Physical Security Policy

Purpose

The purpose of this policy is to establish the requirements and process for controlling access to <Company Name> facilities and requirements for data centers hosting <Company Name> system components.

Scope

This policy applies to the cloud providers used to host <Company Name>'s system components, to <Company Name>'s corporate facilities, to and to home and remote offices used by its employees.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

Most <Company Name> employees are either remote employees or work extensively from home. All employees are required to secure their physical laptops in the following manner:

- The confidentiality, security and privacy of company data must be preserved, by ensuring that no unauthorized individuals may view or gain access to customer data.
- While in public areas, employees are required to avoid viewing customer support emails and data, and to avoid discussing confidential information in person or through teleconference.
- End user devices containing access to internal company resources, such as laptops and cell phones, must be protected at all times and may not be left unattended. Reasonable precautions must be taken to protect company hardware, software, and information from theft and damage.
- Lost, damaged, or compromised hardware must be promptly reported.

The default, company-provided means for workforce members to connect to <Company Name> information systems leverage secure, encrypted protocols, such as SSL/TLS and SSH, as governed by <Company Name>'s Encryption Policy, and multi-factor authentication, governed by the Authentication and Password Policy. Employees must follow those established practices, and are barred from tampering or subverting them.

<Company Name> provides workstations, such as laptops, for remote use. Alternatively, employees may use their own devices. In both cases, these assets and their use are subject to all <Company Name> requirements surrounding security hardening, such as hard-disk encryption, operating system security patches, and anti-malware. Failure to adhere to those requirements is subject to the company's disciplinary process.

Clear Desk Policy

Workforce members and contractors must take measures to avoid inadvertently exposing confidential data by allowing it to be viewed by unauthorized individuals. Displays for all workstations used to access confidential data must not be viewable from outside the immediate work area. Unauthorized viewing from windows, hallways, or by employees without access rights to the same information should be avoided.

Information not in active use that is classified as confidential must not be displayed or left out in a work area. When information is not in active use, any applications displaying it on a computer should be closed. When leaving a workstation unattended, employees must ensure that its screen is locked, and that automatic screen lock settings are not relaxed. If usage of printed or removable media is allowed by company policy, confidential media must be secured in a locked cabinet once it is not in use, and whenever employees are away from their immediate desk area.

Datacenters

The company uses established Infrastructure-as-a-Service cloud providers to procure the necessary infrastructure required to meet the business objectives. The cloud vendor(s) provide and manage best-in-class Data Centers, including Asset Management, Redundant Power and Networks, and Physical Security. The company has security controls to govern its obligations as part of the shared responsibility model required by the cloud provider.

The capabilities of <Company Name>'s cloud infrastructure provider are summarized below.

Secure Design

- Site Selection - the site is carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity.
- Redundancy - data centers are designed to anticipate and tolerate failure while maintaining service levels.
- Availability - each Availability Zone is engineered to operate independently with high reliability, and zones are connected to enable easy fail-over without interruptions.
- Capacity Planning - a capacity planning model assesses infrastructure usage and demands, and supports future demand planning.

Business Continuity and Disaster Recovery

- Business Continuity Plan - a plan outlines measures to avoid and lessen environmental disruptions, including steps to be taken before, during, and after an event.
- Pandemic Response - pandemic response policies and procedures are incorporated into disaster recovery planning.

Physical Access

- Employee Data Center Access - employees who require data center access must first provide a valid business justification. Requests are reviewed and approved by authorized personnel, and access is promptly revoked once access is no longer required.
- Third-party Data Center Access - access requests are granted based on the principle of least privilege, are time-bound, and are approved by authorized personnel.

Monitoring and Logging

- Data Center Access Review - access to data centers is regularly reviewed and is automatically revoked when an employee's record is terminated.
- Data Center Access Logs - physical access to data centers is logged, monitored, retained, and correlated with physical monitoring systems.
- Data Center Access Monitoring - data centers are monitored 24/7 by local teams ready to respond to security incidents by triaging, analyzing, and dispatching responses.

Surveillance and Detection

- CCTV - physical access points to server rooms are recorded by Closed Circuit Television (CCTV) cameras. Images are retained according to legal and compliance requirements.
- Data Center Entry Points - physical access is controlled at building ingress points and requires multi-factor authentication.
- Intrusion Detection - Intrusion detection systems are installed to monitor, detect, and automatically alert appropriate personnel of security incidents.

Device Management

- Asset Management - assets are centrally managed through an inventory management system that tracks owner, location, status, maintenance, and descriptive information.
- Media Destruction - media storage devices used to store customer data are decommissioned using techniques detailed in NIST 800-88.

Operational Support Systems

- Power - electrical power systems are designed to be fully redundant and maintainable without impact to operations.

- Climate and Temperature - data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware.
- Fire Detection and Suppression - data centers are equipped with automatic fire detection and suppression equipment.
- Leakage Detection - data centers are equipped with functionality to detect the presence of water, and mechanisms are in place to remove water.

Infrastructure Maintenance

- Equipment Maintenance - equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.
- Environment Management - electrical and mechanical systems are employed to enable automatic identification of issues, and preventative maintenance is performed.

Governance and Risk

- Ongoing Data Center Risk Management - ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities.
- Third-party Security Attestation - data centers are tested by third parties to ensure appropriately implemented security measures.