IT-3047 Third-Party Vendor and Business Associate Security Policy

Purpose

To establish policy governing security requirements for all Third Party Vendors and Business Associates.

Scope

All Memorial Sloan-Kettering Cancer Center ("MSKCC") third-party vendors/business associates ("BA") are required to implement, test and continually monitor the administrative, physical, and technical controls outlined below to protect MSKCC Sensitive Data (including, but not limited to, Protected Health Information, Financial Data, Credit Card information, and Employee Data.).

The security controls described below are required in addition to any requirements as set forth by Health Insurance Portability and Accountability Act ("HIPAA"), Payment Card Industry Data Security Standards ("PCI-DSS") or other applicable regulations. Satisfactory compliance with these Security requirements is predicated upon the completion of a Security Assessment conducted by the MSKCC Information Security Office. Periodic re-assessments may be required to ensure continued compliance with MSKCC Security requirements.

Policy

1. Authentication and Access Control
    a. Vendor/BA must have a formal, documented process for granting and revoking access to all systems that process or store MSKCC Sensitive Data.
        i. Vendor/BA user access rights shall be strictly limited to a need-to-know basis that permits access only to the systems and resources that are required for users to perform their duties.
        ii. All Vendor/BA users with authorized access to MSKCC Sensitive Data must be assigned a unique User ID which must not be shared with any other individual.
    b. For single-factor authentication solutions, passwords managed by Vendor/BA or implemented within Vendor/BA-provided applications that are used to authenticate to systems processing or storing MSKCC Sensitive Data must meet or exceed the following minimum requirements:
        i. All passwords shall have at least eight (8) characters. Applications not integrated with MSKCC Active Directory must technically enforce this requirement.
        ii. Passwords shall contain at least one alphabetic and one non-alphabetic character. Non-alphabetic characters include numbers (0-9) and punctuation.
        iii. Passwords shall not be constructed of a single word found in the dictionary. Passphrases constructed of multiple words are acceptable as long as they meet the other criteria outlined in this section.
        iv. Users shall not be permitted to construct passwords that are identical or substantially similar to passwords that they had previously employed.

v. Passwords and any application or system passwords protecting sensitive MSKCC data shall be changed at least every 12 months.

vi. Passwords must be hashed (with unique salts) and stored securely. In addition, any public-facing systems must use a slow hashing algorithm that implements a work factor (such as PBKDF2, bcrypt, or scrypt). Clear text storage or reliance only on reversible encryption algorithms to protect passwords is not authorized. Authenticators used in multi-factor authentication mechanisms (such as PKI or biometrics) must be afforded the same secure storage protections.

c. Access rights will be revoked immediately upon termination of any Vendor/BA user with access to MSKCC systems or resources or in the event that a change in job role eliminates the requirement for continued access.

d. All access rights must be reviewed by Vendor/BA no less frequently than once annually.

e. All Vendor/BA user access to systems storing MSKCC Sensitive Data must be audited and those audit records be maintained and made available to MSKCC upon request.

2. Data Transmission Confidentiality and Integrity

a. All MSKCC Sensitive Data transmitted by Vendor/BA will be protected with a transmission encryption solution that complies, as appropriate, with NIST Special Publications 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

i. Approved solutions are limited to those that have been issued a FIPS 140-2 Validation Certificate.

ii. Data transmissions include, but are not limited to web transmissions, file transfers, and email.

3. Media Protection, Sanitization and Destruction

a. All MSKCC Sensitive Data stored by Vendor/BA will be protected with a data-at-rest encryption product utilizing a Validated FIPS 140-2 Cryptographic Module with a 128-bit key or higher.

i. *Removable media and mobile devices will not be used by Vendor/BA users to store or transport any MSKCC Sensitive data unless explicitly approved, in writing, by MSKCC. Such approved* solutions will be limited to those that have been issued a FIPS 140-2 Validation Certificate.

ii. Applicable data storage includes (but is not limited to) storage of Sensitive Data on servers, workstations, and backup media (disk or tape) as well as any approved storage of Sensitive Data on removable media or mobile devices (to include phones, tablets, CD/DVD, USB thumb drives).

b. Upon termination of the contract with MSKCC or at any time prior to reuse or repurposing of media used to store or process MSKCC Sensitive Data, said media must be cleared (using a DoD-compliant 7-pass wipe) or purged in accordance with NIST SP 800-88.

i. If the media is to be destroyed, the method used must ensure that after destruction, the media is able to withstand a laboratory attack as outlined in NIST SP 800-88.
ii. Vendor/BA must provide a certificate of destruction if requested by MSKCC.

4. System Security and Vulnerability Management
    a. Vendor/BA must have a documented patch management and distribution process that ensures security patches are applied to all systems (to include servers, workstations, laptops) that process and/or store MSKCC Sensitive Data. *Note that FDA-governed medical devices are not exempt from this requirement and must be patched.*
        i. All applicable security patches must be deployed within 30 days of vendor release unless otherwise discussed and approved, in writing, by the MSKCC Information Security Office.
    b. Vendor/BA must employ network security architectural components (to include, at a minimum, firewalls and network intrusion detection/prevention solutions) to adequately protect all systems processing or storing MSKCC Sensitive Data that are accessible from the Internet or other public network.
    c. Vendor/BA must employ an anti-virus solution with real-time protection and automatic updates on all systems that store or process MSKCC Sensitive Data.
    d. Vendor/BA will ensure any web-based solutions storing or processing MSKCC Sensitive Data will adhere to security design best-practices including, but not limited to, protecting against the Open Web Application Security Project OWASP Top 10 list of security risks.
5. Auditing
    a. All systems that process or store MSKCC Sensitive Data must maintain an automated audit trail that documents system security events as well as any event that results in the access, modification, and/or deletion of MSKCC Sensitive Data.
    b. The audit trail must, at a minimum record the following information for each event:
        i. type of event occurred
        ii. when (date and time) the event occurred
        iii. the source of the event
        iv. the outcome (success or failure) of the event
        v. the identity of any user/subject associated with the event.
    c. Audit logs must be read-only and protected from unauthorized access. Audit records documenting events resulting in the access, modification, and/or deletion of MSKCC Sensitive Data must be made available to MSKCC upon request.
    d. Vendor/BA must employ a regular audit log review process (either manually or automated) for detection of unauthorized access to MSKCC Sensitive Data.
6. Remote Access
    a. Vendor/BA must sign a Third-Party Remote Access Agreement before being granted remote access to any MSKCC information systems or resources

   b. Unless otherwise explicitly approved and documented by the MSKCC Information Security Office, all remote access must occur using the MSKCC VPN solution or MeetMSK WebEx as outlined in the Remote Access Agreement.
7. Physical Security
   a. In addition to the previously mentioned technical controls, Vendor/BA must employ physical safeguards and visitor access controls to prevent unauthorized access to all systems and media used to process or store MSKCC Sensitive Data.
8. Awareness and Training
   a. Vendor/BA must ensure all Vendor/BA users receive regular security awareness training and are apprised of the requirements outlined within this agreement.

Contact Information

For more information regarding this policy, contact the Information Security Office.