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 CONTROL3.1.1. 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 execute3.1.5. Employ the principle of least privilege, including for specific security functions and privileged accounts3.1.7. Prevent non-privileged accounts or roles when accessing non-security functions3.1.8. Limit unsuccessful logon attempts3.1.10. Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity3.4 CONFIGURATION MANAGEMENT3.4.8. 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 software3.5 IDENTIFICATION AND AUTHENTICATION3.5.5. Prevent reuse of identifiers for a defined period3.5.6. Disable identifiers after a defined period of inactivity3.5.7. Enforce a minimum password complexity and change of characters when new passwords are created3.11 RISK ASSESSMENT3.11.2. 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 assessments3.12 SECURITY ASSESSMENT3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application3.13 SYSTEM AND COMMUNICATIONS PROTECTION3.13.1. Monitor, control and protect communications (ie., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems3.13.2. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security with organizational systems3.13.4. Prevent unauthorized and unintended information transfer via shared system resources3.13.8. Implement cryptographic mechanisms to prevent unauthorized disclosure of confidential unclassified information during transmission unless otherwise protected by alternative physical safeguards3.13.13. Control and monitor the use of mobile code3.13.16. Protect the confidentiality of CUI at rest3.14 SYSTEM AND INFORMATION SECURITY3.14.1. 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 EnforcementAC-6 Least PrivilegeAC-6(10) Least Privilege (prohibit non-privileged users from executing privileged functions)AC-7 Unsuccessful Logon AttemptsAC-11 Session LockAC-17 Remote AccessCM-7(4) Least Functionality (Unauthorized Software / Blacklisting) CM-7(5) Least Functionality (Authorized Software / Whitelisting)IA-4 Identifier ManagementIA-5(1) Authenticator Management (Password-Based Authentication)RA-5 Vulnerability Scanning RA-5(5) Vulnerability Scanning (Privileged Access)CA-2 Security AssessmentsSC-7 Boundary ProtectionSA-8 Security Engineering PrinciplesSC-4 Information in Shared ResourcesSC-8 Transmission Confidentiality and IntegritySC-18 Mobile CodeSC-28 Protection of Information at RestSI-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 AssetsA.9.2.1. User registration and de-registrationA.9.4.1. Information access restrictions A.9.4.2. Secure logon proceduresA.9.4.5. Access control to program source code A.11.2.8. Unattended user policyA.12.6.1. Management of technical vulnerabilities A.14.1.2. Securing application services on public networksA.14.1.3. Protecting application services transactionsA.14.2.5. Secure system engineering principles A.14.2.8. System security testingA.16.1.3. Reporting information security weaknessesA.18.1.3. Protection of records |