ENPOINTE℠

# Access Control Policy

November 20, 2023

Classification: Confidential

Introduction 2
Scope 2
Requirements 2
User Identification 2
Password Management 2
Workforce Clearance 3
Personal and Mobile Devices 4
Automatic Lock/Logoff 4
Clean Desk/Clear Screen 4
Cameras and Camera Phones 5
FireIDs 5
Remote and Virtual Worker Access 5
Access Reviews 6
Account Termination 6
Procedures 6
Access Establishment and Modification 6
Access Reviews 7
Violation of Policy 7
Policy Exceptions 7

# Introduction

Access to ENPOINTE systems and applications is restricted for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity. Access is provided on a minimum necessary basis based on the principle of least privilege. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems. These safeguards have been established to address the HIPAA Security regulations.

## 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

## User Identification

1. Access to ENPOINTE systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user.
    - Temporary and anonymous accounts are not used unless absolutely necessary and approved by the Confidentiality, Availability, Privacy, and Security (CAPS) committee for business purposes
    - In the case of non-personal information, such as generic educational content, identification and authentication may not be required.
2. Users must not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. If a user believes their user ID has been compromised, they are required to immediately report the incident to the IT Department.
4. In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the CAPS committee to limit access and reduce risk of unauthorized access.
5. Default accounts on all production systems, including root, are disabled where possible. If they are required, the default password is changed.
6. Shared or generic service accounts are only to be used for their defined functions and must adhere to these guidelines:
    - Can only log on to specified computers
    - Can only access defined applications
    - File access limited to application required shares
    - Limited access to the Internet
    - Limited access to email
7. Direct system to system, system to application, and application to application authentication and authorization is restricted and not permitted unless absolutely needed.
8. Active Directory accounts and objects are reviewed every 60 days to identify inactive accounts/objects.
    - Accounts that are inactive for over 90 days are disabled
    - Accounts that are inactive for over 180 days are deleted
    - A valid business reason needs to be documented in order to keep an account/object active past 180 days.
9. All endpoints display the following logon message:
    - "This system and the information it contains are the sole property of ENPOINTE and should only be accessed by authorized users. By logging on to this system, you have agreed to the ENPOINTE User Policies and acknowledge that all activity may be logged and monitored"

## Password Management

1. User IDs and passwords are used to control access to ENPOINTE systems and must not be disclosed to anyone for any reason.
2. All ENPOINTE network password configurations are set to require:
    - Minimum length of 12 characters

- Must contain at least three of the following criteria:
    - uppercase characters
    - lower case characters
    - numbers
    - symbols
- Cannot contain the user’s first or last name
- Prevention of password reuse using a history of the last 20 passwords
- 60-day password expiration for all named user accounts
- Account lockout after five invalid attempts
    - Accounts are automatically unlocked after 30 minutes

3. Upon initial login, users must change any passwords that were automatically generated for them.
4. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the organization, based on the criticality and sensitivity of the information contained within the network, system, application, and/or database.
5. Password(s) for domain administrator and network device accounts are changed when an IT employee with access to the password(s) terminates their employment with ENPOINTE, and no less frequently than on an annual basis.
6. All default system, application, and partner passwords are changed before deployment to production.
7. Password change methods must use a confirmation method to correct for user input errors.
8. A user’s identity must be verified in-person or via a known good communication channel before performing password resets.
    - IT staff members must provide passwords for user accounts and client accounts directly to the account user(s) without providing the passwords to other individuals. Client account passwords must not be provided to ENPOINTE staff members including Sales and CSR team members
    - See **IT017 - Identity Verification for Changing/Resetting Passwords** for more information
9. Passwords cannot be displayed in public areas (at your desk, under your keyboard, etc.).
10. Account credentials (usernames and passwords) for business-related websites and applications may only be automatically populated after first authenticating to the device, and only using approved password management tools.
    - The use of auto-populate functions built into Internet browsers (e.g., Google Chrome, Mozilla Firefox) is prohibited
11. All system and application passwords are not displayed at any time and must be stored and transmitted securely.
    - Where possible, passwords must be stored in a hashed format using a salted cryptographic hash function (SHA-256 or equivalent)
    - Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in the **Communications and Operations Management Policy**
    - Passwords must not be distributed via email. The exception is for one-time passwords which immediately require a password reset upon next login
    - ENPOINTE must transfer encrypted documents and associated passwords in separate transmissions
12. All passwords used in configuration scripts are secured and encrypted.
13. Automated log-on configurations that store user passwords or bypass password entry are not permitted for use with ENPOINTE workstations.
    - This applies to unique/named user accounts only. It does not apply to shared or generic service accounts, data collection accounts, and other non-interactive logins

## Workforce Clearance

1. Different access and service levels for different ENPOINTE roles are given to staff depending on the nature of the work.
2. The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification.
3. Role-based access categories for each ENPOINTE system and application are pre-approved by the CAPS committee.
4. Any ENPOINTE workforce member can request change of access using the process outlined in **Access Establishment and Modification.**
5. To prevent unauthorized system changes or application installs, users of local endpoints do not have local administrative rights by default.

- Local administrator rights are only provided when a business case has been demonstrated. In most cases, temporary administrator rights are sufficient to complete the required task, after which time the rights must be revoked
- Only users that require administrative rights to perform day-to-day job functions will be allowed to retain those rights on a permanent basis

6. Privileged users must first access systems using standard, unique user accounts before switching to privileged users and performing privileged tasks.
    - Rights for privileged accounts are granted by IT Systems or the IT Security & Compliance Manager by using the process outlined under **Access Establishment and Modification section of this policy**
7. Individuals are responsible for actions taken by others using their credentials. Users of multi-user computers (e.g., DC Stations, Conference Room PCs, Airport or Café Kiosks) must log-off of the computer when leaving the device.
8. Employees must only use ENPOINTE-purchased and -owned endpoints for accessing production systems with access to ePHI/SPII data.
9. When accessing production systems via remote wireless connections, the same system access policies and procedures apply to wireless as all other connections, including wired.

## Personal and Mobile Devices

1. All mobile computing or storage devices (e.g., laptop, mobile phone, USB flash drive, external hard drive) must be kept secure at all times.
    - If mobile devices will be left unattended in public areas (e.g., coffee shop, client location, park bench) they must be physically secured (e.g., laptop cable lock) to prevent theft
2. Customers, visitors, and other non-ENPOINTE staff are strictly forbidden from accessing ENPOINTE computers or connecting their own device to the wired ENPOINTE corporate network without explicit permission from the IT Systems team.
3. ENPOINTE provides access to the corporate email system for employees that have demonstrated a business need to access email remotely.
4. Users wishing to access ENPOINTE's corporate email system or other ENPOINTE resources with a personal (non-ENPOINTE) owned mobile device must agree to our mobile device requirements in our User Policies.
    - This outlines required technical settings that must be enabled on the device
5. When an employee is terminated, any ENPOINTE data and email accounts must be deleted from the personal device.
6. An audit of ActiveSync settings and devices on all mailboxes is performed annually.

## Automatic Lock/Logoff

1. Information systems must be inaccessible to users via screensaver locks after 15 minutes of inactivity.
    - Workstations in high-traffic areas or used for highly-sensitive roles are configured to automatically lock screens after five minutes of inactivity
    - Exceptions to automatic screen lock requirements are reviewed and approved by the CAPS committee
2. Open application sessions and network sessions must be closed after 30 minutes of inactivity and require the user to reauthenticate.
    - Systems are configured to end open application and network sessions after 30 minutes of inactivity
    - Policy exceptions are created for all systems that cannot follow this requirement due to system limitations or business requirements

## Clean Desk/Clear Screen

1. To prevent co-mingling, employees should only access Confidential Information in physical or electronic form for one job at a time.
2. Employees are required to ensure that all Confidential Information in hardcopy or electronic form are secure in their work areas at the end of the workday and when employees are away for an extended period.
3. Computer workstations that are logged in via user accounts must be locked when the workspace is unoccupied.
4. Confidential Information must be removed from workspaces and placed in a locked drawer or office when the workspace is unoccupied and at the end of the workday.
5. Drawers and cabinets containing Confidential Information must be closed and locked when not in use or attended.

6. Keys used for access to Confidential Information must not be left at an unattended workspace.
7. Mobile devices must not be left unattended in public areas.
8. Passwords must not be left on hardcopy in any work area.
9. Printouts containing Confidential Information must be immediately removed from printers.
10. Disposal of Confidential information must be via secure recycling bins.
11. Whiteboards containing Confidential Information must be erased prior to vacating the corresponding location.
12. Mass storage devices such as CD's, DVD's or USB drives must be treated as containing Confidential Information and stored in locked drawers.

## Cameras and Camera Phones

1. Use of cameras or other photographic devices inside ENPOINTE facilities is restricted.
2. In some production and quality management functions, ENPOINTE staff are required to photograph their work output as part of their standard responsibilities. In all other cases, the use of cameras (or other photo taking devices) is not allowed on ENPOINTE property without the approval of a senior ENPOINTE leader.
3. Employees must not use any form of photographic equipment, including without limitation camera phones or cameras on other mobile devices, without express written permission of ENPOINTE.
   - Team members who are supervising ENPOINTE visitors must ensure that their visitors also comply with this policy

## FireIDs

Access to servers containing client data is prohibited by Developers while they are using their standard login accounts. Administrator-level accounts have been created for each Developer for their occasional, required access to these servers. These local administrator account names are denoted by the Developer's initials plus the prefix of "FIREID." These FIREID accounts are placed into specific groups in AD which are named "LA_" plus the server's name. Developers use their normal user accounts for day-to-day work and will only us their FIREID Accounts when absolutely required to complete the project at hand.

Each month the Director of Business and Custom Applications creates a new TrackIt ticket to log all of the month's FireID usage. Attached to this ticket is a log spreadsheet to track each FireID use.

The Developer logs in using their FireID account which is configured to utilize MFA for windows RDP.

The Security Information and Event Management (SIEM) system sends an email alert to all CAPS team members whenever a FireID is used to access a server that contains non-anonymized client data. The TrackIt tickets and alert emails are corelated, with any missing information updated in TrackIt. The Developer's manager closes the ticket after the month's end.

ENPOINTE utilizes Blumira Security Information and Event Management (SIEM) system to supply an email alert to all CAPS committee whenever a FireID is used to access a server.

## Remote and Virtual Worker Access

1. Methods for remote and virtual access to ENPOINTE computers systems are reviewed and approved by the CAPS committee and must meet the following requirements:
   - Require two-factor authentication
   - Do not allow file transfers to outside of our network
2. All devices used to establish a remote and virtual connection must:
   - Require authentication (e.g., password/PIN)
   - Have up-to-date anti-virus software
   - Have a local firewall
3. The list of employees approved for remote and virtual access is reviewed annually by the Chief Technology Officer (CTO).
4. Employees must not download Confidential Information to any remote devices used to connect to production systems.

5. All remote (teleworking) workforce members are trained on the risks, the controls implemented, their responsibilities, and sanctions associated with violation of policies.
6. Exceptions to the requirement for two-factor authentications are permitted for services that reference internal systems and do not process client data.
    - Examples: Resource Board, Job Initiation, Competitive Analysis, and Sales Toolbox

## Access Reviews

1. All access to ENPOINTE systems and services are reviewed and updated on a recurring basis to ensure proper authorizations are in place commensurate with job functions. The following is a list of systems and the frequency of reviews performed:
    - Permissions of all file shares – Annually
    - Membership of Administrators and Remote Desktop Users groups on all Windows devices – Semi-annually
    - Membership of Administrators on all Mac devices – Semi-annually
    - Permissions of Explicit Access FTP directories and DP Production Share – Semi-annually
    - All users with access to Prinergy – Annually
    - All users with access to Team Foundation Server – Annually
    - All internal (ENPOINTE employee) accounts in all external facing web sites – Annually

## Account Termination

1. The IT Department disables user access rights immediately upon notification and coordinates with the appropriate employees to terminate access to any systems managed by those employees. Or, IT will change password and assign to a single user.
2. All ENPOINTE information disclosed to users must be returned or destroyed. All work done by users for ENPOINTE is ENPOINTE property, and it too must remain with ENPOINTE when a user departs.
3. The IT Security & Compliance Manager may audit and terminate access of users that have not logged into organization's information systems/applications for an extended period.

# Procedures

## Access Establishment and Modification

Requests for physical or logical access to ENPOINTE systems and applications must be made formally using the following process:

1. The ENPOINTE workforce member, Human Resources, or their manager, initiates the access request by creating a request in the IT ticketing system.
    - User identities must be verified prior to granting access to new accounts
    - Identity verification must be done in person or over the phone
2. The IT Security & Compliance Manager along with the IT Systems team will grant access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the request must be approved by the requester's direct manager, the owner of the area/share in question, or by a member of the CAPS committee.
3. Once the review is completed, the team member approves or rejects the request. If the request is rejected, it goes back for further review and documentation.
4. If the review is approved, the team member then grants the requested access, adding any pertinent notes required, and marks the ticket as closed.
    - New accounts must be created with a temporary secure password that meets all requirements from **Password Management**, which must be changed on the initial login
    - All password exchanges must occur over an authenticated channel
    - For production systems, access grants are accomplished by adding the appropriate user account to the corresponding AD group

- For non-production systems, access grants are accomplished by leveraging the access control mechanisms built into those systems. Account management for non-production systems may be delegated to an ENPOINTE employee at the discretion of the CAPS committee

5. Access is not granted until approval receipt, review, and approval by the team member.
6. Access granted to internal and external user/parties must be limited in duration and revoked when no longer needed.
7. The request for access is retained for future reference.

## Access Reviews

The process for conducting access reviews is as follows:

1. The IT Security & Compliance Manager initiates the review of user access by creating a request in the IT ticketing system.
2. The IT Security & Compliance Manager is assigned to review levels of access for each ENPOINTE workforce member.
3. If user access is found during review that is not in line with the least privilege principle, the **Access Establishment and Modification** process is used to modify user access and notify the user of access changes. Once those steps are completed, the request is then reviewed again.
4. Once the review is completed, the team member approves or rejects the request. If the request is rejected, it goes back for further review and documentation.
5. If the review is approved, the team member then marks the ticket as closed, adding any pertinent notes required.

# 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.