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

Purpose
The purpose of this policy is to establish minimum security requirements for all Third-Party Vendors and Business Associates.

Scope
All Memorial Sloan-Kettering Cancer Center ("MSK") Third-Party Vendors/Business Associates (collectively "Vendors") are required to implement, test, and continually monitor the administrative, physical, and technical controls outlined below to protect MSK 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"), and any other applicable regulations. Satisfactory compliance with these security requirements is predicated upon the completion of a security assessment conducted by the MSK Information Security Office. Periodic re-assessments may be required to ensure continued compliance with MSK security requirements.

Authority and Governance
This policy is written and released by the MSK Information Security Office under the authority of the IT Governance Committee.

Policy
1. Authentication and Access Control
    a. Vendor must have formal, documented procedures governing the authorization, provisioning, review, and revocation of access to all systems managed by Vendor, its employees, contractors, or agents which access, process, or store MSK Sensitive Data.
        i. Vendor must ensure user access rights are strictly limited to a "need-to-know" basis that permits access only to the systems, functionality, and data required for its workforce members to perform their duties.
        ii. Vendor must ensure user access to MSK Sensitive Data is authenticated and limited to unique, individually assigned, non-shared User IDs.
        iii. Vendor must ensure access rights are revoked immediately upon termination of any Vendor employee, contractor, or agent with access to MSK systems, data, or other information resources or in the event that a change in job role eliminates the requirement for continued access.
        iv. Vendor must review all provisioned access rights at least annually.
    b. Vendor must ensure passwords used to authenticate to Vendor systems that process or store MSK Sensitive Data meet or exceed the following minimum requirements.

i. Passwords must have at least eight (8) characters. Applications not integrated with the MSK Active Directory must technically enforce this requirement.
ii. Passwords must contain at least one alphabetic and one non-alphabetic (numbers, punctuation, etc.) character. Applications not integrated with the MSK Active Directory must technically enforce this requirement.
iii. Passwords must not be solely 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 must not be permitted to construct passwords that are identical or substantially similar to passwords that they had previously employed.
v. Passwords must be changed at least every 12 months.

c. Passwords must be hashed (with unique salts) and stored securely. Additionally, 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 prohibited. Authenticators used in multi-factor authentication mechanisms (such as PKI or biometrics) must be afforded the same secure storage protections.
d. In the event that remote access to MSK information resources is required, Vendor must ensure that it exclusively occurs using an MSK provisioned and managed solution.

2. Data Transmission Confidentiality and Integrity
   a. Vendor must ensure all MSK Sensitive Data transmitted by its employees, contractors, or agents is protected with a transmission encryption solution utilizing a cryptographic module which has been issued a Federal Information Processing Standards (FIPS) 140-2 validation certificate.
3. Media Protection, Sanitization and Destruction
   a. Vendor must ensure all MSK Sensitive Data stored by its employees, contractors, or agents is protected with a data-at-rest encryption solution utilizing a cryptographic module which has been issued a FIPS 140-2 validation certificate and a 128-bit key or higher.
      i. Vendor, its employees, subcontractors, or agents are prohibited from using removable media and/or mobile devices to store or transport any MSK Sensitive data unless explicitly authorized, in writing, by MSK.
   b. Vendor must, upon termination of the contract with MSK or at any time prior to repurposing, clear (using a DoD-compliant 7-pass wipe) or purge any media used to store or process MSK Sensitive Data in accordance with NIST SP 800-88.
      i. Any destroyed media must be able to withstand a laboratory attack as outlined in NIST SP 800-88.
      ii. Vendor must provide a certificate of destruction if requested by MSK.
4. System Security and Vulnerability Management
   a. Vendor must have documented procedures governing the identification, distribution, and application of security patches to all systems (including servers, workstations, and laptops) managed by Vendor, its employees, contractors, or agents that access, process, or store MSK

Sensitive Data. *Note that FDA-governed medical devices are not exempt from this requirement and must be patched.*

i. Vendor must ensure all applicable security patches are deployed within 30 days of publication unless explicitly authorized, in writing, by the MSK Information Security Office.

b. Vendor must ensure an anti-virus solution with real-time protection and automatic updates is employed on all systems managed by Vendor, its employees, contractors, or agents that access, store or process MSK Sensitive Data.

c. Vendor must ensure network security architectural components (including, at a minimum, firewalls and network intrusion detection/prevention solutions) are employed to adequately protect all systems managed by Vendor, its employees, contractors, or agents that process or store MSK Sensitive Data that are accessible from the Internet or other public network.

d. Vendor must ensure web-based solutions managed by Vendor, its employees, contractors, or agents that process or store MSK Sensitive Data adhere to security design best-practices including, but not limited to, addressing the Open Web Application Security Project (OWASP) Top 10 list of security risks.

5. Auditing
   a. Vendor must ensure all systems managed by Vendor, its employees, contractors, or agents that process or store MSK Sensitive Data maintain an automated audit log that documents at a minimum:
      i. All system security events; and
      ii. Any access, modification, and/or deletion of MSK Sensitive Data.
   b. Audit logs 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.
   d. Vendor must make available, at MSK's request, any audit logs documenting the access, modification, and/or deletion of MSK Sensitive Data.
   e. Vendor/BA must employ a regular audit log review process (either manual or automated) for detection of unauthorized access to MSK Sensitive Data.
6. Physical Security
   a. Vendor must ensure physical safeguards and visitor access controls are employed to prevent unauthorized access to all systems and media managed by Vendor, its employees, contractors, or agents that process or store MSK Sensitive Data.
7. Awareness and Training
   a. Vendor must ensure its employees, contractors, or agents receive regular security awareness training and are trained on security requirements applicable to their duties, including any outlined within this policy.

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

Effective Date:	01/01/2013
Revision Dates:	03/18/2016
	05/16/2018
	07/15/2019
Details of these revisions are tracked in the Information Security Policy Change Control document, available on OneMSK.	