ENPOINTE℠

Physical and Environmental Security Policy

March 13, 2024

Introduction

The security of our buildings and other physical assets is an important consideration, both for staff and for clients. ENPOINTE production facilities are privately owned and single tenant. ENPOINTE controls access to the physical buildings/facilities in which ENPOINTE workforce members operate, in accordance with the HIPAA Security Rule 164.310 and its implementation specifications. In an effort to safeguard Confidential Information from unauthorized access, tampering, and theft, access is allowed to areas only to those persons authorized to be in them and with supervision for unauthorized persons.

Scope

This policy applies to all employees, contractors, consultants, temporary employees, all other workers at ENPOINTE, including all personnel affiliated with external parties, and all equipment that is owned or leased by ENPOINTE.

Requirements

1. ENPOINTE uses electronically controlled door systems to protect all perimeter doors, server rooms, and other areas that may contain Confidential Information.
   - Server room doors require two-factor authentication (badge and PIN)
2. No individuals may enter an ENPOINTE facility without displaying an approved ENPOINTE identification badge.
3. Perimeter doors and restricted areas must be closed and locked when unattended (where feasible):
   - Perimeter doors are never to be blocked open or left unsecured
   - Dock doors must not be left open unless a truck/trailer is parked in front of that door
   - Any exception requires approval by senior leadership
4. Access is given based on business need. Only authorized workforce members receive access to restricted areas as determined by the IT Security & Compliance Manager or Chief Technology Officer (CTO).
5. No “tailgating” or “piggybacking” is allowed through any door, with the exception of other active permanent ENPOINTE staff which may enter the doorway together if both of them are known to have authorized access through this doorway.
6. Employees are responsible for supervising other individuals (e.g., ENPOINTE employees, temporary staff, visitors or vendors) who are provided access.
   - ▪ This includes allowing them to tailgate, opening a door or simply “buzzing” them through the door
   - ▪ If you let them into an area, you are responsible for their behavior.
7. Access and keys are revoked upon termination of workforce members.
8. Workforce members must report lost or stolen key(s) to the Administrative Assistant or IT Security & Compliance Manager.

Security Badges

1. Security ID Badges are issued to every person entering our buildings including all employees, vendors, visitors, and temporary staff.
   - Everyone inside an ENPOINTE building must visibly display their ENPOINTE ID badge at all times
   - Individuals must not loan or give their badge to any other individual
2. Records of all badge access activity are retained.
3. Individuals must report lost/stolen badges to their supervisor or by creating a TrackIt request.
4. Each reception area has an Off Hour Badge Return Box where badges must be returned during off-hour time periods.
5. A visual color-coding system is used to easily identify the individual status of each person on site:

Badge Group	Badge Color
ENPOINTE Employees	Ocean (deep blue)
Temporary Staff	Yellow
Vendors/Contractors	Shoal (teal)
Visitors	Coral (red)

ENPOINTE Employees

1. ENPOINTE employees (Ocean badge) receive a photo-ID security badge during their first days at ENPOINTE.
2. Employee badges have large photos on both sides of the cards.
   - Photos are updated at least once every five years
3. Each badge is authorized for access to specific exterior doors and interior doors as is required by the staff's job functions and responsibilities.
4. Employees who forget their badge must sign-out a 1-Day Employee Badge for that day.
   - These badges do not have building access and are used for identification purposes only
   - During weekday non-holiday office hours, ENPOINTE employees are to obtain a 1-Day Employee Badge from the Receptionist on staff
   - When the front desk is not staffed, the employee must report to a Production Lead or Manager to obtain a 1-Day Employee Badge
   - 1-Day Employee Badges must be returned at the end of shift or the beginning of the staff member's next shift
5. Traditional keys for access to such things as lockers, files cabinets, mechanical or storage rooms, desks, etc., are provided to those staff members whose job functions require them.
   - Company keys are never to be duplicated without advance approval from an ENPOINTE Senior Leader
   - Any additional or replacement keys needed for any reason must be requested from the Administrative Assistant at the Brooklyn Park facility or Corporate Accounting
6. Upon termination, resignation or as requested by management, employee must surrender their ID Badge and key(s)

Temporary Staff

1. ENPOINTE Temp Staff badges are created by temp agency employers following ENPOINTE approved badge designs.
   - Temporary staff are not allowed to use 1-Day Employee Badges
2. Temporary staff must be approved by ENPOINTE Human Resources as having a successful background check, received Security Awareness Training, and having signed the appropriate version of ENPOINTE User Policies prior to any of the following:
   - Accessing any of ENPOINTE most sensitive work areas. (These include Server Rooms, BP Data Production, Network and Telephone Wiring Closets, and 169 Warehouse and Fulfillment Center Distribution Cage.)
   - Working on materials or data containing Protected Health Information (PHI) or Sensitive Personally Identifiable Information (SPII). (Department-specific PHI-SPII training also required.)
   - Working on client or ENPOINTE-owned, high-value assets such as gift cards
   - Obtaining credentials to access the ENPOINTE network beyond shared-user Shopfloor transaction entry
   - Obtaining a restricted version of ENPOINTE facility door access

Vendors

1. Vendor badges are managed by the Purchasing Department.
2. Picture ID Vendor Badges (Shoal badges) are for non-employees who are at ENPOINTE frequently and need access to designated areas of a building at ENPOINTE.
   - These non-employees do not require an escort
3. Vendor Maintenance Badges (Shoal badges) are for repair representatives of frequent ENPOINTE vendors.
   - Individuals must sign in at the front desk, be escorted to the area where they will work, and the sponsoring ENPOINTE staff must monitor this vendor's activity while on the premises
   - These badges must have limited door access and be returned when leaving the building
4. Vendors must sign out and return their badge when leaving at the end of each workday.

Visitors

1. During business hours, visitors must use the main entrance to ENPOINTE buildings and register with the receptionists to receive a visitor badge (Coral badge).
   - Individuals must sign in at the front desk, be escorted to the area where they will work, and the sponsoring ENPOINTE staff must monitor this vendor's activity while on the premises
   - These badges do not provide door access

2. Visitors must show photo identification before being admitted into ENPOINTE facilities.
    - If a visitor or vendor representative arrives to ENPOINTE facilities without proper photo identification, that person will only be admitted into ENPOINTE facilities if an ENPOINTE employee verifies their identity and signs a form to accept responsibility for the person while on ENPOINTE premises
3. The following must be logged for all visitors:
    - Date of visit
    - Visitor name and organization/firm
    - Form of identification shown/checked
    - Visitor badge # issued
    - Name of person visited
    - Time of entry and departure
4. In the case of visitor tours into a secured work area, the department manager of the secured work area must pre-approve visitor access to the secure work area after ensuring there are no PHI or SPII materials visible to visitors.
5. Visitor badges must be returned when the visitor departs ENPOINTE facilities.
    - After business hours, all visitors must be checked in with a shift leader or supervisor
6. External drivers who are picking up and/or delivering materials at our loading dock are exempted from this visitor badge requirement.
    - These individuals are supervised by the ENPOINTE employees who are receiving or sending the shipments
7. All visitors must be supervised at all times. Due to security and insurance reasons, no unauthorized visitors are allowed.
8. Logs of visitor access are retained for two years.
9. Logs of visitor access are collected by Human Resources and reviewed by the CTO semi-annually.
10. Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from ENPOINTE.

Access Reviews

1. Badges (security access cards) are audited on a routine basis to verify that the employees, temporary staff, visitor, and vendor card policies outlined in the ENPOINTE User Policies are being followed.
2. All active badges are audited twice a year to verify that only active employees, approved non-employees, and vendors have access.
3. Annual access reviews are conducted by area managers to ensure employees only have the physical access required to perform their work.
4. Access to sensitive areas (Server rooms, telephony rooms, networking rooms, Data Processing, and Distribution Cage) are audited quarterly by Leaders in the IT department.
5. All active badges are reviewed every 60 days to identify inactive badges.
    - Badges that are inactive for over 90 days are disabled unless approved by CTO or IT Security & Compliance Manager
    - A valid business reason needs to be documented in order to keep a badge active past 90 days

Video Surveillance

1. All entrances and server room doors in production facilities are covered by centralized camera systems to monitor traffic and access at our facilities and enhance the safety and security of our team members.
2. Video recordings are retained for at least 90 days.

External and Environmental Threats

1. Intrusion detection devices including glass break and door sensors motion sensors are installed at ENPOINTE production facilities and monitored 24/7 by a third-party security provider.
2. Fire extinguishers, sprinklers, smoke, heat, and fire detectors are installed at ENPOINTE production facilities, according to applicable laws and regulations, and monitored 24/7 by a third-party security provider.
    - Heat and humidity detectors are installed in all server rooms. E-mail and text notifications are sent to the IT Security & Compliance Manager and IT Systems team if defined thresholds are reached
3. All server room equipment and sensitive production equipment are on UPS backup systems.

4. Customer facing web sites and related application servers are kept offsite at an approved vendor hosting facility with UPS and generator backup.

Maintenance

1. Repairs to physical security equipment are documented and retained in the IT ticketing system.
2. Maintenance is controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies, and the organizations maintenance program.
   - Server room and telecom cabinets are covered under a maintenance calendar that documents required checks for normal cleaning and organizing tasks

Compliance

Violation of Policy

Failure to comply with this policy may result in disciplinary action up to and including termination and/or legal action.

Policy Exceptions

Any exceptions to this policy must receive prior written approval from the Chairman/Chief Executive Officer or Chief Technology Officer.