Description of Iron Mountain Information Technology (IT) Infrastructure Environment and Application Hosting Services System relevant to Security, Confidentiality and Availability for the period January 1, 2019 through September 30, 2019
Table of Contents

Report of Independent Accountants .................................................................1
Assertion of Management..................................................................................3
System Description..........................................................................................4
User Responsibilities.........................................................................................10
Report of Independent Accountants

To the Management of Iron Mountain Information Management, LLC:

Scope
We have examined management’s assertion, contained within the accompanying Management’s Assertion Regarding the Effectiveness of Its Controls over the Information Technology (IT) Infrastructure Environment and Application Hosting Services System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality (Assertion), that Iron Mountain’s controls over the IT Infrastructure Environment and Application Hosting Services System (System) were effective throughout the period January 1, 2019 to September 30, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Management’s Responsibilities
Iron Mountain’s management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the IT Infrastructure Environment and Application Hosting Services System (System) and describing the boundaries of the System
- Identifying our principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the IT Infrastructure Environment and Application Hosting Services System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement.

Our Responsibilities
Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion, which includes: (1) obtaining an understanding of Iron Mountain’s relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.
Our examination was not conducted for the purpose of evaluating Iron Mountain’s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations:
Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Iron Mountain’s principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion:
In our opinion, Iron Mountain’s management assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

November 15, 2019
Boston, Massachusetts
Management’s Assertion Regarding the Effectiveness of Its Controls over the Information Technology (IT) Infrastructure Environment and Application Hosting Services System Based on the Trust Services Principles and Criteria for Security, Availability and Confidentiality

November 15, 2019

We, as management of, Iron Mountain Information Management, LLC are responsible for:

- Identifying the Information Technology (IT) Infrastructure Environment and Application Hosting Services System (System) and describing the boundaries of the System, which are presented in the section below titled System Description of Iron Mountain’s IT Infrastructure Environment and Application Hosting Services System
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in the section below titled System Description of Iron Mountain’s IT Infrastructure Environment and Application Hosting Services System
- Identifying, designing, implementing, operating, and monitoring effective controls over the IT Infrastructure Environment and Application Hosting Services System (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period January 1, 2019 to September 30, 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, and confidentiality set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

The Management of Iron Mountain Information Management, LLC
System Description of Iron Mountain’s IT Infrastructure Environment and Application Hosting Services System

Business and Organization

Iron Mountain is a trusted global outsourcing partner for both records management and data management services. The Company’s comprehensive services help businesses save money and manage risks associated with legal and regulatory compliance, protection of vital information, and business continuity.

Four of Iron Mountain’s primary business operation relevant to the system description include: Records Management, Data Management, Secure Destruction and Digital Solutions.

Records Management

Iron Mountain’s Record Management Service provides clients the ability to choose from a variety of document management solutions, which include:

- Records Management program development and implementation
- Policy-based records management programs, which feature secure, cost-effective storage, flexible retrieval access and retention management
- Customized services for vital records, film & sound and regulated industries
- Digital record center content management

Data Management

Iron Mountain’s Data Management Service offers clients the ability to securely vault backup tapes at offsite facilities. Iron Mountain works with their clients to develop a solution that allows for fast and efficient data recovery.

Iron Mountain manages two primary tape vaulting programs for customers. These programs are Open Media and Closed Containers.

- Open Media: Storage of customer media at the tape level and tracked via the designated volume serial (VolSer) label of the tape. Storage is allocated by a unique customer number and segregated in racking assigned to the customer. Media delivery and pickup is accomplished through the assignment of “transport” containers individually assigned to the customer with their unique customer number.
- Closed Container: Storage of customer media in containers. The customer is assigned a unique customer number and storage containers which are not opened by Iron Mountain Staff.

Secure Destruction

The Iron Mountain Secure Destruction Services develops, implements, and manages secure, sustainable destruction solutions that help and enable customers to manage the risks associated with the disposal of information. The Iron Mountain Secure Destruction Service is a nationally recognized service provider targeting customers of all sizes and in nearly all industries. The Service is a natural fit with Iron Mountain’s Records Management core service offering, customer base and supporting operations. Iron Mountain offers off site destruction through a plant hub and spoke network as well as onsite destruction using mobile shred fleet.
Iron Mountain’s Secure Destruction Service is predicated on the security of customer’s material. Iron Mountain has invested millions of dollars in safeguards throughout the chain of custody to help ensure best in class technology and well defined, auditable handling procedures to keep customer’s material secure from the time of pick up to the actual destruction.

**Digital Solutions / Technology Escrow Services**

As data continues to move in a digital format, Iron Mountain has designed solutions to assist companies with maintaining the availability and security of their digital records using their Digital Solution Services. The solution includes:

- Digital Record Center (DRC)
- Document Imaging Services

Iron Mountain’s Digital Solutions services provides the resources necessary to convert hardcopy documents already stored in Iron Mountain facilities or received from customers via mail or courier to an electronic format and make them readily available to users across a customer’s organization, share documents electronically across the organization, enhance business processes, and safeguard their information from loss or destruction.
Executive Summary

This description covers Iron Mountain’s IT Infrastructure and Application Hosting Services System (herein referred to as the ‘System’) that supports the aforementioned services provided by Iron Mountain. The scope of this description includes the technology infrastructure hardware and software components supporting the application operating system, databases and network devices by Iron Mountain’s Global Information Services and Application Development groups. The systems are physically located in the Iron Mountain data center locations in Boyers, Pennsylvania, Milton Keynes, United Kingdom, along with co-locations managed by Cyxtera in Toronto, Ontario, Canada and/or Montreal, Quebec, Canada (collectively referred to as the ‘in-scope production data centers’). Iron Mountain utilizes their data center in Kansas City, Missouri to host the disaster recovery systems supporting the IT Infrastructure Environment and Application Hosting Services System.

The System is comprised of the following components:
- Infrastructure (facilities, equipment and networks)
- Software (systems and utilities)
- People (developers, operators, users and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, databases and tables).

The following sections of this description define each of these five components comprising the System.

Infrastructure

The system includes five data centers, located in Pennsylvania, United States; Missouri, United States; Quebec, Canada, Ontario, Canada and Milton Keynes, United Kingdom. Housed within these data centers are the supporting operating system platforms (UNIX/Linux, and Windows based), networking components (routers, switches, firewalls), and data storage devices. The data centers are inter-connected to several designated Iron Mountain office locations by an IP based network architecture.

This system description covers the IT infrastructure (e.g., network, operating system, and database components) supporting the following applications, which are managed by Iron Mountain’s Global Infrastructure Services group:
- Iron Mountain Connect Web Portal
- SafeKeeper Plus (SKP)
- SecureBase / SecureSync
- Digital Record Center (DRC)
- Kofax Central (Kofax)
- Intellectual Property Management (“IPM”) solution
- Cloud Storage for Medical Images
Software

The software utilized to manage and support the in-scope System consists of various business line applications and supporting infrastructure and tools that are used to support the monitoring, job scheduling and processing, change management, and help desk support. Iron Mountain uses a three-tiered network architecture as its standard: Web Tier, Application Tier, and Database Tier. All tiers are separated by firewalls and protected by Intrusion Detection scanners, which are strategically placed over critical network points and are monitored by the Iron Mountain IT Department.

People

In order to support and maintain the security, availability and confidentiality of the in-scope System, the following core support services are fully involved:

- Global Infrastructure Services Group
- Global Technology Office Group
- Global Service Delivery Group
- Software Engineering Support Group
- Information Security Group

Below is a brief description of each of these functional areas:

- The Global Infrastructure Services group is responsible for the following functional areas:
  - The Global Systems group is responsible for server operating system and middleware configuration, integration and operations. Additionally, this group is responsible for some system access administration functions.
  - The Global Operations Center is responsible for system and network monitoring as well as job scheduling.
  - The Global Networks group is responsible for global network management including global network communication device (router/switch) and network security device (firewall, IDS) configuration, integration, and operations.
  - The Global Storage group is responsible for the global storage configuration, integration and operations, along with the backup/recovery, disaster recovery planning and testing.
  - The Global Databases group is responsible for the global database configuration, integration and operations.
  - The Enterprise Change Management committee is responsible for managing the Change Advisory Board (CAB).

- The Global Technology Office group is responsible for developing strategic plans to align business and IT objectives as well as communicate current IT concerns and environmental changes to the respective business lines. This plan is communicated and presented on a quarterly basis during the GTO all hands meeting.

- The Global Service Delivery group is responsible for Access Administration, Access Control, Desktop Support, End User Support, and Application Support (Level 1). Additionally, CTO reporting’s are a shared responsibility between the Global Services Delivery group and the Global Infrastructure Services group

- The Software Engineering Support group is responsible for Service Level Agreement Management Solution Developments as well as manages and plans for the overall enterprise architecture design and development.

- The IT Security group is responsible for securing the systems and network based on the guidelines and policies defined by Information Security group.
Iron Mountain has engaged HCL, a third-party vendor, for cross-functional IT services based on the ITIL model, including Service Strategy, Service Design, Service Transition, Service Operations and Continual Service Improvement. Iron Mountain maintains management oversight of the activities HCL is performing. On a weekly basis, operational leads from HCL and IRM meet to discuss the day-to-day operations and concerns, while leadership meetings occur on a monthly basis. HCL’s relationship with Iron Mountain is managed through Iron Mountain’s overall vendor management program, which includes vendor assessments.

**Procedures**

Iron Mountain has documented policies and procedures to support the operations and controls in support of their service. Relevant policies and procedures are made available to employees through the Iron Mountain Compliance & Security Services (COMPASS) and SharePoint intranet sites. Policies and procedures are reviewed and updated on a regular basis.

Specific examples of the relevant policies and procedures include the following:
- Requirements of authorized users regarding responsibility and accountability
- Account administration
- Data classification, retention and destruction
- Security incident report and response
- Training and education
- Change management and application development
- Physical and environmental protection
- Third party access and management
Data

Client data is retained in accordance with applicable data protection and other regulations set out in Client contracts and Iron Mountain policies. As defined within the Iron Mountain data classification policy, Client data is considered confidential and is retained and disposed of in accordance with Iron Mountain’s commitments and requirements as defined within the data classification policy and customer contract. Confidential client data includes the physical data stored in boxes and on tapes stored at Iron Mountain facilities, digital images, and electronic escrow data stored within the systems. This does not include the data (e.g. metadata) securely retained within the systems used solely for tracking the assets stored with Iron Mountain. Client confidential data, electronic or hard copy, is retained according to the commitments and requirements, as defined within the contracts and agreements. The standard retention of client confidential information is for Iron Mountain to retain data indefinitely. Client confidential data is retained, returned, or destroyed solely at the specific request of the client or based upon the agreement within the client termination agreement. These requests, along with client requests for changes to retention or disposal requirements, are documented and tracked within a ticket until closure. Access to client data is limited to authorized Iron Mountain personnel and is only granted in accordance with physical and logical Iron Mountain system security administration policies.

Service Commitments and System Requirements

Iron Mountain designs its processes and procedures relevant to the IT Information Technology (IT) Infrastructure Environment and Application Hosting Services System to meet objectives for its services. Iron Mountain’s objectives are based on the service commitments made to customers in applicable contracts, applicable laws and regulations, and the financial, operational and compliance requirements that Iron Mountain has established for its services. The principal service commitments and system requirements commitments include:

- Implementing logical and physical access restrictions to help ensure that logical and physical access to programs, data, and IT resources is restricted to appropriately authorized users and that access is restricted to performing appropriately authorized actions.
- Implementing technical and non-technical controls, along with safeguards, to help ensure the availability of data in accordance with the system documentation and requirements.
- Implementing technical and non-technical controls to retain and dispose of confidential data in accordance with agreed upon retention terms.

Iron Mountain establishes operational requirements that support the achievement of its security, availability and confidentiality commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Iron Mountain’s policies and procedures, system design documentations and contracts with third parties (customers and vendors).
User Responsibilities

Iron Mountain communicates the responsibilities of its user entities (e.g., Customers) through the contract acceptance and addendum process. The following highlight some of those responsibilities:

- Users of the IT Infrastructure and Application Hosting Services System are responsible for ensuring that access to the system limited to authorized and appropriate individuals. (Criteria CC6.2, CC6.3)
- Users of the IT Infrastructure and Application Hosting Service System are responsible for reviewing documentation provided by Iron Mountain related to changes made to the systems. (Criteria CC8.1)
- Users of the IT Infrastructure and Application Hosting Service System are responsible for reporting any security or confidentiality breaches and availability incidents, which impact the systems. (Criteria CC7.3)
- User entities are responsible for approving and validating the appropriateness (and maintaining the confidentiality) of data provided to Iron Mountain and any changes to that data. (Criteria CC1.5)
- User entities are responsible for adequately securing data contained in any output reports provided by Iron Mountain, including appropriateness of individuals accessing the output reports through the systems and storage/disposal of the output reports. (Criteria CC6.6)
- User entities are responsible for communicating security and confidentiality provisions to individuals accessing information within the systems and/or produced by the System. (Criteria CC1.1)
- User entities are responsible for communicating any identified security, availability and/or confidentiality violations impacting the in-scope system and/or data to Iron Mountain on a timely basis, as necessary. (Criteria CC7.3)
- User entities are responsible for communicating retention period of confidential information, when to dispose of confidential information, and to confirm requests of disposals are processed. (Criteria C1.1, C1.2)