IT Information Security Requirements

Vendor recognizes that due to the nature of Iron Mountain's data management business, Iron Mountain requires a high level of security to be maintained for the protection of information. This Exhibit sets forth the security measures that Vendor must maintain during the term of the underlying agreement between Iron Mountain and Vendor ("Agreement") for all data and information in any form ("Iron Mountain Information") that Vendor or Vendor’s Consultants (as defined herein) access, store, transmit, process or make subject to any operation or service performed ("Handled") by Vendor as part of the services provided under the Agreement. The terms and conditions contained herein are expressly incorporated into the Agreement.

1. GENERAL INFORMATION SECURITY REQUIREMENTS

a) Information Security Requirements. Vendor shall maintain a formal, comprehensive information security program for the management of information security. The information security program shall include, but not be limited to:

1) Documentation, internal publication, and communication of Vendor information security policies, standards, and procedures;
2) Documented and clear assignment of responsibility and authority for establishment and maintenance of the information security program;
3) Documented permissions and authorizations included in this Exhibit;
4) Regular testing of the key controls, systems and procedures of the information security program;
5) Administrative, technical and operational measures required in this Exhibit which are designed to protect all Iron Mountain Information, to the extent they are applicable to the format in which the Iron Mountain Information is Handled.

b) Minimum controls. In no event during the term of the Agreement shall Vendor's security program use controls materially less protective than those provided in this Exhibit.

c) Additional controls. Vendor agrees that it will adhere to any additional Iron Mountain data security requirements that may be reasonably provided by Iron Mountain to Vendor.

d) Vendor Consultants. Vendor shall be liable for the compliance of its employees, third-party agents, service providers, temporary workers, contractors, subcontractors, representatives and assigns ("Vendor Consultants") that have access to Iron Mountain Information with the terms of this Exhibit. Further, Vendor shall impose on any Vendor Consultants that have access to Iron Mountain Information privacy and security obligations substantially similar to those in this Exhibit prior to any such access taking place.

2. RISK ASSESSMENT REQUIREMENTS

a) Risk Assessment Program. Vendor shall maintain an information security risk assessment program designed to identify and assess reasonably foreseeable internal and external risks and vulnerabilities to the security, confidentiality, and/or integrity of Iron Mountain Information. Vendor shall further maintain an information security risk assessment program designed to identify any violation of law by Vendor or Vendor Consultants. No less frequent than once every twelve (12) months, and upon a material change in risk or vulnerability to Iron Mountain Information, Vendor shall evaluate and improve, as reasonable and appropriate, the effectiveness of Vendor’s information security program for limiting any security risks.

3. INFORMATION PROCESSING ASSETS AND PHYSICAL MEDIA MANAGEMENT REQUIREMENTS

a) Program requirements. Vendor shall maintain a program to manage information processing assets (such as computers, servers, storage devices, communications networks, personal computers, laptops and peripheral devices) that includes, but is not limited to, the following:

1) Assignment of asset ownership to ensure appropriate classification of information access, determination of access restrictions, and review of access controls;

2) Maintain an inventory of assets to facilitate asset lifecycle management and the identification of unauthorized assets accessing Vendor systems, infrastructure or resources;

3) Sanitization of assets prior to their disposal; and

4) Require management authorization prior to removal of equipment or software from Vendor premises that is not assigned to a specific individual.

b) Controls. Vendor shall maintain controls that include, but are not limited to, the following:

1) Operating procedures and technical controls designed to protect documents, computer media, input/output/backup data, and system documentation from unauthorized disclosure, modification and destruction.

2) Procedures for the secure disposal of electronic or physical media containing Iron Mountain Information.

3) An established process to track and maintain a chain of custody for all of Iron Mountain’s electronic or physical media from initial Vendor custody through to permanent removal or destruction.

4. WORKFORCE SECURITY MEASURE REQUIREMENTS

a) Confidentiality. Notwithstanding anything to the contrary, and in addition to any confidentiality terms in the Agreement, Vendor shall (i) treat all Iron Mountain Information as confidential information and (2) strictly adhere to Vendor’s internal information security and acceptable use requirements. Vendor shall enter into confidentiality agreements with all Vendor Consultants with access to Iron Mountain Information which include confidentiality terms and conditions that are substantially similar to the terms of the Agreement and this Exhibit.

b) Employees. To the extent permitted by applicable law and as required under the Agreement, Vendor shall conduct background investigations for all applicable employees and Vendor Consultants. Please reference the applicable language within the agreement for further details.

c) Security Awareness Training. No less than once per twelve (12) months, Vendor shall conduct general security awareness training and role-specific security training for all Vendor employees Handling Iron Mountain Information. Vendor shall maintain records identifying the names of such
Vendor employees in attendance and the date of each security awareness training. Vendor shall also routinely review and update its security awareness training program.

d) Violations. Vendor shall maintain a disciplinary process for all Vendor employees who violate the security requirements contained herein. Vendor employees who commit intentional violations of the terms of this Exhibit shall be immediately prohibited from providing services under the Agreement, and such employee’s access to Iron Mountain Information shall be revoked within no more than twenty-four (24) hours from being removed from performing services.

5. PHYSICAL AND ENVIRONMENTAL SECURITY REQUIREMENTS

a) Physical Security Controls. Vendor’s facilities shall utilize physical controls that reasonably restrict access to Iron Mountain Information, including, as Vendor deems appropriate, access control protocols, physical barriers such as locked facilities and areas, employee access badges, visitor logs, visitor access badges, card readers, video surveillance cameras, and intrusion detection alarms. All visitors to Vendor’s facilities must sign in and be escorted at all times. Video surveillance recordings and other records of physical access shall be retained for a minimum of ninety (90) days.

b) Supporting Utilities. Vendor shall employ measures designed to protect its facilities and systems containing Iron Mountain Information from power, telecommunications, water supply, sewage, heating, ventilation and air-conditioning failures.

c) Transmission System Security. At no time shall Vendor employ less than Industry Standard Safeguards designed to protect the physical security of its network infrastructure and telecommunication systems from transmission interception and damage.

d) Offsite Equipment. In the event that Vendor outsources functions for Handling Iron Mountain Information that use of offsite equipment, Vendor shall require that the security measures for any such offsite equipment be substantially similar to measures required for on-site equipment used for the same purpose.

e) Physical Access to Information Processing Assets. Vendor shall retain records of Vendor employees and Vendor Consultants authorized to access Vendor-controlled computer environment(s) used by Iron Mountain for no less than three (3) years. Upon Iron Mountain’s request, Vendor shall permit Iron Mountain to view all such records. Notwithstanding the foregoing, Iron Mountain shall not be given access to the confidential information of other Vendor customers or information which Vendor is restricted from providing under applicable law.

f) Physical Access Restricted. Vendor shall limit physical access to Vendor-controlled facilities that Handle Iron Mountain Information to those Vendor employees and Vendor Consultants who have a business need for such access. Vendor shall maintain a process for authorizing and tracking requests for physical access to such facilities.

g) Repairs and Modifications. Vendor shall record all security-related repairs and modifications to any physical components, including but not limited to hardware, walls, doors and locks for secure areas within facilities where Iron Mountain Information is Handled.

h) Hardware and Software Records. Vendor shall maintain a record of the movement and storage of hardware and electronic media that Handle Iron Mountain Information and the identity of any person responsible therefore.

6. COMMUNICATIONS AND INFORMATION PROCESSING OPERATIONS MANAGEMENT REQUIREMENTS
a) **Device Configuration Standards.** Vendor shall include Industry Standard Safeguards for security hardening procedures and standardized configurations for all devices such as servers, routers, switches and other network equipment used in Handling Iron Mountain Information, or with network connectivity to those devices. Vendor shall regularly monitor devices for compliance with standardized configurations and take prompt remedial action to correct deviations from these standards when appropriate.

b) **Information Processing Systems Change Control.** Vendor shall maintain a formal change management request process for all communications network systems and any Handling of Iron Mountain Information. Vendor shall ensure that all change requests are documented, tested, and approved by the asset owner, information owner, or management level personnel as appropriate prior to any new implementations for network communications capabilities, system patches, changes to existing systems or Handling of information. Emergency changes required to maintain or restore service shall subsequently be reviewed, documented and appropriate approvals obtained for the change.

c) **Segregation of Duties.** Vendor shall segregate duties and areas of responsibility so that no one person has sole access to information processing systems that Handle Iron Mountain Information. Vendor shall segregate the duties to limit the access of Vendor employees or Vendor Consultants to Iron Mountain Information only to the extent necessary to perform their required job functions. Vendor shall prohibit personnel whose primary responsibility is software development shall from accessing production systems, resources, or environments, except when such access is specifically approved for a defined and documented period of time. Vendor shall terminate or specifically re-approve such access when the defined period of time has elapsed.

d) **Separation of Development and Production Facilities.** Vendor shall logically or physically separate all development, test and production environments for information processing systems.

e) **Technical Architecture Management.** Vendor shall establish a configuration management process to define, manage, and control the information processing system components utilized to provide the Services and the technical infrastructure of such components.

f) **Intrusion Detection.** Vendor shall continually monitor computer systems and processes for attempted or actual security intrusions or violations. Vendor shall notify Iron Mountain within twenty-four (24) hours of any unauthorized access to Iron Mountain Information.

g) **Network Security.** Vendor shall ensure no less than the following measures are in place:

1) Maintain logs with daily reports for network intrusion detection system ("IDS")/intrusion prevention sensors ("IPS") alert event for all Vendor-hosted environment(s) used to Handle Iron Mountain Information;

2) Install updates for all Vendor-hosted environment(s) used to Handle Iron Mountain Information and IDS/IPS systems no less frequently than once per week, or as soon as possible after the updates are received, including prompt deployment to production of the latest threat signatures or rules;

3) High-risk ports on externally-facing systems shall not be accessible from the internet;

4) Maintain log files of all Vendor’s network connections for no less than twelve (12) months;

5) Deploy firewall(s) designed to protect internal systems, inspect all inbound and outbound network traffic, limit such traffic to define protocols and ports, and specify source and destination hosts where possible;

6) Maintain hardening policies for defining inbound and outbound network ports or service traffic for all Vendor-owned or managed systems and document such policies and any associated authorizations within the information security program;

7) Properly secure network and diagnostic ports; and
8) Implement policies, procedures and technical controls that are designed to prevent, detect and remove malicious code or known attacks on Vendor’s information systems.

h) **Encrypted Authentication Credentials.** Vendor shall ensure that authentication credentials transmitted over Vendor’s network devices are encrypted in transit.

i) **Secure Network Administration.** Vendor shall reasonably manage and control Vendor’s networks to protect such networks from known threats, and to maintain security for all Vendor managed applications and data on or in transit over the network. Vendor shall implement technical controls and secure communication protocols consistent with Industry Standard Safeguards to prohibit unrestricted connections to untrusted networks or publicly accessible servers.

j) **Virus Protection.** Vendor shall maintain an anti-virus management program, including malware protection, up-to-date signature files, patches, and virus definitions, for Vendor managed servers and workstations used to Handle Iron Mountain Information.

k) **Website – Client Encryption.** Vendor shall ensure that for each of its websites Transport Layer Security (TLS) is enabled and contains a valid certificate requiring confidentiality, authentication or authorization controls.

l) **Email Relaying.** Vendor shall ensure that unauthenticated email relaying/forwarding in the Iron Mountain-dedicated hosted environment(s) is disabled on Vendor’s Internet email servers.

m) **Information Backup.** Vendor shall create and securely store appropriate back-up copies of system files.

n) **Electronic Information in Transit.** Vendor shall utilize encryption using an industry standard algorithm with a minimum 128 bit key length to protect Iron Mountain Information transmitted over public networks when originating from Vendor hosted infrastructure.

o) **Cryptographic Controls.** Vendor shall follow a documented policy on the use of cryptographic controls. Vendor’s cryptographic controls shall:
   1) Be designed to reasonably protect the confidentiality and integrity of Iron Mountain Information being Handled by Vendor in any shared network environments in accordance with the terms of this Exhibit;
   2) Be applied to Vendor-hosted environment(s) used to transmit Iron Mountain Information across or to “untrusted” networks (i.e., networks that Vendor does not legally control), including those environments or networks used for sending data to Iron Mountain’s corporate network from Vendor’s network, subject to Iron Mountain’s cooperation in management of encryption keys necessary to decrypt transmissions received by Iron Mountain; and
   3) Include documented encryption key management practices to support the security of cryptographic technologies.
   4) Include encryption of all Iron Mountain Information on laptops and other portable devices.

p) **Logging Requirements.** Vendor shall ensure the following:
   1) Significant security and system events are logged and reviewed;
   2) At minimum, log all successful and failed login events related to the Cloud Services accounts assigned to Customer Authorized Users and Affiliates logs shall minimally include the attributes: Date, Time, True Source IP Address, UserID, Action Detail (e.g., Successful/Failed Login) and web session history (click stream);
   3) Monitor all login sessions for potential security breaches;
   4) Audit logs for systems in Vendor-hosted environments used to provide services are retained for a minimum of twelve (12) months;
   5) Vendor shall make available to Customer session logging data related to Cloud Service accounts assigned to Customer Authorized Users and/or Affiliates on demand;
   6) Vendor shall also facilitate the secure electronic transport of session logging data related to Cloud Service accounts assigned to Iron Mountain personnel and affiliates of Iron Mountain
for integration into Iron Mountain’s Security Incident and Event Management tool (SIEM) in near real time (e.g., API or SFTP);
7) System audit logs are reviewed for anomalies; and
8) Log facilities and systems information are reasonably protected against tampering and unauthorized access.
q) **Network Time Synchronization.** Vendor shall synchronize the system clocks of all information processing systems using a common authoritative time source.
r) **Segregation on Networks.** Vendor shall appropriately segregate related groups of information services, users, and information systems on networks. Internet facing systems and server systems Handling Iron Mountain data shall reside on a dedicated DMZ network segment segregated from corporate and user segments.

### 7. ACCESS CONTROL REQUIREMENTS

a) **Access Control Policy.** Vendor shall maintain an access control policy for all assets that Handle Iron Mountain Information. Vendor shall formally approve, publish and implement such access control policy.
b) **Logical Access Authorization.** Vendor shall maintain an approval process for requests for logical access to Iron Mountain Information and requests for access to Vendor systems used by Vendor in providing services to Iron Mountain.
   1) Vendor shall maintain a user registration and deregistration procedure for granting and revoking access to Vendor systems that Handle Iron Mountain Information.
   2) Vendor shall retain a record of access to Vendor’s information processing systems and Privileged Accounts (as defined below) in Vendor-hosted environment(s) for no less than twelve (12) months. Upon Iron Mountain’s request, Vendor shall provide such access records and reasonably cooperate with Iron Mountain for all inquiries relating to such access records.
c) **Privileged Access Control.** A “Privileged Account” is an account that enables an individual to establish or modify identification credentials, access rules, production applications or operating systems or network parameters. Vendor shall ensure that Privileged Accounts are only provided by Vendor to individual users that are expressly approved by Vendor or Iron Mountain, and Vendor shall ensure that such Privileged Accounts are strictly limited to those individuals who have a legitimate business need to use a Privileged Account. Vendor shall maintain a process for obtaining approvals for Privileged Account users. Additionally, Vendor shall maintain an audit trail of all approved individuals and actions performed by these Privileged Accounts.
d) **Access Control and Access Review.** Vendor shall grant access to Iron Mountain Information to current Vendor employees or Vendor Consultants who need such access in order to perform their job function only. Every three (3) months, or on a quarterly basis, Vendor shall review and confirm that all access to Iron Mountain Information or Privileged Accounts is only granted by Vendor to individuals who require such access in the performance of their current job function. Vendor shall further maintain record of such access reviews and updates.
e) **Control of Third Party Access.** Prior to granting third parties access to Vendor’s information systems that Handle Iron Mountain Information, Vendor shall ensure that appropriate controls are in place including, but not limited to: restrictions on protocols and ports used to access information, encryption to protect sessions and information in transit, appropriate background checks for third party personnel as required herein, anti-virus software running current signatures on devices used to access Iron Mountain Information, and current patches on devices used to access Iron Mountain Information.
f) Operating Systems Access Control. Vendor shall control access to operating systems (both software and hardware based operating systems) by requiring a secure log-on process that uniquely identifies the individual who is accessing the operating system.

g) Mobile Computing Devices. Vendor shall maintain a program designed to protect Vendor’s mobile computing devices from unauthorized access. Such program shall address physical protection, access control and security controls such as encryption, virus protection and device backup.

h) Iron Mountain Systems Isolation. Vendor shall logically separate and segregate Iron Mountain Information from all other information in hosted environments used to Handle Iron Mountain Information.

i) Accounts. Vendor shall require the following with respect to accounts:
   1) Authentication of the identity of each Vendor employee or Vendor Consultant who attempts to access Vendor systems that Handle Iron Mountain Information and prohibit the use of shared user accounts, or user accounts with generic credentials (i.e. IDs) for accessing such Iron Mountain Information or the associated systems.
   2) That all user account IDs, including Privileged Accounts, be tied directly to an individual person (as opposed to a position) with the sole exception of service accounts required to run server software. Vendor shall ensure that (i) all service accounts are subject to at least the same password restrictions as Privileged Accounts, (ii) use of such services accounts is restricted to the specific servers required for the account and (iii) interactive logins are prohibited for any unusual activity and wherever possible.
   3) The use of temporary passwords that meet or exceed the complexity requirements for individual accounts, check out IDs, or similar controls for default administration account access if default administration accounts are not disabled or removed.
   4) That inactive accounts are locked or disabled after ninety (90) days of inactivity.
   5) Access to an account is prohibited after no more than five (5) unsuccessful access attempts.
   6) Unique identifiers and strong passwords with a required minimum number of characters that must be changed every ninety (90) days.
   7) Employees are prohibited from sharing or writing down passwords.

j) Controls for Unattended Systems. Vendor shall utilize a password protected screensaver for any system that is inactive for thirty (30) minutes or longer.

8. INFORMATION SYSTEMS ACQUISITION DEVELOPMENT AND MAINTENANCE REQUIREMENTS

a) Systems Development Security. Vendor shall ensure that security measures are included in all information systems development and operations. Further, Vendor shall publish and adhere to internal secure coding methodologies based on application development security standards.
   1) Vendor shall include in the development process application functionality designed to prevent errors, losses, unauthorized modifications or misuse of information.
   2) Vendor shall control access to system files and program source code. Vendor shall assign, document and conduct in a reasonably secure manner all information technology development, implementation and support project activities.
   3) Vendor shall formally approve application changes and such changes will be controlled by a documented change control process.

b) Software Security Management. Vendor shall design its information systems (including operating systems, infrastructure, business applications, services and user-developed applications) to be in compliance with Industry Standard Safeguards.
   1) Vendor shall maintain the security of production application system software and information.
2) Vendor shall appropriately supervise and monitor all outsourced software development activities.

3) Vendor shall maintain policies and technical controls designed to prevent non-administrative users from installing software on operations systems.

c) **Network Diagrams.** Vendor shall develop, document, and maintain physical and logical diagrams of networking devices and traffic.

d) **Application Vulnerability Assessments/Ethical Hacking.** No less frequently than once every twelve (12) months, Vendor shall, perform vulnerability assessments on applications in its hosted environment(s) used to Handle Iron Mountain Information.

1) If Vendor does not permit Iron Mountain or agents of Iron Mountain to test or assess Vendor infrastructure or applications in any capacity, upon Iron Mountain’s request Vendor shall provide attestation to the security of its applications and infrastructure through independent certifications, third party application security testing, and internal security assurance processes. Additionally, Vendor shall make available to Iron Mountain all executive summaries of the results of independent security tests. Vendor shall not be required to provide detailed results that are the confidential and proprietary information of Vendor.

e) **Change Testing and Review.** Vendor shall review and test changes to applications and operating systems prior to deployment to ensure there is no adverse effect on Iron Mountain Information or systems and to negative impact to functionality required by Iron Mountain to consume the scoped services.

9. **SECURITY BREACHES AND INCIDENT RESPONSE REQUIREMENTS**

a) **Notification.** Vendor shall notify Iron Mountain promptly upon learning of a Security Incident. For purposes of this Addendum, a “Security Incident” shall mean (a) the actual unauthorized access to or use of Iron Mountain Information, or (b) the unauthorized disclosure, loss, theft or manipulation of unencrypted Iron Mountain Information (or encrypted Iron Mountain Information where unauthorized decryption has or is likely to occur) or other information under control of Vendor that has the potential to cause harm to Iron Mountain’s business, clients, employees, systems, or reputation.

Notification must include a phone call to the primary Iron Mountain account contact. In the event Vendor is unable to reach such contact promptly, Vendor must contact globalsecurity@ironmountain.com and legal.department@ironmountain.com. Notification shall include at a minimum (a) a detailed description of the Incident, (b) the expected resolution time (if it has not already been resolved), and (c) the name and phone number of the Vendor representative that Iron Mountain may contact to obtain further information and updates.

b) **Updates.** Vendor agrees to keep Iron Mountain informed of progress and actions taken to address the Security Incident, and to provide Iron Mountain with all facts about the Security Incident as appropriate for Iron Mountain to conduct its own assessment of the risk to Iron Mountain Information and of Iron Mountain’s overall exposure to such Security Incident.

c) **Disclosure.** Unless such disclosure is mandated by law, Iron Mountain in its sole discretion will determine whether to provide notification to Iron Mountain’s customers or employees concerning incidents involving Iron Mountain Information.
d) **Remediation.** Notwithstanding any other provisions of the Agreement or a Statement of Work, in the event of a Security Incident involving unencrypted Personal Data, Vendor agrees to provide at Vendor’s expense one year of credit monitoring and identity restoration services reasonably acceptable to Iron Mountain to affected individuals and all other service(s) required by applicable law or even if not so required which are customarily provided to individuals impacted by a breach in confidentiality of their Personal Data in their jurisdiction. For purposes of this Exhibit, Personal Data shall mean any data related to or associated with an identified or identifiable natural person, including, but not limited to, any Iron Mountain employee information, or Iron Mountain customer information. Personal Data shall also include Protected Health Information or “PHI” which shall have the same meaning as the term ‘protected health information’ in 45 CFR §160.103 and shall include any PHI of Iron Mountain and/or its customers. A natural person is identifiable if, with reasonable effort, the individual could be identified from the data or a grouping of data.