**RFP 23167: Records Management Solution**

**Attachment C: Supplemental Security Questions**

**Office of the County Clerk**

**Lake County, IL**

**Instructions:**

Please review the requirements in **Attachment A Requirements** carefully. If a Respondent cannot provide a SOC 2 report as mentioned in ID 1.9.1 of the Technical tab, please complete the below Supplemental Security Questions for the County’s IT Department.

Use the yellow shaded fields to indicate your answers to the following questions.  The yellow fields will automatically expand to accommodate content.  Every attempt should be made to preserve the original format of this form.  A completed Supplemental Security is a requirement for proposal submission if Respondent cannot provide a SOC 2 report. Failure to complete and submit this form may impact your proposal’s responsiveness.  Diagrams, certificates, graphics, and other exhibits should be referenced within the relevant answer field and included as legible attachments.

1. **Supplemental Security Questions** 
   1. How do you verify that the backup process is functional and that restores work? How often is this done?

|  |
| --- |
|  |

* 1. Are all backup media (onsite, offsite, full and/or incremental), rendered unreadable at the end of their useful life? If yes, please describe the method used to render this media unreadable.

|  |
| --- |
|  |

* 1. Are procedures in place to fully destroy data contained on back-up media before they are reused? If so, how?

|  |
| --- |
|  |

* 1. Are the backups protected from unauthorized access and tampering? If yes, describe how they are protected.

|  |
| --- |
|  |

* 1. Is backup media containing confidential information encrypted and stored in a locked container during transport? Please describe encryption method.

|  |
| --- |
|  |

* 1. Do you store backups offsite?

How do you secure access to offsite media? Please specify the name of any 3rd party service providers.

How do you secure access to media in transit? Please specify the name of any 3rd party service providers.

|  |
| --- |
|  |

* 1. Will any Internet-accessible systems contain data? If so, how is the data on those systems protected?

|  |
| --- |
|  |

* 1. What type of data will you be exchanging with customers? What type of data will you be processing and/or storing FROM customer? How is data transfer secured?

|  |
| --- |
|  |

* 1. Describe the different operating environments for storing and processing customer data. This list of systems names and purposes will help customers with initial evaluation and possible incident response.

|  |
| --- |
|  |

* 1. Is sensitive data (i.e. PII or cardholder) securely disposed of when no longer needed?

|  |
| --- |
|  |

* 1. Is there one person assigned to lead, manage, and be accountable for security?

|  |
| --- |
|  |

* 1. Is that person at least at a director level?

|  |
| --- |
|  |

* 1. Does your company have a dedicated security team? If so, roughly how many people are on it.

|  |
| --- |
|  |

* 1. Does your company have a corporate security policy?

|  |
| --- |
|  |

* 1. Are each of the following areas covered in your security policy?

1. Information Classification
2. Data privacy
3. Data-handling (including use, storage and destruction)
4. Email use and retention
5. Encryption
6. Security configuration for network, operating systems, applications and desktops
7. Change control
8. Network and User system access
9. Security incident management
10. Physical access
11. External communication
12. Asset management

|  |
| --- |
|  |

* 1. Are your systems subjected to penetration testing? Is testing performed by internal personnel or outsourced? When was the last penetration test? What were the results?

|  |
| --- |
|  |

* 1. Which of the policies above have been substantially modified in the past year?

|  |
| --- |
|  |

* 1. Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?

|  |
| --- |
|  |

* 1. Are the policies communicated in a way that requires employees to certify their understanding and compliance at least annually?

|  |
| --- |
|  |

* 1. Do the security policies apply to contract employees (offsite and onsite), dependent Service Providers, etc.?

|  |
| --- |
|  |

* 1. Is there a security training and awareness program in place for all employees (new, existing, permanent, temporary, or contract staff)? If yes, describe the program and frequency of re-certification or re-education.

|  |
| --- |
|  |

* 1. Is there a formal procedure for reporting a suspected security violation?

|  |
| --- |
|  |

* 1. Is the identity and background of all your staff servicing customer known based on security background checks? If yes, describe the screening activities performed on job applicants (e.g., credit, drug screening, references, and criminal background checks) and provide a copy of the policy, procedure, or checklist.

|  |
| --- |
|  |

* 1. Are employees with access to sensitive information prevented from working prior to completion of the background checks?

|  |
| --- |
|  |

* 1. Are re-investigations conducted on employees based on job function or length of employment? If yes, describe the re-investigations process performed (e.g., credit, drug screening, references, and criminal background checks).

|  |
| --- |
|  |

* 1. Is there a process in place to screen your outside contractors such as security guards, janitorial services, etc.? If yes, describe the process used to screen these individuals (e.g., credit, drug screening, references, and criminal background checks).

|  |
| --- |
|  |

* 1. Does your organization scan and/or test for vulnerabilities in your service / application, and if so, how quickly are any identified vulnerabilities remediated? Please provide as much detail in your answer as possible.

|  |
| --- |
|  |

* 1. Does your organization embrace and incorporate the best practices and recommendations provided in the OWASP Developer’s Guide and OWASP Cheat Sheet Series to implement or enhance your secure software engineering? Please provide as much detail in your answer as possible.

|  |
| --- |
|  |

* 1. Does your organization utilize the OWASP Testing Guide and/or OWASP Code Review Guide to effectively find vulnerabilities in your service / application (with the intent of remediating identified vulnerabilities)? Please provide as much detail in your answer as possible.

|  |
| --- |
|  |

* 1. Can you provide a copy of your most recent vulnerability scan results?

|  |
| --- |
|  |

* 1. Can you provide a scan that identified issue(s), and provide the follow-up scan that shows the issue(s) resolved? Please ensure that dates are clearly listed on each report.

|  |
| --- |
|  |

* 1. If you don't scan for vulnerabilities, how do you identify and remediate vulnerabilities? Please provide as much detail in your answer as possible.

|  |
| --- |
|  |

* 1. What concerns or considerations would you have, if any, to customer conducting periodic vulnerability scans of your service / application?

|  |
| --- |
|  |

* 1. How do you secure access to your data facilities where customer data will be stored?

|  |
| --- |
|  |

* 1. Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?

|  |
| --- |
|  |

* 1. How are these security controls monitored?

|  |
| --- |
|  |

* 1. Are the vendor premises separated into different control areas such as server / computer room, operation areas, loading / delivery areas, and others? Please specify how the access controls are in place in each separate area.

|  |
| --- |
|  |

* 1. Are multiple tenants occupying this facility? If yes, please specify how tenants are separated.

|  |
| --- |
|  |

* 1. Is access to areas where work is performed for customer physically separated from that of other clients? If yes, describe the separation.

|  |
| --- |
|  |

* 1. Is access to the facility controlled by the use of a token-based card access control system? If yes, describe the authorization process for requesting access, including changes.

|  |
| --- |
|  |

* 1. Are visitors required to sign-in, receive ID badge, and be escorted while on premises?

|  |
| --- |
|  |

* 1. Is the facility equipped with surveillance camera(s) 24/7/365?

|  |
| --- |
|  |

* 1. Do security cameras cover inside and outside doors and confidential areas?

|  |
| --- |
|  |

* 1. Are precautions taken to prevent the removing of customer information or related assets (checks, credit card information, storage media, hardware) from the premises? Please give details of these precautions.

|  |
| --- |
|  |

* 1. Are controls or safeguards in place to prevent unauthorized interception or damage to network, power or telecommunications cabling (e.g., wiring and router closets, etc.)?

|  |
| --- |
|  |

* 1. Please describe whether security guards are required to patrol areas that contain network, power, or telecommunications cabling (e.g., wiring and router closets, etc.).

|  |
| --- |
|  |

* 1. How do you secure access to conduits (e.g., wire, fiber, etc.)?

|  |
| --- |
|  |

* 1. How do you secure access to wire closets?

|  |
| --- |
|  |

* 1. Has a clear desk, clear screen policy been implemented where necessary to protect information in shared environments?

|  |
| --- |
|  |

* 1. How do you secure access to consoles that may display customer or cardholder information?

|  |
| --- |
|  |