prime Contractor's efforts are sufficient to be deemed Good Faith Efforts, in lieu of goal attainment, under the Business Opportunity Act.

Prime Contractor understands that a determination of Good Faith Efforts to meet the CBE participation goal is contingent upon the information provided by Prime Contractor with this application and the other factors listed in Section 1-81.5(d) of the Business Opportunity Act, as applicable with respect to this solicitation. *See* § 1-81.5(d), County Code of Ordinances. Prime Contractor acknowledges that the determination of Good Faith Efforts is made by the OESBD Director and is not subject to appeal.

Signature: _____

Name / Title: Lucky Gobindram | EVP of Sales and Marketing

Date: December 29, 2020

THE HARTFORD
BUSINESS SERVICE CENTER
3600 WISEMAN BLVD
SAN ANTONIO TX 78251

November 18, 2020

Broward County
115 S ANDREWS AVE
FORT LAUDERDALE FL 33301

Account Information:

Policy Holder Details :	CEMTREX INC

Contact Us

Business Service Center
Business Hours: Monday - Friday
(7AM - 7PM Central Standard Time)
Phone: (866) 467-8730
Fax: (888) 443-6112
Email: agency.services@thehartford.com
Website: https://business.thehartford.com

Enclosed please find a Certificate Of Insurance for the above referenced Policyholder. Please contact us if you have any questions or concerns.

Sincerely,

Your Hartford Service Team

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 11/18/2020

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATIONIS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME:	
UNITED ASSURANCE INC 13659347 16 00 POLLIT AVE FAIR LAWN NJ 07410	PHONE (A/C, No, Ext): (201) 797-6600	FAX (A/C, No): (201) 797-4455
	E-MAIL ADDRESS:	
	INSURER(S) AFFORDING COVERAGE	NAIC#
	INSURER A : Twin City Fire Insurance Company	29459
INSURED	INSURER B :	
CEMTREX INC 110 BI COUNTY BLVD STE 124 FARMINGDALE NY 11735-3923	INSURER C :	
	INSURER D :	
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED.NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/Y YYY)	LIMITS	
A	COMMERCIAL GENERAL LIABILITY CLAIMS-MADE [X] OCCUR [X] General Liability GEN'L AGGREGATE LIMIT APPLIES PER: POLICY [ ] PRO-JECT [X] LOC OTHER:	X		13 SBA AB2155	09/24/2020	09/24/2021	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$1,000,000 $1,000,000 $10,000 $1,000,000 $2,000,000 $2,000,000
A	**AUTOMOBILE LIABILITY** ANY AUTO ALL OWNED AUTOS [X] HIRED AUTOS SCHEDULED AUTOS [X] NON-OWNED AUTOS			13 SBA AB2155	09/24/2020	09/24/2021	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$1,000,000
A	[X] **UMBRELLA LIAB** **EXCESS LIAB** [X] OCCUR CLAIMS-MADE DED [X] RETENTION $ 10,000			13 SBA AB2155	09/24/2020	09/24/2021	EACH OCCURRENCE AGGREGATE	$1,000,000 $1,000,000
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N/ A					PER STATUTE [ ] OTH-ER E.L. EACH ACCIDENT E.L. DISEASE -EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	
A	EMPLOYEE BENEFITS LIABILITY			13 SBA AB2155	09/24/2020	09/24/2021	Each Claim Limit Aggregate Limit	$1,000,000 $2,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES **(ACORD 101, Additional Remarks Schedule, may be attached if more space is required)**

Those usual to the Insured's Operations. Certificate holder is an additional insured per the Business Liability Coverage Form SS0008 attached to this policy.

CERTIFICATE HOLDER	CANCELLATION
Broward County 115 S ANDREWS AVE FORT LAUDERDALE FL 33301	**SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.** **AUTHORIZED REPRESENTATIVE** Susan L. Castaneda

UNITED ASSURANCE
Protection • Service • Trust
16-00 Pollitt Drive Fair Lawn, NJ 07410 · Phone (201) 797-6600 · Fax (201) 797-4455
www.unitedassurance.com

January 8, 2021

Cemtrex Advanced Technologies, Inc DBA Cemtrex Labs
110 Bi-County Blvd
Ste 124
Farmingdale, NY 11735

Re: Broward County Insurance

To Whom it May Concern,

We are currently in the process of obtaining quotes to fulfill the insurance requirements for Broward County.

Thank you and Regards,
Nancy Ha
Commercial Insurance Account Executive
Email: n.ha@unitedassurance.com
Direct Phone # (201)254-1863

Enterprise Technology Services
Vendor Security Questionnaire (VSQ)
(For RFPs and Sole Source/Only Reasonable Source as applicable)

The Vendor Security Questionnaire's (VSQ) purpose is to assess your organization's security policies and/or system protocol and to identify any security vulnerabilities. Each responding vendor will be required to complete and submit the VSQ (for applicable solution – services, hardware, and/or software). If not included with the proposal submittal at the time of the solicitation opening deadline, the proposing vendor will be required to complete and submit the VSQ within three business days of County's request.

If a response requires additional information, the Vendor should attach a written detailed response; each response should be numbered to match the question number. The County will review Vendor's VSQ response and any security concerns will be addressed during Evaluation Committee Meetings or negotiations. Unresolved security concerns shall be considered by the committee as part of its final evaluation and may lead to impasse during negotiations.

The questionnaire is divided into the following areas: **Section 1: Software-as-a-Service/Hosting/Application Development/Managed and Professional Services**; **Section 2: Software**; and **Section 3: Hardware.** Each section(s) should be completed as applicable to your organization's proposed product and/or service. If applicable, failure to complete the questionnaire may deem a vendor non-responsible. The questionnaire should be submitted with your proposal. Vendor should immediately inform the assigned Purchasing Agent of any changes in vendor's responses after submittal.

Vendor Name:	Cemtrex Advanced Technologies DBA CemtrexLabs
Vendor Type (Manufacturer, Reseller, Other? If Other, specify.):	Reseller
Technical Contact Name / Email Address:	Gaurav Taywade - gaurav@cemtrex.com
Product Name / Description:	
Solicitation Number and Title (If applicable):	GEN2120797p1

For each applicable section, complete the matrix by using the dropdown option to select YES or NO. Use "Comments" section to provide as much explanation as possible to clearly support your response. Additional pages may be attached to provide further detail, but any attachments should be referenced in "Comments" section. **Select "N/A" if a question within a given section is not applicable. IMPORTANT:** Vendors must complete ATTESTATION SECTION at bottom of form using digital signature or pdf. Unsigned forms or incomplete forms will be returned.

SECTION 1: SOFTWARE-AS-A-SERVICE (SaaS) / HOSTING / APPLICATION DEVELOPMENT / MANAGED AND PROFESSIONAL SERVICES

No.	Area	Question	Vendor Response	
			YES/NO	Comments
1		**REQUIRED:** Will your organization provide **SOFTWARE-AS-A-SERVICE (SaaS)**?	Yes	
2		**REQUIRED:** Will your organization provide **HOSTING SERVICES**?	Yes	
3		**REQUIRED:** Will your organization provide **APPLICATION DEVELOPMENT SERVICES**?	Yes	
4		**REQUIRED:** Will your organization provide **MANAGED OR PROFESSIONAL SERVICES (UNSUPERVISED BY COUNTY PERSONNEL)?** (Note: "Managed or Professional Services" used herein refers to unsupervised (by County personnel) installation, configuration, and maintenance or monitoring of systems, applications or infrastructure related to your organization's proposed solution.)	Yes	We do provide all kind of managed and professional services for software development.
		STOP: If you selected NO for Questions 1 through 4 above, **PROCEED TO SECTION 2.**		
5	**Supporting Documentation**	Provide the following: a) Workflow diagram of stored or transmitted information (for SaaS and Hosting Services only)		Please refer to WP Engines VSQ
6		b) Security / Network Architecture diagram (for SaaS and Hosting Services only)		Please refer to WP Engines VSQ
7		c) Secure Coding standard (for Application Development Services only)		Please refer to WP Engines VSQ
8		d) Application Security Program standard (for Application Development Services only)		Please refer to WP Engines VSQ

9	**Audit Reporting Requirements**	Does your organization have a current Service Organization Controls (SOC) II, Type II report, inclusive of all five Trust Service Principles (Security, Availability, Processing Integrity, Confidentiality, and Privacy?). (Note: For any SaaS or hosted application, the SOC report should be for the organization or application specifically, not the datacenter only.)	NO	
10	**Payment Card Industry (PCI) environments - Applicable only if Organization or its third party partner processes or collects credit card information.**	Does your organization have a current Payment Card Industry (PCI) certification (e.g., Attestation of Compliance (AOC), Self-Assessment Questionnaire (SAQ))?	NO	
11		Will the product or solution process or collect credit card information?	YES	We used payment processor here which are already PCI compliance.
12		Does your organization maintain a file integrity monitoring program to ensure critical file system changes are monitored and approved with respect to Confidential County data?	YES	We do have secure server and system in place to maintain file integrity as per country norms.
13	**Electronic Protected Health Information (ePHI) - Applicable only if Organization has access to or will be hosting or storing County ePHI.**	Has your organization had a Risk Assessment performed in the past 5 years by an external auditor in conjunction with the HIPAA Security rule?	NO	
14		Does your organization maintain current HIPAA specific policies and procedures in conjunction with the HIPAA Security Rule?	YES	Based on application we received we use their HIPAA compliance document to maintain this.
15		Does your organization have a designated HIPAA Security and Privacy Officer(s)?	NO	
16		Does your organization provide HIPAA Security training to your employees at time of hire and at least annually thereafter?	YES	We do provide this training using online training platform only when we received project based on HIPAA compliance.
17	**Roles & Responsibilities**	Has your organization appointed a central point of contact for security coordination?	YES	
18		Does your organization have an expected timeframe to respond to initial contact for security related issues? Provide timeframe.	Yes	Our first support will reply within 1 hr of incident reported.
19		Does your organization define the priority level of an issue (e.g., minor vs. major, 0-4 scale, etc.)? Describe.	Yes	We define priority of issue highest from level3, level2 and level1
20		Does your organization have an expected Service Level Agreement (SLA) to implement changes needed to fix security issues according to priority level? Describe.	YES	Yes we do have agreement with all our customer to support for specific amount of time as per client requirement where we will fix all issues reported to us.
21	**Federated Identity Management and Web Services Integration**	Does your organization's product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory)? Describe.	YES	Most of our product is having single sign in and OAUTH.
22		Does your organization use web services and/or data import/export functions (e.g., API, FTP)? Describe.	YES	We do use FTP, SFTP and RESTful API's

23	**External Parties**	Will third parties, such as IT service providers have access to the County's data that is stored or transmitted by your organization?	NO	
24		Does your organization have Disaster Recovery and Continuity of Operations plans where third-party dependencies are concerned?	Yes	
25		Does your organization outsourcing any aspect of the service to a third party?	YES	It depends on whenever we need subject matter expert.
26		Does your organization utilize any off-shore resources for development? Provide location(s).	YES	India
27		Does your organization outsource or build the application in-house?	YES	We do outsource and build application in house.
28		Does your organization share customer data with or enable direct access by any third-party?	NO	
29		Will any third party vendors process, access, transmit or store any County data?	NO	
30		Does all third party vendors contractually comply with your organization's security standards for data processing?	YES	Whenever needed it will go through strict contract and NDA.
31		Does your organization regularly audit your critical vendors? Describe.	YES	We do audit our vendor every year with our standard audit process.
32	**Information Security Policy & Procedures**	Does your organization have documented standard policies and procedures for security and compliance?	YES	We do have standard security policies in place.
33	**Risk Assessment**	Does your organization have a process that addresses: (a) the identification and measurement of potential risks with mitigating controls (measures taken to reduce risk), and (b) the acceptance or transfer (e.g. insurance policies, warranties, etc.) of the remaining (residual) risk after mitigation steps have been applied?	YES	Tool we use for project management will cover this aspect.
34	**Regulatory Compliance**	Is the product or solution currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.	NO	
35		Does your organization have a documented process to identify new laws and regulations with IT security implications (e.g., FIPA, new state breach notification requirements, monitoring newsletters, webinars, security or regulatory forums, etc.)?	NO	
36		Has your organization experienced a legally reportable data breach within the past 5 years?	NO	
37		Does your organization have procedures for preservation of electronic records and audit logs in case of litigation hold?	YES	
38	**During Employment – Training, Education &**	Have employees and third party vendors received formal information security awareness training? Provide frequency.	YES	We provide this every quarter
39		Have your organization's security policies and procedures been communicated to your employees?	YES	
40		Are periodic security reminders provided to your organization's employees?	YES	Every 4 months.

41	**Background Checks**	Does your organization perform background checks (e.g., credential verification, criminal history, credit history) to examine and assess an employee's or third party vendor's work and criminal history?	YES	We do have complete background verification process in place.
42		Are individuals who would have access to the County's data subjected to periodic follow-up background checks?	YES	
43	**Prior to Employment - Terms and Conditions of Employment**	Are employees and third party vendors required to sign a non-disclosure agreement (e.g., non-disclosure and/or confidentiality form upon initial employment)?	YES	Yes, and we will update it every year and resign it from all our employees.
44		If so, are employees and third party vendors required to sign the non-disclosure agreement annually?	Yes	
45	**Termination or Change in Employment**	Does your organization require that all equipment of any terminated employee or third party vendor is returned and that his/her user ID is disabled in all systems and badges and/or keys are returned?	YES	This is standard process we have in place.
46		Upon transfer, is existing access reviewed for relevance for employees and third party vendors?	Yes	
47	**Secure Areas**	Does your organization have effective physical access controls (e.g., door locks, badge /electronic key ID and access controls) in place that prevent unauthorized access to facilities and a facility security plan?	YES	We do have door lock as well as electronics key
48		Do personnel abide by a clean desk policy and lock workstation screens prior to leaving work areas?	Yes	
49		Does your organization have a contingency plan in place to handle emergency access to facilities?	YES	
50		Are physical access controls authorized? Describe who is responsible for managing and ensuring that only appropriate persons have keys or codes to the facility and to locations within the facility with secure data.	YES	We have two dedicated personnel for this who handle it and review it on day-to-day basis.
51		Are there policies and procedures to document repairs and modifications to physical components of the facility that are related to security?	Yes	We do have complete record base for this.
52		Are employees or third party vendors permitted access to customer environments from your physical locations only?	YES	Yes, it's necessity but we have amended this by considering Work from home facility during covid-19
53	**Application and Information Access Control - Confidential System Isolation**	Are systems and networks that host, process, and/or transfer Confidential information "protected" (i.e., isolated, logically or physically separated) from other systems and/or networks?	YES	We do have special LAB to keep secure servers.
54		Are internal and external networks separated by firewalls with access policies and rules?	YES	We do have firewall policy in place.
55		Can your organization restrict access to the solution to and from the County's network in a "deny all, permit by exception" configuration (i.e. whitelist County IP addresses only)?	YES	

56	**Data Security**	Are development, test, and production environments separated from operational, IT environments to protect production (actively used) applications from inadvertent changes or disruption?	YES	
57		Does your organization apply database and application logical segregation of customer data?	YES	
58		Is there a standard approach for protecting network devices to prevent unauthorized access/network related attacks and data-theft (e.g. firewall between public and private networks, internal VLAN, firewall separation, separate WLAN network, secure portal, multi-tenancy, virtualization, shared storage, etc.)?	YES	We do use virtualization and multi-tenancy
59		Are employees allowed to connect to customer environments remotely (e.g., working from home, public Wi-Fi access)?	YES	Yes, only during pandemic work from home situation else strictly no.
60		Is there a remote access policy? Provide documentation.	NO	
61		Does your organization have protections in place for ensuring secure remote access (e.g., up-to-date antivirus, posture assessment, VPN enforcement, split tunneling)?	YES	
62		Will your organization restrict inbound and outbound traffic to the County network to a “deny all, permit by exception” configuration?	YES	
63		Is this a multi-tenant solution?	YES	
64		Will County’s data be co-mingled with any other multi-tenant customer?	NO	
65		Will County’s data be processed, accessed, transmitted or stored through an off shore environment (e.g., Outside continental U.S, Alaska, Hawaii)?	YES	It will be processed in our India office based on pre permission of client else we will do this in our USA office.
66	**Audit Logging**	Does the software or solution perform audit logging? Describe.	Yes	We do have advance audit logging mechanism for all our software’s.
67		Does the software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?	Yes	We do allow audit log retention up to 30 days, but it can be increased based on client requirement.
68		Does the software track events for user activity (e.g., failed/successful logins, privileged access)? Describe.	YES	This will be tracked under audit log.
69	**Encryption**	Does your organization provide a means to encrypt County Confidential information in transit? Describe controls that are in place to protect Confidential information when transferred (e.g., encryption).	YES	We do use symmetric and asymmetric data encryption.
70		Does your organization use a secure VPN connection with third parties and/or IT vendors for email encryption?	YES	
71		Does your organization provide a means to encrypt data at rest (e.g., AES)?	YES	

72	**Vulnerability Assessment and Remediation**	Does your organization perform periodic vulnerability scans on your IT systems, networks, and supporting security systems? Provide frequency.	YES	We do it every two months.
73		Are internal or third party vulnerability assessments automated?	NO	It's manual process
74		Does your organization have a security patch management cycle in place to address identified vulnerabilities?	YES	
75		Does your organization provide disclosure of vulnerabilities found in your environment and remediation timelines?	No	
76		Does your organization notify customer of applicable patches?	YES	
77	**Security Monitoring**	Are third party connections to your network monitored and reviewed to confirm only authorized access and appropriate usage (e.g., with VPN logs, server event logs, system, application and data access logging, automated alerts, regular/periodic review of logs or reports)?	YES	
78		Does your organization monitor your systems and networks for security events? Describe monitoring (e.g., server and networking equipment logs such as servers, routers, switches, wireless APs, monitored regularly).	YES	
79		Does your organization periodically review system activity? Provide frequency.	YES	Every 2 weeks
80	**Identity & Access Management**	Does your organization have a formal access authorization process based on "least privilege" (i.e. employees are granted the least amount of access possible to perform their assigned duties) and "need to know" (e.g., access permissions granted based upon the legitimate business need of the user to access the information, role-based permissions, limited access based on specific responsibilities, network access request form)?	YES	
81		Are systems and applications configured to restrict access only to authorized individuals (e.g. use of unique IDs and passwords, minimum password length, password complexity, log-in history, lockout, password change, expiration)?	YES	
82		Is there a list maintained of authorized users with general access and administrative access (e.g., active directory user lists within a Confidential application, a spreadsheet of users, a human resources file)?	YES	
83		Does your organization maintain a list of "accepted mobile devices" (e.g., smart phones, cell phones) exist and are these devices tracked and managed (e.g., Mobile Device Management)?	YES	
84		Is a Data Loss Prevention (DLP) in place to prevent the unauthorized distribution of Confidential information?	NO	
85		Is software installation for desktops, laptops, and servers restricted to administrative users only?	YES	

86		Does software or system have automatic logoff for session inactivity?	YES	
87		Is access to source application code restricted? Describe how and provide a list of authorized users maintained and updated.	YES	We achieve this using version control software and we do have special admin to perform this task.
88		Are user IDs for your system uniquely identifiable?	YES	
89		Does your organization have any shared accounts? Describe.	NO	
90		Will your organization allow remote access from third party vendors to the County network, with immediate deactivation after use?	NO	
91		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?	NO	
92		Is Multi-Factor Authentication (MFA) required for employees/contractors for remote access to production systems?	YES	Only in case we decided to provide an access.
93	**Entitlement Reviews**	Does your organization have a process to review user accounts and related access (e.g., manual process of reviewing system accounts to user accounts in AD for both users and privileged access, such as admins, developers, etc.)?	YES	
94	**Antivirus**	Is antivirus software installed and running on your computers and supporting systems (e.g., desktops, servers, gateways, etc.)?	YES	
95		Is this antivirus product centrally managed (e.g., is the antivirus monitored to verify all endpoints have functional agents, agents are up to date with the latest signatures, etc.)? Explain your policies and procedures for management of antivirus software.	YES	
96		Does your organization have a process for detecting and reporting malicious software?	YES	
97	**Network Defense and Host Intrusion Prevention Systems**	Does your organization have any Intrusion Protection System (IPS) in place for your environment?	YES	
98		Does your organization install personal firewall software on any mobile or employee-owned device?	NO	
99	**Media Handling**	Does your organization have procedures to protect documents and computer media (e.g., tapes, disks, hard drives, etc.) from unauthorized disclosure, modification, removal, and destruction?	YES	
100		Is Confidential data encrypted (e.g., data at rest) when stored on laptop, desktop, and server hard drives, flash drives, backup tapes)?	YES	In most cased we don't allow to store it.
101	**Secure Disposal**	Are there security procedures (e.g., use of secure wiping, NIST 800-88, etc.) for the decommissioning (replacement) of IT equipment and IT storage devices which contain or process Confidential information?	NO	
102	**Separation of Duties**	Are duties separated (e.g., front desk duties separated from accounting, data analysts access separated from IT support), where appropriate, to reduce the opportunity for unauthorized modification, unintentional modification, or misuse of your IT assets?	YES	

103	**Change Management**	Do formal testing and change management procedures exist for networks, systems, desktops, software releases, deployments, and software vulnerability during patching activities, changes to the system, changes to the workstations and servers with appropriate testing, notification, and approval, etc.?	YES	
104	**Incident Management**	In the event of a major security incident or data breach, do you provide the County a third party digital forensics/incident report?	YES	On request only
105		Does your organization identify, respond to, and mitigate suspected or known security incidents (e.g., incident form completed as a response to each incident)?	YES	
106		Does your organization have a formal incident response and data breach notification plan and team?	YES	
107		Is evidence properly collected and maintained during the investigation of a security incident (e.g., employing chain of custody and other computer forensic methodologies that are monitored by internal and/or external parties)?	YES	
108		Are incidents identified, investigated, and reported according to applicable legal requirements?	YES	
109		Are incidents escalated and communicated? Describe.	NO	
110		Do you have a contingency plan in place to handle emergency access to the software?	YES	
111	**Disaster Recovery Plan & Backups**	Does your organization have a mechanism to back up critical IT systems and Confidential data? Describe.	YES	We do have backup mechanism on local as well as cloud infra.
112		Does your organization periodically test your backup/restoration plan by restoring from backup media?	YES	
113		Does your organization have a disaster recovery plan?	YES	
114		Are disaster recovery plans updated and tested at least annually?	YES	
115		Do any single points of failure exist which would disrupt functionality of the product or service?	NO	
116	**Product Security Development Lifecycle**	Does your organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing)?	YES	
117		Does your organization maintain end-of-life-schedule for the software product?	YES	
118		Is the product engineered as a multi-tier architecture design?	YES	
119		Is the product or service within 3 year end of life?	YES	
120	**Crypto Materials and Key Management**	Does your organization have a centralized key management program in place (e.g., any Public Key Infrastructure (PKI), Hardware Security Module (HSM)-based or not, etc.) to issue certificates needed for products and cloud service infrastructure?	YES	

121	**Application Development - This section is applicable only if Organization is providing Application Development Services.**	Do your organization's development and testing teams receive training specific to application security? Describe.	YES	
122		Does your organization follow application security and coding standards and utilize a development framework?	YES	
123		Does your organization's development team use a development framework? List development languages and framework.	YES	
124		Will the County receive a copy of the source code?	YES	
125		Does your organization review security at each phase of the software development life cycle?	YES	
126		Does your organization use an industry standard methodology for conducting security testing? Describe.	YES	We do use lot of third-party tools which comply industry standard and provide training to our employees.
127		Does your organization use an independent 3rd party for periodic security penetration testing?	YES	
128		Does your organization use automated tools for security testing or code reviews?	YES	
129		Does your organization perform security testing based on industry standards (e.g. OWASP Top 10, SANS Top 25)?	YES	
130		Does your organization use SAST and DAST tools to scan code for vulnerabilities prior to production deployment?	NO	
131		Does your organization perform peer code reviews on source code prior to production deployment?	YES	
132		Does your organization remediate all vulnerabilities identified prior to production deployment?	YES	
133		Does your organization have a security methodology for continuous maintenance of the application and applicable components?	YES	

SECTION 2: SOFTWARE INSTALLED LOCALLY IN COUNTY'S NETWORK

No.	Area	Question	Vendor Response	
			YES/NO	Comments
1	**REQUIRED:** Will your organization provide **SOFTWARE INSTALLED LOCALLY IN COUNTY NETWORK**?			
STOP: If you selected NO for Question 1, **PROCEED TO SECTION 3.**				
2	**Reseller**	Will your organization act as a reseller to provide software to the County? If so, provide manufacturer documentation regarding the security controls of the software and a secure configuration document.	NO	
3	**Supporting Documentation**	Provide the following: a) Hardware and Software requirements (i.e. Operating System, CPUs, RAM)		
4		b) Network connectivity requirements		
5	**Software Installation Requirements**	Can the application and service accounts used to run the application be configured to run as non-privileged users (e.g. non-Local Administrator rights)	NO	
6		Does software require admin rights to be installed? Describe the level of administrative access the software will need on the County domain.	YES	It needs super admin rights to get installed.
7		Is remote access required for installation and support? Describe.	NO	We will train admin for installation process.
8		Can the software be installed on and operated in a virtualized environment?	YES	
9	**Third Party Software Requirements**	Is third party software (e.g., Java, Adobe) required to be installed for your software to work? Provide software and minimum version.	YES	It's depended upon tech stack we are using, and we need all latest version of SDK.
10		Will the software remain compatible with all updates and new releases of required third party software?	NO	Software need to be modified to support latest releases.
11		Are there contingencies where key third-party dependencies are concerned?	NO	
12	**Secure Software Design/Testing**	Is the software currently certified by any security standards? (e.g., PCI-DSS). Provide standards.	NO	
13		Is security testing performed on product to identify security vulnerabilities (e.g., injection, buffer overflows)?	YES	
14		Has the software been developed following secure programming standards like those in the OWASP Developer Guide?	YES	We will do based on client requirement.
15		Is your organization outsourcing any aspect of the service to a third party?	NO	

16		Is the product engineered as a multi-tier architecture design?	YES	
17		Does your organization have capability to respond to and update product for any unforeseen new regulatory requirements?	YES	
18	**Audit Logging**	Does software or solution perform audit logging? Describe.	YES	
19		Does software or solution allow for the configuration of audit log retention for a minimum of 90 days or more?	NO	Standard is 60 days, but we can increase it based on requirement.
20		Does software have audit reporting capabilities (e.g., user activity, privileged access)? Describe.	YES	
21	**Security Updates/Patching**	Does software have a security patch process? Describe your software security patch process, frequency of security patch releases, and how security vulnerabilities are identified.	YES	
22		Does your organization support electronic delivery of digitally signed upgrades?	YES	
23	**Secure Configuration / Installation (i.e. PA-DSS configuration)**	Does software allow for secure configuration and installation (e.g., OS hardening, disabling unnecessary services, antivirus compatibility)?	YES	
24		Will software or solution process or collect credit card information?	NO	
25	**Software Upgrade Cycles**	Does software have upgrade cycles? Identify those cycles.	YES	Based on additional scope request
26	**Confidential Data**	Does software restrict confidential data (e.g., Social Security Number or Date of Birth) from being used as a primary identifier?	YES	
27		Does software have documentation showing where all confidential data is stored in the application?	YES	
28		Does product or solution collect Confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?	YES	Depend on requirement.
29	**Encryption**	Does software support encryption of data in motion (e.g., SSL)?	YES	
30		Does software support encryption of data at rest (e.g., column-level encryption, etc.)?	YES	
31		Does software have built-in encryption controls? List controls.	YES	
32	**Authentication**	Does product have Single Sign-on (SSO) and Federated Identity Enablement integration options (e.g., support for standards like SAML v2 and OAuth 2.0, active directory, etc.)? Describe.	YES	SSO and OAuth
33	**Roles and Responsibilities**	Does software provide role-based access control?	YES	
34		Is a service account required for this software?	YES	
35		If so, does the service account require admin rights?	YES	
36	**Product Security Development Lifecycle**	Does organization have any product pre-release security threat modeling in place (e.g., secure coding practice, security architecture review, penetration testing, etc.)?	YES	
37		Does your organization maintain end-of-life-schedule for the software product?	YES	
38		Is product or service within 3 year end of life?	YES	
39	**Regulatory Compliance**	Is the software or solution currently certified by any security standards (e.g., PCI-DSS, HIPAA)? Provide proof of compliance documentation.	NO	

SECTION 3: HARDWARE

No.	Area	Description	Vendor Response	
			YES/NO	Comments
1	**REQUIRED:** Will your organization provide **HARDWARE**?			
	STOP: If you selected NO to Question 1, **PROCEED TO SECTION 4.**			
2	**Reseller**	Will your organization act as a reseller to provide hardware products to the County? If so, provide manufacturer documentation regarding the supply chain security controls around the hardware and a secure configuration document.	YES	
3	**Secure Hardware Design/Testing**	Are there physical security features used to prevent tampering of the hardware? Identify features.	YES	
4		Is security testing performed on product to identify security vulnerabilities (e.g., injection, buffer overflows)?	YES	
5		Do you take security measures during the manufacturing of the hardware? Describe.	YES	We do have security testing in place.
6	**Security Updates/Patching**	Is your hardware scanned to detect any vulnerabilities or backdoors within the firmware?	YES	
7		Has the operating system installed on the hardware been scanned for vulnerabilities?	YES	
8		Is your firmware upgraded to remediate vulnerabilities? Provide frequency.	YES	
9		If a new vulnerability is identified, is there a documented timeframe for updates/releases? Provide frequency.	YES	Within 48 hrs
10	**Identity & Access Management**	Are remote control features embedded for the manufacturer's support or ability to remotely access? Describe.	YES	
11		Do backdoors exist that can lead to unauthorized access? Describe.	NO	

12		Do default accounts exist? List all default accounts.	NO	
13		Can default accounts and passwords be changed by Broward County?	NOI	
14		Can service accounts be configured to run as non-privileged user (i.e. non-Domain Admin)?	NO	
15	**Confidential Data**	Does the product or solution collect Confidential data (e.g., Social Security Number, Date of Birth, Credit Card information)?	YES	Based on requirement
16	**Roles and Responsibilities**	Is a service account required for this hardware?	NO	
17		If so, does the service account require admin rights?	NO	
18	**Product Security**	Is an end-of-life schedule maintained for the hardware?	NO	
19	**Development Lifecycle**	Is product or service within 3 year end of life?	YES	
20	**Media Handling**	Does your organization have a secure data wipe and data destruction program for proper drive disposal (e.g., Certificate of destruction, electronic media purging)? Describe.	NO	
21	**Regulatory Compliance**	Is the hardware currently certified by any security standards? (e.g., PCI-DSS, HIPAA). Provide proof of compliance documentation.	NO	
22		Will product or solution process or collect credit card information?	NO	
23		Does your organization have a process to identify new laws and regulations with IT security implications?	NO	

SECTION 4: ATTESTATION SECTION - ALL VENDORS MUST FULLY COMPLETE AND SIGN THIS SECTION.	
I possess the authority to sign and act as an agent on behalf of this organization. I have read the above questionnaire in its entirety and responded in a truthful manner to the best of my ability.	
Vendor Name:	Cemtrex Advanced Technologies DBA CemtrexLabs
Printed Representative Name:	Lucky Gobindram
Printed Representative Title:	EVP, Sales and Marketing
Signature:	
Date:	January 13,2021