ENPOINTE℠

# User Policies

**February 26, 2025**

**Classification: Confidential**

# ENPOINTE User Policies

**Protecting ENPOINTE and Client Assets**

## Introduction

### Purpose

These policies exist to define the standards for responsible use of ENPOINTE's assets, communication systems, and proprietary information. It is designed to protect the company, workforce members, and clients by ensuring compliance with security best practices, legal requirements, and ethical responsibilities. By adhering to these guidelines, workforce members contribute to a secure and professional working environment that upholds ENPOINTE's integrity and business operations.

### Policy Overview

These policies outline the acceptable use, security, and confidentiality expectations for all ENPOINTE workforce members, contractors, and affiliated personnel. It covers topics such as communication system usage, remote access, proprietary rights, privacy, and security incident reporting. All workforce members must read, understand, and comply with these guidelines to protect company and client assets, mitigate security risks, and ensure compliance with industry standards and legal regulations.

### Scope

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

### Responsibilities

All workforce members (including contractors) are responsible for:

1. Reading and signing off on all requirements stated in this policy.
2. Reading applicable information security policies and procedures at least annually.
3. Actively participating in all security awareness and training events.
4. Complying with the requirements described in this procedure and for reporting any deficiencies, security incidents or instances of non-compliance.
5. Workforce members are responsible for all activity performed under their assigned user IDs.

## Requirements for Use of ENPOINTE Communication Systems

Corporate communication systems are ENPOINTE property to be used for general business purposes to increase productivity and employee's effectiveness. These systems include telephone, voicemail, e-mail, internet technologies, and any other system that has access to confidential materials or information. Incidental personal use of some of these systems is permissible so long as it does not consume more than a trivial amount of resources, interfere with productivity, preempt any business activity, or disclose Confidential Information.

Workforce members agree and understand that they:

1. will not use software licensed to ENPOINTE on a personally owned device that is not authorized unless the usage has been approved by the IT Systems team;
2. will not download software or executables to ENPOINTE-owned devices unless specifically authorized to do so by the IT Systems team or automatically executed by a process managed by IT (e.g., printer drivers);
3. will seek and receive approval from the IT Systems team before connecting any computers, switches, wireless adapters, phone modems or other devices to the ENPOINTE network;
4. will not store business data or customer files on local desktops;
5. will not store personal files on ENPOINTE computer systems.

In addition, workforce members understand that:

1. Testing, monitoring or attempting to compromise any information security mechanism is prohibited unless authorized by the IT Systems team.
2. Devices purchased by ENPOINTE are the property of ENPOINTE and must only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.

a) All workforce members are required to monitor their devices and report unauthorized users and/or unauthorized attempts to access systems/applications.

3. Encryption techniques are implemented; however, email messages are only encrypted if the receiver of the message also uses encryption. Users must assume that any message they draft and send could be intercepted and read by others.
4. Credit card numbers and Social Security Numbers must not be stored or transmitted via ENPOINTE systems without the advance permission of the ENPOINTE Chief Executive Officer (CEO), Chief Financial Officer (CFO) or Vice President of Technology).
5. The transmittal, retrieval or storage of information that is knowingly false, harassing, obscene or discriminatory about a person's race, color, sex, age, disability, religion, national origin, physical attributes, sexual orientation or any form of illegal discrimination is not permitted.
6. The use of corporate communication systems for personal gain, charitable endeavor or any other purpose which is illegal or against company policy is not permitted.

***Internet Use***

1. ENPOINTE prevents users from connecting to certain non-business web sites.
2. The ability to connect with a specific web site does not in itself imply that users of ENPOINTE systems are permitted to visit these sites.
3. Users must not use the Internet for any use that may result in a violation of ENPOINTE policies.

***Monitoring and Privacy***

1. Workforce members should not assume any expectation of privacy when using ENPOINTE information systems, including voicemail, email, and the Internet.
2. Modern security practices sometimes include the use of biometric data to verify the identity of individuals who are accessing systems. (E.g., Laptops use fingerprint readers, and our Colo facility uses retinal scanners.) The data (e.g., fingerprints) are stored inside such systems for ongoing comparison to an individual who is attempting to access the systems. ENPOINTE will utilize such modern technologies to continually improve our security practices.
3. ENPOINTE may routinely log and review any and all activity and data created, viewed, sent or received on the network including telephone numbers dialed, web sites visited, email traffic, and all other keystrokes.
4. ENPOITNE may occasionally correspond with workforce members via their personal mobile devices. This includes telephone and/or SMS (text) messages sent for informational and/or emergency purposes.

***Physical Security***

1. Each trusted workforce member at ENPOINTE must take responsibility to ensure that our physical assets are safe and secure and comply with all the requirements of our **Physical and Environmental Security Policy** available on company Intranet.
2. ENPOINTE uses electronically-controlled door systems to protect all perimeter doors and other areas that may contain Confidential Information.
3. Perimeter doors and restricted areas must be closed and locked when unattended:
    a. Perimeter doors are never to be blocked open or left unsecured.
    b. Dock doors must not be left open unless a truck/trailer is parked in front of the door
    c. Any exception requires approval by senior leadership.
4. No "tailgating" or "piggybacking" is allowed through any door.
5. Workforce members are responsible for supervising other individuals (e.g., ENPOINTE staff, temporary workforce members, visitors or vendors) who are provided with access.
    a. This includes allowing them to tailgate, opening a door or simply "buzzing" them through the door
    b. If you let them into an area, you are responsible for their behavior and actions.
6. In addition to electronic locks and badge access, the company has video cameras in various locations inside and/or outside of the buildings.
    a. Workforce members consent to being monitored with actions recorded by video cameras.

***Remote Access (VPN or LogMeIn Remote Control)***

1. Workforce members must comply with all ENPOINTE network access security requirements when remotely connecting to ENPOINTE systems.
2. Manager approval is required before remote access to the ENPOINTE network is granted.
3. Only ENPOINTE-approved remote access software that requires multi-factor authentication (MFA) may be used.

4. While connected to the ENPOINTE network, workforce members are responsible for ensuring that no unauthorized individuals access their device.
5. Remote access is limited to:
    a. Controlling an ENPOINTE-owned workstation physically located inside an ENPOINTE facility via LogMeIn.
    b. Connecting to the ENPOINTE corporate network via VPN using an ENPOINTE-issued device.
    c. No data files may be transferred outside of the ENPOINTE network during remote access sessions.
6. When using LogMeIn from a personal device, the device must meet the following security requirements:
    a. An actively supported operating system with the latest security patches installed.
    b. Up-to-date antivirus software and an active local firewall.
7. Client-owned data and graphics files may not be transferred from the ENPOINTE network. Remote access sessions rely on encrypted connections to internal ENPOINTE workstations and do not involve external file transfers.
8. Removing physical materials, including client documents or samples, for remote work is only allowed with prior written approval from the department manager, Chief Administration Officer, or Vice President of Technology.

***Mobile Device***

1. ENPOINTE provides mobile email access to the ENPOINTE corporate email system for users who have demonstrated a business need to access our email remotely.
2. All mobile device connections to ENPOINTE technology and communications systems must comply with the same acceptable use policies as required for other ENPOINTE technology connections.
3. All mobile devices that interact with ENPOINTE systems (e.g., email, ftp, remote connections) are covered by this policy.
4. ENPOINTE will only provide email access to mobile devices which comply with supported ENPOINTE network access technology and security requirements.
5. Mobile devices may not be configured to access ENPOINTE email without approval of their manager.
6. The following security practices must be followed:
    a. Mobile device users must agree to have the following technical settings enabled.
        i. Auto-Lock/Screen Timeout enabled at a minimum of five minutes of inactivity.
        ii. Unlock with a method such as:
            1. PIN with minimum of four digits
            2. Biometric such as fingerprint
            3. Swipe pattern
7. Users of mobile devices with access to ENPOINTE email must take appropriate measures to protect their devices and any corresponding removable storage media from loss, theft, unauthorized access or misuse.
8. Users of mobile devices with access to ENPOINTE email must immediately report to IT Support (via TrackIt helpdesk work order) if their device is lost or stolen.
9. When a user upgrades or changes phones, the old phone must be wiped and reset to factory settings.
10. Users of mobile devices must understand and agree that ENPOINTE and client data may be deleted from the device at the discretion of ENPOINTE and/or the data owner. Some reasons the data may be deleted include user job role changes, termination, resignation or retirement.
11. Mobile devices may not have an ENPOINTE email account unless they are fully supported with regular security patches by their manufacturers and/or carriers.
12. Mobile devices with expiring vendor support must have ENPOINTE email accounts removed prior to vendor's end-of-support dates.
13. Mobile devices with access to ENPOINTE email must be updated with all available security patches within 30 days of availability.
14. Mobile devices that have circumvented security controls (e.g., jailbreaking or rooting) may not connect into the ENPOINTE corporate systems.

# Confidentiality

ENPOINTE, its clients, and their respective agents and affiliates may disclose to workforce members or they may create on behalf of ENPOINTE and its clients, Internal or Confidential Information. It is every employee's responsibility to ensure all Internal and Confidential Information, as defined by our **Asset Management Policy**, is treated as non-public and all intellectual property generated as a part of employment must be owned by ENPOINTE.

| | Public Information | Internal Information | Confidential Information |
|---|---|---|---|
| **Definition** | Information "that everybody already knows" and does not expose ENPOINTE to adverse risk. | Information "for business use only." Internal information is unique and/or valuable to ENPOINTE or our clients and is not readily available to the public or our competitors. | Intended solely for use by those with a "need-to-know. Confidential Information is unique and/or valuable to ENPOINTE, includes anything a client deems to be confidential or sensitive in nature, and must be protected from disclosure. |
| **Examples** | ENPOINTE Marketing Brochures,<br>Any Business Cards<br>Any Press releases<br>Public information about ENPOINTE clients | ENPOINTE Employee handbook<br>ENPOINTE Telephone directory<br>Client Correspondence<br>Non-Sensitive Customer Data<br>Client Graphics without Personal Data<br>ENPOINTE Trade Secrets, Inventions, Processes | ENPOINTE Personnel records<br>ENPOINTE Policies<br>Sensitive Personally Identifiable Information (SPII)<br>Protected Health Information (PHI)<br>Client Trade Secrets, Inventions, Processes, Business Plans, Strategies, Models, Customer Lists, Contracts, Bids/Costs, Reports, Finances<br>Anything a customer deems as Confidential |
| **Reproduction, Transfer or Disclosure** | Unless otherwise stated, may be reproduced, transferred, or disclosed to anyone without violating an individual's or customer's right to privacy. | Requires ENPOINTE Data Owner authorization.<br>Must only be disclosed to ENPOINTE workers and non-ENPOINTE personnel covered by a non-disclosure agreement. | Requires ENPOINTE Data Owner authorization and/or customer consent.<br>Must be encrypted while at rest and while being transmitted over untrusted or non-secure networks and devices. |
| **Criticality** | Public Data is not deemed critical. | Internal Information is deemed critical.<br>Unauthorized disclosure, compromise, or destruction of Internal Data would potentially impact ENPOINTE reputation and could lead to a loss of business. | Confidential Information is deemed critical.<br>Unauthorized disclosure, compromise, or destruction could have an adverse impact on ENPOINTE, its members, customers, or workforce members and result in potential federal and state legal action. |
| **Incidence Response** | No response is required for incidents of reproduction, transfers, or disclosure of Public Data | Unauthorized reproduction/transfers/disclosure of ENPOINTE Internal Information is categorized as a Low impact incident.<br>Unauthorized reproduction/transfers/disclosure of Customer Internal Data is categorized as a Medium impact incident. | Unauthorized reproduction/transfers/disclosure of ENPOINTE Confidential Information is categorized as a Medium impact incident.<br>Unauthorized reproduction/transfers/disclosure of Customer Confidential Information is categorized as a High impact incident. |

1. ENPOINTE workforce members must prevent unnecessary internal exposure by keeping Internal and Confidential Information secured while in their possession and within their work areas as defined by our **Access Control Policy**.
2. Transmitting or disclosing any Internal or Confidential Information to unauthorized parties is prohibited without explicit permission from the information owner.
3. Internal or Confidential Information cannot be transmitted over a non-secure channel (e.g., email, FTP, USB drive) unless specifically requested by the customer or information owner.
4. Some workforce members at ENPOINTE are provided with privileged access to use collaboration tools which provide the ability to transfer files between system users (e.g., Microsoft Teams).
    a. These collaboration tools may not be used in any manner to transfer Confidential Data or any client-owned data files containing names and/or addresses.
5. The use of Internal or Confidential Information for personal gain, the benefit of another, or any other non-business related purpose is prohibited.
6. Internal or Confidential Information furnished in any form must not be duplicated except as is reasonably necessary in the performance of their duties for ENPOINTE.
7. Removing any client-owned Internal or Confidential Information, including without limitation samples of work, copies, electronic files, proofs, overs, spoilage, materials, supplies, and job specifications, from an ENPOINTE facility is prohibited.

8. Upon the request of ENPOINTE, a Client, or in the event of termination (voluntarily or involuntarily), the following must be returned within 24 hours:
    a. All Internal or Confidential Information received in any form, including copies, or reproductions or other media;
    b. All ENPOINTE property including without limitation, all keys, access cards, credit cards, computers, phones, computer storage media, computer login information, and the like.

***Transmission of Files via Non-ENPOINTE Systems***

Client assets must not be transmitted via any system which is not managed or supported by ENPOINTE, specifically requested by our client (owner of the assets), or approved in advance by the ENPOINTE Confidentiality, Availability, Privacy, and Security (CAPS) committee. This includes the following:
1. Social media websites such as Facebook, LinkedIn, etc.
2. Personal email accounts such as Gmail, Yahoo, Comcast, etc.
3. File-sharing systems not managed by ENPOINTE

Client assets must not be transmitted via publicly-hosted collaboration sites (e.g., Microsoft Teams).

# Proprietary Rights

Our customers trust us with confidential data and other materials, and they require us to ensure that all proprietary rights are properly assigned to ENPOINTE. For these reasons, all team members must assign to ENPOINTE all proprietary rights developed as a part of their employment.

“Proprietary Rights,” as used herein is intended to include all forms of intellectual property in whatever form including, without limitation, any and all: patents and patent applications (whether in existence now or in the future), inventions, industrial designs, industrial models, utility models, certificates of invention, processes, ideas, know-how, trade secrets, Confidential Information, copyrights, copyright applications, moral rights, works of authorship, software and software code, trademarks, trademark registrations and applications, whether or not any of the foregoing is in writing or reduced to practice, is patentable, copyrightable, trademarkable or otherwise perfected, registered or recorded, and any and all indicia of commercial source or origin and all goodwill associated with any of the foregoing anywhere in the world.

***Assignment of Proprietary Rights***

Workforce members agree that all Proprietary Rights they conceive of or make, including those they have already conceived of or made, either alone or in conjunction with others, while employed by ENPOINTE are the sole and exclusive property of ENPOINTE. With respect to any such Proprietary Rights, workforce members agree to:

1. Provide ENPOINTE with current, accurate, and complete records of all Proprietary Rights, which records will belong to ENPOINTE and be kept by ENPOINTE.
2. Promptly and fully disclose the existence and describe the nature of any Proprietary Rights to ENPOINTE.
3. Assign, in writing, and workforce members hereby do assign, to ENPOINTE all of their rights, titles, and interests, whether legal or equitable, including rights to all past infringement actions and damages or settlement recoveries, to the Proprietary Rights.
4. Acknowledge and deliver promptly to ENPOINTE any written instruments, and perform any other reasonable acts necessary in ENPOINTE opinion and at its expense to preserve its Proprietary Rights against forfeiture, abandonment, or loss and to obtain and maintain letters patent, copyrights and/or trademarks on Proprietary Rights and to vest the entire right, title, and interest to Proprietary Rights in ENPOINTE, provided that workforce members make no warranty or representation to ENPOINTE as to rights against third parties hereunder.
5. Provide to ENPOINTE, at its request and expense, assistance, including testimony in all legal proceedings, and generally do all things which may be necessary or desirable to effectually secure to, and vest in ENPOINTE, its successors, or its assigns, the entire right, title, and interest in and to any Proprietary Rights and aid ENPOINTE in enforcement of its rights in the Proprietary Rights.

Workforce members hereby designate and appoint ENPOINTE and its duly authorized officers and agents as their agents and attorneys-in-fact, with full power of substitution, to act for and in their behalf and instead of them, to execute and file any documents and to do all other lawfully permitted acts to further the above purposes related to Proprietary Rights with the same legal force and effect as if executed by them.

Workforce members also agree that their obligations to cooperate with ENPOINTE with respect to any Proprietary Rights made by them while employed for ENPOINTE will survive the termination of their employment with ENPOINTE.

### *Exclusions from Assignment*

Pursuant to the requirements of Minnesota Statutes Section 181.78, the provisions related to Proprietary Rights shall not apply to any inventions for which no equipment, supplies, facility or trade secret information of ENPOINTE was used and which was developed entirely on workforce members own time, and (1) which does not relate (a) directly to the business of ENPOINTE or (b) to ENPOINTE actual or demonstrably anticipated research or development, or (2) which does not result from any work performed by workforce members for ENPOINTE.

## Corporate Public Image

ENPOINTE has expectations from its workforce members regarding their behavior towards their colleagues, supervisors, the overall organization, while in public. Although we promote freedom of expression and open communication practices, all workforce members are still obliged to follow a code of appropriate conduct established by the company.

### *Workforce Member Conduct in Public*

All communications as a representative of ENPOINTE reflects on our corporate image. Workforce members agree that they will refrain from abusive, discriminatory, harassing, bullying, threatening, knowingly false, illegal or offensive communication. This includes, but is not limited to, verbal, telephone, email, social networking sites, forums, and any other methods of communication used in relations to their employment.

Unless expressly authorized by ENPOINTE, workforce members must express only their personal opinions. Workforce members must not represent themselves as a spokesperson for ENPOINTE unless that is part of their formal job description. If ENPOINTE is a subject of communication, workforce members must be clear and open about the fact that as non-authorized workforce members, their views do not represent those of ENPOINTE, fellow workforce members, customers, suppliers or people working on behalf of ENPOINTE.

### *Workforce Member Identity*

No messages may be transmitted without the workforce members identifying themselves in the message. Transmittal of messages with anonymous or fictitious names is prohibited.

## Security Incidents

ENPOINTE workforce members are required to report all security incidents to their manager and the IT department as soon as they are aware of them. If the incident needs immediate attention (e.g., a stranger in an ENPOINTE building without an ID Badge), workforce members must either:

1. Communicate the problem to the nearest Lead/Manager.
2. Address the problem and then immediately communicate with a Lead/Manager.

Security incidents should be reported to IT via securityincidents@alwaysenpointe.com.

## Background Check and Communications Requirements

ENPOINTE will conduct background checks via a contracted third party on all new workforce members, rehires within one year of termination, and any non-workforce members that have badge/physical access to an ENPOINTE facility or electronic access to the ENPOINTE network/email. ENPOINTE also reserves the right to perform additional background checks as needed in the course of ENPOINTE business.

In addition, this ENPOINTE policy requires all workforce members and non-workforce members to communicate the details of their criminal convictions to the ENPOINTE Human Resources Manager within one business day for any conviction of a crime(s) which are felonies, thefts, forgeries or crimes of public mistrust.

## Privacy

In addition to meeting our confidentiality and non-disclosure requirements for client-owned information assets, ENPOINTE expects all workforce members to comply with our **Privacy Policy** which protects individuals who share their information directly with ENPOINTE. The **Privacy Policy** is available to all workforce members via the ENPOINTE website https://alwaysenpointe.com/privacy-policy.

If workforce members have any other security, confidentiality or privacy-related concerns, they should contact the Vice President of Technology at mike.starrett@alwaysenpointe.com or 763-592-5579.

# Other Documents

Below is a list of documents referenced in these policies, which can be found on the ENPOINTE Intranet site (http://intranet.alwaysenpointe.com/) under Human Resources -> Policies, Procedures and Resources.

1. Asset Management Policy
2. Access Control Policy
3. Physical and Environmental Security Policy

# 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, Vice President of Technology, or Human Resources Manager.

## Retaliation

ENPOINTE prohibits taking negative action against any workforce members for reporting a possible deviation from this policy or for cooperating in an investigation. Any workforce member who retaliates against another workforce member for reporting a deviation from this policy or for cooperating in an investigation will be subject to disciplinary action.

## Acceptance Form

# ENPOINTE User Policies

**Protecting ENPOINTE and Client Assets**
**Policy Date: February 26, 2025**

I have read the attached policies carefully. I understand that these policies describe the basic responsibilities that ENPOINTE workforce members are required to observe for ENPOINTE. I understand that ENPOINTE believes that these policies strike a fair balance between their interests and workforce members' needs and expectations. These policies have been written to protect team members and ENPOINTE by being as clear and precise as possible. These policies are subject to periodic updates and continued employment at ENPOINTE requires compliance with any future revisions.

I understand that violation of the Company's rules of conduct is grounds for disciplinary action up to, and including, termination.

I understand that a copy of these policies is available on the ENPOINTE intranet and available via ENPOINTE Human Resources.

**I have received a copy of the ENPOINTE User Policies, I have read it, I understand it and I agree and consent to all of its terms, including the terms regarding monitoring and privacy.**

Signature: _____

Printed Name: _____

Date: _____