**VENDOR PARTNER BUSINESS CONTINUITY, DISASTER RECOVERY, AND**

**CYBER SECURITY FORM**

1. Does your organization have a disaster recovery plan in place? Does it specifically cover the information systems, data, and networks that would support this contract? Please explain.

Click or tap here to enter text.

If yes, please describe the following:

1. DR Testing frequency

Click or tap here to enter text.

1. Recovery Time Objective – How long will it take your organization to fully recover applications, data, services, network, processes, facilities? Is this measured from the time of the outage or from the time your organization decides to start the recovery process?

Click or tap here to enter text.

1. Recovery Point Objective – When services are fully restored, will there be data loss? Are systems replicated real-time or from backup?

Click or tap here to enter text.

1. Tell us specifically how your organization will ensure there is prompt and ongoing communication regarding a disruption to business/contact partners during a disaster.

Click or tap here to enter text.

1. Does your organization have a business continuity plan in place? Does it specifically cover the people, processes, and facilities that would support this contract? Please explain.

Click or tap here to enter text.

1. Describe your organization’s approach and response to Cyber Security, detailing specifics as follows:
2. If you support a SaaS model, what external security audits and penetration testing results or certifications have you received for the product you are specifying for this proposal? Have you received a SOC2 audit? If yes, can you provide a copy of the official report(s)?

Click or tap here to enter text.

1. Does each customer have a dedicated, firewalled instance?

Click or tap here to enter text.

1. How is KEMI/customer data protected?

Click or tap here to enter text.

1. Describe all methods of user authentication? Specifically indicate if you support the following:

Click or tap here to enter text.

* 1. Local Username and Password – describe password requirements and change frequency restrictions

Click or tap here to enter text.

* 1. Multi-Factor Authentication with SAML/SSO providers

Click or tap here to enter text.

* 1. Synchronized Active Directory accounts with client environment. Indicate if windows login credentials can be passed for single sign-on capability

Click or tap here to enter text.

* 1. Describe user permissions.
     1. Role-based?
     2. Templates?
     3. Internal verses External?

Click or tap here to enter text.

1. Describe the structure and options available for the backend database configuration? For example, would KEMI data be segregated from another client or are they stored in the same database with access being controlled by the application?

Click or tap here to enter text.

1. Describe mechanism for controlling software vendor employee access to KEMI data? How is it controlled, audited, and verified?

Click or tap here to enter text.

1. What company policies and procedures are in place to prevent, detect and audit the vendor employees from exporting KEMI data and preventing data loss?

Click or tap here to enter text.

1. Describe data encryption methods utilized. Include the specific items of at rest, in transit and any backup or replicated copies? How are the encryption keys stored and protected?

Click or tap here to enter text.

1. Provide a summary of methods, tools, hardware, or log correlation applications that you use to monitor, detect and alert of any type of attempted cyber-attack or data breach.

Click or tap here to enter text.

1. What type of enterprise antivirus software do you run on all employee workstations?

Click or tap here to enter text.

1. What physical controls are in place to prevent unauthorized access to servers, data storage and backup tapes?

Click or tap here to enter text.

1. Provide a summary of user security within the application? Is it role-based? How granular can security be defined?

Click or tap here to enter text.

1. Describe the audit tracking and reporting capabilities.

Click or tap here to enter text.

1. Do you provide a mechanism to escrow the software and provide a mechanism for clients to get access to their data if the business experiences a catastrophic event or business operating failure? This includes being purchased or going out of business.

Click or tap here to enter text.

1. Has the application code for the product we are considering been reviewed by a third-party security assessment team for any coding vulnerabilities?   Is the application code regularly scanned for vulnerabilities after each update, modification, or change?

Click or tap here to enter text.

1. Provide a brief overview of your development and quality assurance testing processes. Include any special emphasis regarding security testing, awareness, and validation.

Click or tap here to enter text.

1. Do you have a cyber liability insurance policy? If yes, what are the specific coverages and associated limits?

Click or tap here to enter text.

1. Are you willing to enter into a specific Service Level Agreement (SLA), under any contract awarded, to address the following?
2. Guaranteed performance metrics (e.g. system uptimes) during normal operations; and
3. Specific business continuity measures to ensure minimal disruption to operations.

Please explain:

Click or tap here to enter text.