Non-Conformance with Privacy and Data Protection Guidelines

\_\_# of weaknesses have been detected that represent source vectors for unauthorized access to read or modify data and represent indicators of data leakage or data corruption. If the software is running as part of a network-connected asset, then the organizational enterprise is at risk of not being conformant with CMMC, GDPR, CCPA, or HIPAA regulatory requirements.

1. With these weaknesses present in software, the following NIST SP 800-171 Rev 2 Security Requirements are at risk of not being properly implemented or supported:

|  |
| --- |
| 3.1 ACCESS CONTROL  3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)  3.1.2. Limit systems access to the types of transactions and functions that authorized users are permitted to execute  3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts  3.1.7. Prevent non-privileged accounts or roles when accessing non-security functions  3.1.8. Limit unsuccessful logon attempts  3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity  3.4 CONFIGURATION MANAGEMENT  3.4.8. Apply deny-by-exception (blacklisting) policy or prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software  3.5 IDENTIFICATION AND AUTHENTICATION  3.5.5. Prevent reuse of identifiers for a defined period  3.5.6. Disable identifiers after a defined period of inactivity  3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created  3.11 RISK ASSESSMENT  3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.  3.11.3. Remediate vulnerabilities in accordance with risk assessments  3.12 SECURITY ASSESSMENT  3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application  3.13 SYSTEM AND COMMUNICATIONS PROTECTION  3.13.1. Monitor, control and protect communications (ie., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems  3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security with organizational systems  3.13.4. Prevent unauthorized and unintended information transfer via shared system resources  3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of confidential unclassified information during transmission unless otherwise protected by alternative physical safeguards  3.13.13. Control and monitor the use of mobile code  3.13.16. Protect the confidentiality of CUI at rest  3.14 SYSTEM AND INFORMATION SECURITY  3.14.1. Identify, report, and correct system flaws in a timely manner |

2. With these weaknesses present in software in network-connected assets, the following NIST SP 800-53 Controls are at risk of not being properly implemented:

|  |
| --- |
| AC-3 Access Enforcement  AC-6 Least Privilege  AC-6(10) Least Privilege (prohibit non-privileged users from executing privileged functions)  AC-7 Unsuccessful Logon Attempts  AC-11 Session Lock  AC-17 Remote Access  CM-7(4) Least Functionality (Unauthorized Software / Blacklisting)  CM-7(5) Least Functionality (Authorized Software / Whitelisting)  IA-4 Identifier Management  IA-5(1) Authenticator Management (Password-Based Authentication)  RA-5 Vulnerability Scanning  RA-5(5) Vulnerability Scanning (Privileged Access)  CA-2 Security Assessments  SC-7 Boundary Protection  SA-8 Security Engineering Principles  SC-4 Information in Shared Resources  SC-8 Transmission Confidentiality and Integrity  SC-18 Mobile Code  SC-28 Protection of Information at Rest  SI-1 Flaw Remediation |

3. With these weaknesses present in software in a network-connected asset, the following ISO/IEC 27001 Controls are at risk of not being properly implemented:

|  |
| --- |
| A.8.2.3. Handling of Assets  A.9.2.1. User registration and de-registration  A.9.4.1. Information access restrictions  A.9.4.2. Secure logon procedures  A.9.4.5. Access control to program source code  A.11.2.8. Unattended user policy  A.12.6.1. Management of technical vulnerabilities  A.14.1.2. Securing application services on public networks  A.14.1.3. Protecting application services transactions  A.14.2.5. Secure system engineering principles  A.14.2.8. System security testing  A.16.1.3. Reporting information security weaknesses  A.18.1.3. Protection of records |