FlexProtection

Physical Security Policy for:

National Training Systems, Inc.

Jan 1, 2020

Table of Contents

Purpose

This policy document, like other security policies, is intended to be a framework for various rules and practices that will help secure the company's assets, its technology, its data, and the privacy of its customers.

This particular policy focuses on physical security, leaving data and system-oriented policy matters to other security policy documents. It is as simple as it can be, in accordance with the need to also be effective and reliable.

Usage

Compliance

This policy is meant to be easily understood and easily followed. It is acknowledged that every security-oriented rule or guideline carries with it a cost, which in some cases may be only a small inconvenience.

Therefore, every security measure should represent a balance between enhancing security and being reasonably easy to comply with. It is not intended that this physical security policy, or any other security policy, make it more difficult for the company to conduct its day-to-day business.

Revisions

This policy was created for National Training Systems, Inc. by the Flex-Protection team. Until further notice, any changes or updates will be made by either the Flex-Protection team or NTS management. It is necessary that due to the expanding threat landscape and emerging penetration and social engineering methods, the policy will be updated at least annually.

Enforcement

The Policy applies to all employees, contractors, customers and business partners who might need to be present at either the office or the server location. Violations of the policy will be investigated, corrected, and in extreme cases may be grounds for termination of employment or of an existing business relationship.

Technology

Various technology aspects run through the course of normal business, such as online processes, authentication procedures, documentation, databases, barriers, password practices and rules. These are mainly covered in a separate Data Security Policy.

However, there is some inter-connection between Physical Security Policies and various aspects of technology. In order to prevent information about security details and protections being made public, these factors will be described and identified only in general terms. Therefore, this document will not reveal proprietary or protection-related information which could be used in a malicious manner.

Ownership

This Policy is owned by National Training Systems, Inc. NTS retains all rights and has the sole authority to modify or replace this Physical Security Policy.

Policy Objectives

The objective of this policy is to prevent unauthorized access, property damage, data loss, privacy violations, or processes or systems being disabled, and to allow for continuity of operation.

It will balance security protections and controls with the need to conduct business and use data and online systems in day-to-day work.

Security risks will be identified and managed, and where possible, eliminated.

Two Operating Locations

Office / User Network

Our offices represent the site where our employees and contractors do their daily work. The usual deployment of computers and networks are in place. There is also a test lab in the building, for the purposes of testing attacks and defenses as regards data security and hacking vulnerabilities

This document will not reveal what brands are used in network components and desktop computers, what operating system(s) is/are in use, or what protections are in place to thwart attacks.

This policy calls for the internal network to be well defended, without giving additional detail.

Off-site Server Network

Our off-site server network is the highly-secure location where our customers data resides. The data is on a multi-server architecture in a SAS-70 certified facility with robust physical security.

Physical security protecting our network will include, but not be limited to, the following:

Security cards, locked doors, attended reception screening, a man-trap door system, video cameras, locked server racks, and hardware separated into internet-facing and non-internet-facing.

Backups are taken daily to insure continuity in the event of unexpected hardware failure of multiple disk storage drives.

This document will not reveal what brands are used in network components and server hardware and software, what operating system(s) is/are in use, or what specific protections are in place to thwart attacks.

Office Controls

Customer proprietary data will not be retained on the network or computers in the office. Live training data will generally not be used for testing or other in-office activity. If customer data needs to be copied onto any computer in the office for analysis or testing, it will be removed when the activity is completed.

Each employee and contractor will be issued a key for the front office door. A single key for the mailbox will hang on the wall so that various people can check the mail. When an employee or contractor is terminated, he/she will return his/her door key.

Laptops and other portable devices should not be left in the office overnight, which would defeat the purpose of their being portable, and also expose easily-carried devices to actual theft should a break-in occur.

Company-owned desktop computers and printers will remain in the office and not be taken home except with permission. At the end of the day, windows should be closed and locked and the last person to leave should always lock the front door.

Critical electronic documents such as quotes, sales collateral, and important spreadsheets should be stored in Google docs as backup in case of a natural disaster or a break-in wherein the entire office network and/or specific computers are destroyed or stolen.

Similarly, this offers protection against a ransomware attack which destroys all data on a single computer, or multiple computers. It will be the policy of the company to not pay ransom money to a ransomware attacker. More information about protections from Ransomware attacks can be found in the Data Security Policy document.

Personnel may download, or load from a CD or thumb-drive, software and data as needed. USB ports and CD drives will not be removed from office computers or disabled. Employees will be expected to exercise good judgement when selecting tools, data, or software to utilize on their desktop computers.

Server Network Controls

Company Controls

Database server machines will not be connected to the internet; only web sites and web applications will be physically connected to external data lines.

Access to the server network, located at Peak 10, will be granted via photo ID card, only for those employees whose job responsibilities require a physical presence in the server network location.

A complete inventory of server network equipment, including brands, models, serial numbers, and physical descriptions, should be completed, retained in the office, and kept up to date.

A system for securely disposing of unwanted discs, tapes, cards, hard drives, printed paper, and anything else that could contain confidential information should be implemented.

Company personal will abide by Peak 10 (hosting co-location facility provider) rules and regulations at all times.

Controls Provided by Peak 10

The data center facilities are also manned by on-site technical experts 24/7/365 to help ensure equipment and/or critical applications are up and running, immediately accessible and secure. In addition, Peak 10 employs a comprehensive training program to help ensure that Peak 10 data center personnel are trained data center operations and security.

Technical Physical Controls

Peak 10 data center facilities incorporate multiple physical and operational security features and protocols including the following:

- Biometric fingerprint readers
- Card/Personal Identification Number (PIN) access
- Combination lock cabinets
- 24/7/365 monitored video surveillance with video stored for review for non-repudiation.
- Multifactor authentication system
- Staff trained to maintain stringent physical security policies and controls
- Perimeter doors alarmed and monitored
- Exterior landscaping to prevent concealment of intruders

Environmental Controls/Redundancy

Peak 10 data centers incorporate efficient cooling solutions to ensure consistent temperature and humidity levels for protection of mission-critical technology. The data centers are also equipped with distributed cooling with cold aisle containment. In addition, critical facility components (e.g., generators, uninterruptible power supply (UPS) and cooling systems) throughout Peak 10 are redundant. With this level of redundancy, Peak 10 can perform regular preventative maintenance on the equipment with no impact to user entities.

Redundant Network

The Peak 10 network was built to meet or exceed commercial telecommunications standards worldwide for availability, integrity and confidentiality. It incorporates redundancy to ensure reliable connectivity and maximum uptime with no single-point data transmission bottlenecks to or from the data center. Peak 10 data centers are equipped with robust network features, including:

- Dual path data flow
- Redundant carrier class infrastructure
- 10/100/1000Mb ports available
- Redundant Internet access in 100Mb/1Gb/10Gb
- Multiple diverse, ring-protected fiber providers
- Multiple, redundant Tier 1 Internet access providers
- Carrier-neutral telecom services
- Metro Ethernet at 10 Mbps, 100 Mbps, 1 Gbps

Network Features

- Redundant paths for Internet connectivity providing connectivity to other Peak 10 locations
- Redundant carriers per location, providing flexibility to users when choosing private connectivity to their premises and trusted third parties
- Dynamic, performance optimized routing via automated, ongoing hop-count and latency monitoring Burstable services to accommodate unforeseen or seasonal demand
- Redundant, carrier-class infrastructure with no single points of failure
- 300 Gb/s aggregate inter-site network capacity
- 230 Gb/s aggregate Internet capacity
- Choice of 10, 100, 1000, or 10000 Mbps access port options

Security Incidents - Reporting

A security incident is defined as any event that could result or has resulted in:

- The continuity of day-to-day operations being put at risk.
- The availability of a team-member, customer, or resource being put at risk.
- An adverse impact on any process or revenue opportunity, for example:
  - Legal obligation or penalty.
  - Financial loss or disruption of cash flow.
  - Disruption of activities.

An incident that meets the above description must be reported immediately to management.

Other Policies

This Policy is related to, and should be viewed in relation to, all other existing security policies, including the following:

- Data Security Policy
- Cloud Security Policy (if one is created)
- Mobile Devices Security Policy

Compliance Agreement

I have read and understand this Physical Security Policy and agree to abide by the contained rules and guidelines.

I further agree to familiarize myself and agree to any other existing security policies created for National Training Systems, Inc.

Signed	
Print Name	
Date	

This Agreement is to be read and signed by all personnel.