|  |  |  |
| --- | --- | --- |
| State of Wisconsin  Department of Administration  Division of ENTERPRISE TECHNOLOGY  DOA-10816 (R05/2022) |  |  |

**VENDOR CLOUD SOLUTION INFORMATION**

**PURPOSE:** DOA has established the cloud brokerage process to conduct a comprehensive evaluation of security risks and compatibility for usage of the cloud solution. This form should be completed by the vendor providing the cloud solution.

**SCOPE:** This form should be completed and submitted prior to executing any written agreement to purchase, lease, or implement a cloud solution or purchasing or obligating funds to purchase a cloud solution. The cloud brokerage process is part of DOA’s statutory oversight responsibilities for State of Wisconsin executive branch agencies. This includes all State of Wisconsin executive branch agencies subject to DET oversight, which excludes the University of Wisconsin system (including campuses) and statutory authorities.

**DEFINITIONS:** Technical terms in this form are from the FEDRamp [Master Acronym and Glossary Document](https://www.fedramp.gov/assets/resources/documents/FedRAMP_Master_Acronym_and_Glossary.pdf) unless otherwise noted. Definitions for the terms “cloud computing,” “IaaS,” “PaaS,” and “SaaS” are from [NIST Special Publication 800-145](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf). Approval of IaaS and PaaS cloud solutions will be granted on a case-by-case basis where the agency can justify not using DET services.

**DESIGNATION OF CONFIDENTIAL AND PROPRIETARY INFORMATION:** The State of Wisconsin is subject to the Wisconsin Public Records Law ([Wis. Stat. §§ 19.31 to 19.39](https://docs.legis.wisconsin.gov/document/statutes/19.31)). As such, all records in the custody of the agency may be subject to disclosure under the Public Records Law. Vendors may use Appendix 1 at the end of this document to designate any confidential or proprietary information that should not be released under the Public Records Law. The two categories of information vendors may mark as confidential are cybersecurity information or trade secrets, as further explained and defined within Appendix 1 of this document. Vendors must include the number for each question response individually in Appendix 1 and cannot mark the entire document as confidential.

**NON-DISCLOSURE AGREEMENTS:** If a vendor wishes to execute a non-disclosure agreement with DET, please contact [DOADETCloudBrokerage@wisconsin.gov](mailto:DOADETCloudBrokerage@wisconsin.gov) for additional guidance.

**EXEMPTION FROM SECURITY QUESTIONS:** If a vendor provides a SOC 2 Type 2 document or FedRAMP certification document, questions 8 – 87 in the security section may be skipped unless the vendor would like to provide additional information. The vendor is still required to complete the General Section, Appendix 1, and sign the questionnaire before submission.

**DIRECTIONS:** All questions are required. Vendors should contact [DOADETCloudBrokerage@wisconsin.gov](mailto:DOADETCloudBrokerage@wisconsin.gov) with any questions regarding this form. The Cloud Brokerage Review form is to understand the security posture of the vendor, any implementation and integration solutions will need to be reviewed by DET Security Operations. Please submit a separate service request for implementation and integration permission review.

**GENERAL SECTION**

1. Provide the name of the product being evaluated: Click or tap here to enter text.

1. Provide the following information for the vendor and each subcontractor that will perform any work or process, transmit, or store any agency data:
   1. business name, United States headquarters address, and website.
   2. individual name, mailing address, direct phone number, and direct email address for the vendor point of contact.
   3. cities and states where work will be performed or where agency data will be processed, transmitted, or stored.

Click or tap here to enter text.

1. Provide a comprehensive list of vendor roles and responsibilities.

Click or tap here to enter text.

1. List all other state governments and state or local government agencies in Wisconsin using the cloud solution.

Click or tap here to enter text.

1. Provide the following information:
   1. If the vendor is headquartered in the United States, provide the state of incorporation: Click or tap here to enter text.
   2. If the vendor is headquartered outside the United States, provide the country where the vendor is incorporated: Click or tap here to enter text.
   3. For all vendors and subcontractors, provide the location of all cloud infrastructure where agency data will be processed, transmitted, or stored that is located outside the contiguous United States (this excludes Hawaii, Alaska, and United States territories): Click or tap here to enter text.
   4. For all vendors and subcontractors, provide all locations outside the contiguous United States where employees or contractors will have access to agency data: Click or tap here to enter text.
2. List all current IT and IT security certificates for the cloud solution (e.g. SOC 2 Type II, ISO 14001, ISO 27001, ITSM, etc.):

Click or tap here to enter text.

Please attach current copies of all IT and IT security certificates to this submission. If the certificates contain cybersecurity information or trade secrets as defined in Appendix 1 of this form, please attach both redacted and unredacted copies of certificates.

1. Mark if the cloud solution is FedRAMP Authorized or StateRAMP Authorized:

FedRAMP Authorized (provide authorization date and package ID): Click or tap here to enter text.

StateRAMP Authorized (provide authorization date): Click or tap here to enter text.

**SECURITY SECTION**

The State of Wisconsin operates on the [NIST SP 800-53 Revision 5](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf) security and privacy control framework, so vendors should utilize this framework in developing policies and procedures or be able to crosswalk policies and procedures to NIST SP 800-53 security and privacy controls. Questions are grouped below by NIST SP 800-53 control family and include relevant security and privacy controls in parentheses at the end of each question. Where any conflicts exist between the questions below and the requirements in NIST SP 800-53 Revision 5, the requirements in NIST SP 800-53 Revision 5 shall control. The identifiers listed in parentheses at the end of each question refer to corresponding NIST SP 800-53 security and privacy controls.

**IMPORTANT:** If a vendor provides a current SOC 2 Type II document or FedRAMP certification document, questions 8 – 87 may be skipped unless the vendor would like to provide additional information. The vendor is still required to complete the General Section, Appendix 1, and sign the questionnaire before submission.

Mark here if you are providing a SOC 2 Type II document or FedRAMP certification document and skipping questions 8 – 87 in the security section. Vendors may choose to provide additional information at their discretion.

*Access Control*

1. Summarize account management policies and procedures, including access control decisions, the types of accounts allowed and prohibited; processes for authorizing users, groups, roles, and access authorizations; processes for account provisioning, deprovisioning, and position changes; reviews for compliance with account management policies and procedures; processes for managing shared or group account authentication; and alignment with personnel termination and transfer policies. (AC-2)

Click or tap here to enter text.

1. Summarize access control policies and procedures. (AC-3)

Click or tap here to enter text.

1. Summarize information flow control policies and procedures. (AC-4)

Click or tap here to enter text.

1. Summarize policies and procedures for separation of duties, least privilege, unsuccessful logon attempts, device locking, session termination, permitted actions without identification or authentication, remote access (including VPN usage), use of external systems, and information sharing. (AC-5, AC-6, AC-7, AC-11, AC-12, AC-14, AC-17)

Click or tap here to enter text.

1. Summarize wireless network configuration measures to prohibit unauthorized traffic, protect wireless security settings, replace default settings, and detect and remove unauthorized wired and wireless networks. (AC-18)

Click or tap here to enter text.

1. Summarize policies and procedures to allow authorized individuals to access the cloud solution from external systems and process, store, and transmit data using external systems. (AC-20)

Click or tap here to enter text.

*Awareness and Training*

1. Summarize employee security awareness training procedures, including procedures for confirming employee compliance, incorporation of lessons learned, updates to curricula, role-based training, and maintenance of training records. (AT-2, AT-3, AT-4)

Click or tap here to enter text.

*Audit and Accountability*

1. Describe event types that are logged, the retention period by event type for all logs, the review process for adding or removing event types, and procedures for remediating audit logging process failures. (AU-2, AU-3, AU-4, AU-5)

Click or tap here to enter text.

1. Describe policies and procedures for maintaining, reviewing, analyzing, and reporting audit records, describe minimum required information that must be included, and provide the retention period for audit records. (AU-6, AU-11)

Click or tap here to enter text.

*Assessment, Authorization, and Monitoring*

1. Summarize policies and procedures governing the completion of independent security assessments. Include copies of the three most recently completed reviews. (CA-2)

Click or tap here to enter text.

1. Summarize policies and procedures for remediating identifying weaknesses and deficiencies identified through the security assessment process, including processes for verifying remediation. (CA-5)

Click or tap here to enter text.

1. Summarize penetration testing policies and procedures, including the frequency of testing, any events that would trigger off-cycle penetration testing, the organization conducting the testing, and the results of the most recent test. (CA-8)

Click or tap here to enter text.

*Configuration Management*

1. Summarize policies and procedures governing the baseline configuration of the system, the frequency and process for updating and cascading changes to the baseline configuration, and the process for configuring system components when they are installed or upgraded. (CM-2)

Click or tap here to enter text.

1. Describe the process for documenting changes to configuration-controlled components of the system, the security and privacy review process for reviewing and approving changes, the process for implementing changes, the process for recording changes, the process for monitoring and reviewing activities associated with changes, and the process for providing coordination and oversight to the change control process. (CM-3)

Click or tap here to enter text.

1. Summarize policies and procedures to establish and document configuration settings for system components that reflect the most restrictive mode possible within operational requirements, including processes to implement the settings, processes to document and approve deviations from established settings, and processes to monitor and control settings. (CM-6)

Click or tap here to enter text.

1. Summarize policies and procedures to harden information systems to provide only ports, protocols, and services necessary to meet business needs using technical controls. (CM-7)

Click or tap here to enter text.

1. Summarize policies and procedures to maintain an up-to-date inventory of system components that accurately reflects the system, includes all system components, is sufficiently granular for tracking and reporting, provides appropriate accountability, and notes the frequency of reviews and updates. (CM-8)

Click or tap here to enter text.

1. Summarize policies and procedures for configuration management planning, including roles, responsibilities, processes, and procedures. (CM-9)

Click or tap here to enter text.

1. Summarize policies and procedures for the appropriate use of software and user installation of software. (CM-10, CM-11)

Click or tap here to enter text.

*Contingency Planning*

1. Summarize contingency planning policies and procedures, which must identify essential mission and business functions and contingency requirements; recovery time objectives and recovery point objectives; roles, responsibilities, and assigned individuals; restoration policies and procedures; and the sharing of contingency information. (CP-2)

Click or tap here to enter text.

1. Summarize policies and procedures for testing contingency plans, including a description of the tests conducted, the process for reviewing test results, and the development and completion of corrective action plans. (CP-4)

Click or tap here to enter text.

1. Summarize policies and procedures for conducting system backups of user-level information, system-level information, and system documentation, including the frequency of such backups necessary to maintain the recovery time objectives and recovery point objectives noted above and measures to maintain the confidentiality, integrity, and availability of backup information. (CP-9)

Click or tap here to enter text.

1. Summarize policies and procedures to recover and reconstitute the system to a known state following a disruption, compromise, or failure, including the time allowed for doing so in line with the recovery time and recovery point objectives noted above. (CP-10)

Click or tap here to enter text.

*Identification and Authentication*

1. Summarize policies and procedures for identifying and authenticating vendor-utilized devices before establishing a system connection, Explain, if different, procedures for local, remote, and network access. (IA-3)

Click or tap here to enter text.

1. Summarize policies and procedures for managing system identifiers, including reviewing authorization from designated employees to assign individual, group, role, service, or device identifiers, selecting an identifier, assigning an identifier, and preventing reuse of identifiers. (IA-4)

Click or tap here to enter text.

1. Summarize policies and procedures for managing system authentication by verifying the identity of the individual, group, role, service, or device receiving the authenticator, establishing authenticator content, ensuring that authenticators have sufficient strength, changing default authenticators prior to first use, providing the time period or events that trigger changing or refreshing authenticators by user type, protecting authenticator content from unauthorized disclosure and modification, requiring specific controls to protect authenticators, and changing authenticators when membership in group or role accounts change. (IA-5)

Click or tap here to enter text.

1. Summarize policies and procedures for obscuring feedback of authentication information to protect information from possible exploitation and use by unauthorized individuals. (IA-6)

Click or tap here to enter text.

1. Summarize policies and procedures for identifying and authenticating non-organizational users and processes. (IA-8)

Click or tap here to enter text.

1. Summarize policies and procedures for requiring individuals accessing the system to use supplemental authentication under certain circumstances or situations, including the circumstances or situations that require additional authentication. (IA-10)

Click or tap here to enter text.

*Incident Response*

1. Summarize policies and procedures for providing role-based training to system users regarding incident response, including the time allowed to receiving incident response training upon assuming an incident response role or acquiring system access, when required by system changes, the minimum frequency for additional training, and the frequency with which training content is reviewed and updated. (IR-2)

Click or tap here to enter text.

1. Summarize policies and procedures for testing incident response capabilities, including the frequency for such testing and the tests used. (IR-3)

Click or tap here to enter text.

1. Summarize policies and procedures for handling incidents consistent with the incident response plan, including coordination of incident handling and contingency planning activities, incorporating lessons learned from prior and ongoing incident handling activities, making changes to policies, procedures, training, and testing based on lessons learned, and ensuring the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization. (IR-4)

Click or tap here to enter text.

1. Summarize policies and procedures for the development and maintenance of an incident response plan, including a roadmap for implementing incident response, the structure and organization for the incident response capability, how the incident capability fits within the overall organization, meets the requirements of the organization, defines incidents that must be reported, measures incident response capability, defines resources and management support required to maintain and mature the incident response capability, addresses sharing of incident information, the frequency of and position responsible for incident response plan review and approval, designation of responsibility for incident response, distribution of the incident response plan, triggers that result in updates to the incident response plan, communication of incident response plan changes, and protection of the incident response plan from unauthorized modification and disclosure. (IR-8)

Click or tap here to enter text.

*Maintenance*

1. Summarize policies and procedures for scheduling, documenting, and reviewing maintenance, repair, and replacement of system components in line with manufacturer or vendor specifications and organizational requirements. (MA-2)

Click or tap here to enter text.

1. Summarize policies and procedures for approving, controlling, and monitoring the use of system maintenance tools and reviewing previously-approved updates to system maintenance tools. (MA-3)

Click or tap here to enter text.

1. Summarize policies and procedures for approving and monitoring nonlocal maintenance and diagnostic activities, allowing the use of nonlocal maintenance and diagnostic tools, employing strong authentication in the establishment of nonlocal maintenance and diagnostic sessions, and terminating connections when nonlocal maintenance is completed. (MA-4)

Click or tap here to enter text.

1. Summarize policies and procedures for obtaining support and parts for system components within a specified time period of failure, including a list of components and the time period by which support and parts will be obtained. (MA-6)

Click or tap here to enter text.

*Media Protection*

1. Summarize policies and procedures for restricting access to system media to authorized personnel and roles, marking system media to indicate distribution limitations, handling caveats, and security markings, marking exemption requirements for system media within defined areas, and control and secure storage measures for system media within defined areas until appropriate destruction and sanitization. (MP-2, MP-3, MP-4)

Click or tap here to enter text.

1. Summarize policies and procedures for transporting system media outside defined areas, including accountability for system media during transport out of defined areas, documentation of transport activities outside defined areas, and restriction of transport activities to authorized personnel. (MP-5)

Click or tap here to enter text.

1. Summarize policies and procedures for sanitizing system media prior to disposal, release by the organization, or release for reuse by the organization, including mechanisms to ensure that sanitization is commensurate with the security category or classification of the information on the system media. (MP-6)

Click or tap here to enter text.

1. Summarizing policies and procedures restricting or prohibiting the use of certain system media on system components and prohibiting the use of portable storage devices without an identifiable owner, including all types of system media that are restricted or prohibited. (MP-7)

Click or tap here to enter text.

*Physical and Environmental Protection*

1. Summarize policies and procedures to develop, approve, and maintain a list of individuals with authorized access to the facility where the system is housed, issuing credentials for facility access, the frequency with which the access list is review, the removal of individuals from the list who no longer require access, the enforcement of physical access authorizations, the maintenance of physical access audit logs, controls for publicly-accessible areas of the facility, visitor escorting and visitor controls, secure keys, combinations, and other physical access devices, inventory all physical access devices within a specified time period, changing combinations and keys within a specific time period or when physical access devices are lost, compromised, when individuals possessing physical access devices are transferred or terminated, monitor physical access to the facility, respond to physical security incidents at the facility, review physical access logs within a specified time period or upon event triggers, and coordinating reviews and investigations with the incident response capability. (PE-2, PE-3, PE-6, PE-8)

Click or tap here to enter text.

1. Summarize policies and procedures for protection of power equipment and cabling, emergency power shutoff, emergency power in the event of a primary power source loss, automatic emergency lighting, fire detection and suppression systems, environmental controls, water damage protection, delivery, and removal of system components from the facility, and the establishment of alternate work sites, and the employment and enforcement of controls at alternate work sites. (PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, PE-17)

Click or tap here to enter text.

*Risk Assessment*

1. Summarize policies and procedures for conducting risk assessments, including identification of system threats and vulnerabilities, determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and related information, determining the likelihood and impact of adverse effects on individuals arising from the processing of PII, integrating risk assessment results and risk management decisions and mission or business process perspectives with system-level risk assessments, documenting and disseminating risk assessment results, and updating the risk assessment within a specific time period or when there are significant changes to the system, its environment of operation, or other conditions that may affect the security or privacy state of the system. (RA-3)

Click or tap here to enter text.

1. Summarize policies and procedures for monitoring and scanning for vulnerabilities in the system and hosted applications within a specific time period or randomly in line with established processes, employing vulnerability monitoring tools and techniques that facilitate interoperability and automate parts of the vulnerability monitoring process by using standards for enumerating platforms, system flaws, and improper configurations, formatting checklists and test procedures, analyzing vulnerability scan reports and results from vulnerability monitoring, remediating legitimate vulnerabilities within specific response times in accordance with relevant risk assessments, sharing information obtained from the vulnerability monitoring process and control assessments with personnel or roles to help eliminate similar vulnerabilities, and employing vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned. (RA-5)

Click or tap here to enter text.

1. Summarize policies and procedures for remediation to findings from security and privacy assessment in accordance with established risk tolerance. (RA-7)

Click or tap here to enter text.

*System and Services Acquisition*

1. Summarize policies and procedures for acquiring, developing, and managing the system using the system development life cycle that incorporates information security and privacy considerations, defining and documenting information security and privacy roles and responsibilities, and integrates the information security and privacy risk management process into system development life cycle activities. (SA-3)

Click or tap here to enter text.

1. Summarize policies and procedures for applying system security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components, including the principles utilized. (SA-8)

Click or tap here to enter text.

1. Summarize policies and procedures that require the developer of the system, system component, or system service to perform configuration management during system, component, or service design, development, implementation, operation, and disposal, document, manage, and control the integrity of all configuration items under configuration management, implement only approved changes to the system, component, or service, document approved changes to the system, component, or service, including the security and privacy impacts of such changes, and track security flaws and flaw resolution within the system, component, or service, and report findings to personnel.(SA-10)

Click or tap here to enter text.

1. Summarize policies and procedures that require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to develop and implement a plan for ongoing security and privacy control assessments, perform unit, integration, system, and regression testing within a specified time period at a defined depth and coverage, produce evidence of the execution of the assessment plan and the results of the testing and evaluation, implement a verifiable flaw remediation process, and correct flaws identified during testing and evaluation. (SA-11)

Click or tap here to enter text.

1. Summarize policies and procedures that require the developer of the system, system component, or system service to follow a documented development process that explicitly addresses security and privacy requirements, identifies the standards and tools used in the development process, documents the specific tools options and tool configurations used in the development process, documents, manages, and ensure the integrity of changes to the process or tools used in development, and review the development process, standards, tools, tool options, and tool configurations within a specified time period to determine if the process, standard, tools, tool options, and tool configurations selected and employed can satisfy defined security and privacy requirements. (SA-15)

Click or tap here to enter text.

1. Summarize policies and procedures that require the replacement of system components when support for the components is no longer available from the developer, vendor, or manufacturer, or provide the following options for continued support for unsupported components, including in-house support or defined support from external providers. (SA-22)

Click or tap here to enter text.

*System and Communications Protection*

1. Summarize policies and procedures that prevent unauthorized and unintended information transfer via shared system resources. (SC-4)

Click or tap here to enter text.

1. Summarize policies and procedures for monitoring and controlling communications at the external managed interfaces within the system, implementing subnetworks for publicly-accessible system components that are physically or logically separated from internal organizational networks, and connecting to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with the security and privacy architecture. (SC-7)

Click or tap here to enter text.

1. Summarize policies and procedures to protect the confidentiality and integrity of transmitted information. (SC-8)

Click or tap here to enter text.

1. Summarize policies and procedures for establishing and managing cryptographic keys when cryptography is employed within the system in accordance with defined requirements for key generation, distribution, storage, access, and destruction. (SC-12)

Click or tap here to enter text.

1. Summarize policies and procedures for determining cryptographic uses and implementing cryptography for each specific cryptographic use. (SC-13)

Click or tap here to enter text.

1. Summarize policies and procedures prohibiting remote activation of collaborative computing devices and applications with defined exceptions and provide an explicit indication of use to users physically present at the devices. (SC-15)

Click or tap here to enter text.

1. Summarize policies and procedures for issuing public key certificates under a defined certificate policy or obtaining public key certificates from an approved service provider and include only approved trust anchors in trust stores or certificate stores. (SC-17)

Click or tap here to enter text.

1. Summarize policies and procedures for providing additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution inquiries and providing the means to indicate the security status of child zones and to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. (SC-20)

Click or tap here to enter text.

1. Summarize policies and procedures for requesting and performing data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. (SC-21)

Click or tap here to enter text.

1. Summarize policies and procedures for ensuring the systems that collectively provide name/address resolution service are fault-tolerant and implement internal and external role separation. (SC-22)

Click or tap here to enter text.

1. Summarize policies and procedures to protect the confidentiality and integrity of information at rest. (SC-28)

Click or tap here to enter text.

1. Summarize policies and procedures for partitioning the system residing in separate physical and logical domains or environments based on defined circumstances for physical and logical separation of components. (SC-32)

Click or tap here to enter text.

1. Summarize policies and procedures for implementing hardware-enforced and software-enforced separation and policy enforcement mechanisms. (SC-49, SC-50)

Click or tap here to enter text.

*System and Information Integrity*

1. Summarize policies and procedures for identifying, reporting, and correcting system flaws, testing software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation, installing security-relevant software and firmware updates within a specified time period of the release of the updates, and incorporating flaw remediation into the organizational configuration management process. (SI-2)

Click or tap here to enter text.

1. Summarize policies and procedures for implementing malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code, automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures, configuring malicious code protection mechanisms to perform periodic scans of the system within a specified frequency and real-time scans of files from external sources at endpoint and network entry and exit points as files are downloaded, opened, or executed, and block or quarantine malicious code take a certain action, and send an alert to defined personnel or roles in response to malicious code detection, and addressing the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system. (SI-3)

Click or tap here to enter text.

1. Summarize policies and procedures for monitoring the system to detect attacks and indicators of potential attacks in accordance with defined monitoring objectives and unauthorized local, network, and remote connections, identify unauthorized use of the system through defined techniques and methods, invoke internal monitoring capabilities or deploy monitoring devices strategically within the system to collect essential information and at ad hoc locations within the system to track specific transactions of interest, analyze detected events and anomalies, adjust the level of system monitoring activity when there is a change in risk to operations and assets, individuals other organizations, or the Nation, obtain legal opinion regarding system monitoring activities, and provide monitoring information to defined personnel or roles as needed or within a specified frequency. (SI-4)

Click or tap here to enter text.

1. Summarize policies and procedures to employ integrity verification tools to detect unauthorized changes to software, firmware, and information, and take defined actions when unauthorized changes to the software, firmware, and information are detected. (SI-7)

Click or tap here to enter text.

1. Summarize policies and procedures to employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages and update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. (SI-8)

Click or tap here to enter text.

1. Summarize policies and procedures to validate information inputs. (SI-10)

Click or tap here to enter text.

1. Summarize policies and procedures to generate error messages that provide information necessary for correction actions without revealing information that could be exploited and reveal error messages only to defined personnel. (SI-11)

Click or tap here to enter text.

1. Summarize policies and procedures to implement the following controls to protect the system memory from unauthorized code execution. (SI-16)

Click or tap here to enter text.

*Supply Chain Risk Management*

1. Summarize policies and procedures for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems, system components, and system services, reviewing and updating the supply chain risk management plan within a specific frequency or as required to address threat, organizational, or environmental changes, and protecting the supply chain risk management plan from unauthorized disclosure and modification. (SR-2)

Click or tap here to enter text.

1. Summarize policies and procedures for establishing a process or processes to identify and address weaknesses in supply chain elements and processes, employ defined controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events, and documenting the selected and implemented supply chain processes and controls in the security and privacy plan, supply chain risk management plan, and other defined documents. (SR-3)

Click or tap here to enter text.

1. Summarize policies and procedures to employ defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks. (SR-5)

Click or tap here to enter text.

1. Summarize policies and procedures to assess and review the supply-chain related risks associated with suppliers and contractors and the system, system component, or system service they provide within a defined frequency. (SR-6)

Click or tap here to enter text.

1. Summarize the policies and procedures for establishing agreements and procedures with entities involved in the supply chain for the system, system component, or system service for notification of supply chain compromises, results of assessments or audits, or other defined information. (SR-8)

Click or tap here to enter text.

1. Summarize the policies and procedures to develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system and report counterfeit system components to the source of the counterfeit component, external reporting organizations, and defined personnel. (SR-11)

Click or tap here to enter text.

1. Summarize the policies and procedures to dispose of data, documentation, tools, or system components using defined techniques and methods. (SR-12)

Click or tap here to enter text.

**APPENDIX 1: DESIGNATION OF CONFIDENTIAL OR PROPETIARY INFORMATION**

This questionnaire contains confidential or proprietary information which qualifies as cybersecurity information or a trade secret:

*Cybersecurity information*, which is defined as information that, if released, would significantly compromise the vendor’s ability to secure the cloud solution against unauthorized access, including unauthorized access to individuals’ personally identifiable information or to other information that is confidential pursuant to statutory or regulatory requirements.

*Trade secrets*, as defined under Wisconsin law in [Wis. Stat. § 134.90(1)(c)](https://docs.legis.wisconsin.gov/document/statutes/134.90(1)(c)).

As such, we request that our responses to certain questions, designated by question number below, of this questionnaire be treated as confidential material and not be released without our written approval. We understand that marking the entire questionnaire without specifying specific question numbers below may result in portions of the questionnaire being released. We further understand that markings within the questionnaire itself will not be considered.

We request that our responses to the following question numbers not be released:

Cybersecurity Information

Click or tap here to enter text.

Trade Secrets

Click or tap here to enter text.

If submitting other documents along with the questionnaire which contain cybersecurity information or trade secrets that should be treated as confidential, we have checked the box below and have submitted a redacted and unredacted copy of each document.

I certify that the documents submitted with this questionnaire contain cybersecurity information or trade secrets and both a redacted copy and an unredacted copy are being submitted.

**SIGNATURE STATEMENT**

I attest that the information in this questionnaire and any attached documents is complete and accurate to the best of my knowledge and that I am authorized to sign this document on behalf of the vendor listed in Question 1 in the General Section of this questionnaire.

I certify that all information marked as confidential or proprietary in Appendix 1 of this document, along with all information marked in the redacted copy of any documents submitted with this questionnaire, is either a trade secret or cybersecurity information as defined in Appendix 1 of this document. I am asking that the information marked as confidential or proprietary in Appendix 1 of this document be treated as confidential material and not be released without our written approval.

In the event that the confidentiality of the information I have marked is challenged, the vendor will provide legal counsel or other necessary assistance to defend the designation of confidentiality and agrees to hold the state harmless for any costs or damages arising out of the State’s agreeing to withhold the materials.

Failure to mark information as confidential or proprietary in Appendix 1 of this document may mean that the information not marked will be open to examination and copying. The State considers other markings of confidential or proprietary in the questionnaire to be insufficient. The undersigned agrees to hold the state harmless for any damages arising out of the release of any materials unless they are specifically designated in Appendix 1 of this document.

If I subsequently identify any inaccurate or incomplete information, I will immediately contact the Division of Enterprise Technology at [DOADETCloudBrokerage@wisconsin.gov](mailto:DOADETCloudBrokerage@wisconsin.gov).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Click or tap here to enter text.

Position: Click or tap here to enter text.

Agency: Click or tap here to enter text.

Direct Phone Number: Click or tap here to enter text.

E-mail Address: Click or tap here to enter text.