SECURITY ASSESSMENT METHODOLOGY

Schellman submitted an information request list to the organization which requested evidence to demonstrate that controls are consistent with requirements to meet NIST 800-53 Rev. 5. Virtual onsite inspections and procedures of the data centers were performed from June 1, 2022, to October 31, 2022. Due to concerns resulting from the COVID-19 pandemic, all site inspections were conducted virtually.

A selection of NIST 800-53 Rev. 5 security controls were used as the basis for this assessment. The physical and environmental control family selection was agreed upon and requested by Flexential. The selected security controls determine whether an organization is compliant with FISMA High sensitivity physical and environmental controls.

As part of the assessment, Schellman performed testing procedures based on the in-scope data center locations to determine if Flexential implemented controls to meet the requirements as defined in Section 4. Testing procedures followed the guidance defined in the table below and included interviewing Flexential personnel, inspecting evidence such as Flexential policies, procedures, system security settings, and observing Flexential personnel and system components to ensure the Flexential controls were in place.

Method	Definition
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

PHYSICAL AND ENVIRONMENTAL PROTECTION

#	NIST Control	Status
PE-1	The organization: a. Develops documents and disseminates to internal users: 1. Organizational-level; Mission/business process-level; System-level physical and environmental protection policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; b. Designate: organization-defined official to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and c. Review and update the current physical and environmental protection: 1. Policy: organization-defined frequency and following: organization-defined events; and 2. Procedures: organization-defined frequency and following: organization-defined events.	In place.
PE-2	The organization: a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issues authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals: organization-defined frequency; and d. Remove individuals from the facility access list when access is no longer required.	In place.
PE-3	The organization: a. Enforce physical access authorizations at organization-defined entry/exit points to the facility where the system resides by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using: organization-defined physical access control systems or devices; guards; b. Maintain physical access audit logs for: organization-defined entry/exit points; c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: organization-defined physical access controls; d. Escort visitors and control visitor activity: organization-defined circumstances requiring visitor escorts and control of visitor activity; e. Secure keys, combinations, and other physical access devices; f. Inventory: organization-defined physical access devices every organization-defined frequency; and g. Change combinations and keys: organization-defined frequency and/or when keys are lost, combinations are compromised, or when individuals possessing the keys ore combinations are transferred or terminated.	In place.

#	NIST Control	Status
PE-3(1)	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at: organization-defined physical spaces containing one or more components of the system.	In place.
PE-4	Control physical access to: organization-defined system distribution and transmission lines within organizational facilities using: organization-defined security controls.	In place.
PE-5	Control physical access to output from: organization-defined output devices to prevent unauthorized individuals from obtaining the output.	In place.
PE-6	The organization: a. Monitor physical access to the facility where the system resides to detect to detect and respond to physical security incidents; b. Review physical access logs: organization-defined frequency and upon occurrence of: organization-defined events or potential indications of events; and c. Coordinate results of reviews and investigations with the organizational incident response capability.	In place.
PE-6(1)	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.	In place.
PE-6(4)	Monitor physical access to the system in addition to the physical access monitoring of the facility at: organization-defined physical spaces containing one or more components of the system.	In place.
PE-8	The organization: a. Maintain visitor access records to the facility where the system resides for: organization-defined time period; b. Review visitor access records: organization-defined frequency; and c. Report anomalies in visitor access records: organization-defined personnel.	In place.
PE-8(1)	Maintain and review visitor access records using: organization-defined automated mechanisms.	In place.
PE-9	Protect power equipment and power cabling for the system from damage and destruction.	In place.
PE-10	The organization: a. Provide the capability of shutting off power to: organization-defined system or individual system components in emergency situations; b. Place emergency shutoff switches or devices in: organization-defined location by system or system component to facilitate access for authorized personnel; and c. Protect emergency power shutoff capability from unauthorized activation.	In place.
PE-11	Provide an uninterruptible power supply to facilitate: an orderly shutdown of the system; transition of the system to long-term alternate power in the event of a primary power source loss.	In place.
PE-11(1)	Provide an alternate power supply for the system that is activated: manually; automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.	In place.
PE-12	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	In place.
PE-13	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.	In place.

#	NIST Control	Status
PE-13(1)	Employ fire detection systems that activate automatically and notify: organization-defined personnel or roles and: organization-defined emergency responders in the event of a fire.	In place.
PE-13(2)	The organization: a. Employ fire suppression systems that activate automatically and notify: organization-defined personnel or roles and: organization-defined emergency responders; and b. Employ and automatic fire suppression capability when the facility is not staffed on a continuous basis.	In place.
PE-14	The organization: a. Maintain: temperature; humidity; pressure; radiation; organization-defined environmental control levels within the facility where the system resides at; and b. Monitor environmental control levels: organization-defined frequency.	In place.
PE-15	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.	In place.
PE-15(1)	The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts: IT personnel.	In place.
PE-16	The organization: a. Authorize and control: organization-defined types of system components entering and exiting the facility; and b. Maintain records of the system components.	In place.
PE-17	The organization: a. Determine and document the: organization-defined alternate work sites allowed for use by employees; b. Employ the following controls at alternate work sites: organization-defined controls; c. Assesses the effectiveness of controls at alternate work sites; and d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.	In place.
PE-18	Position system components within the facility to minimize potential damage from: organization-defined physical and environmental hazards and to minimize the opportunity for unauthorized access.	In place.