

Recovery Technology

Information Technology Plan and Report

2026

Information Services Department

Introduction: Recovery Technology is an Outpatient Behavioral Health Clinic in Jackson, Michigan. Recovery Technology's current strategic plan and business operational needs dictate that the Information Technology Department keep pace with the organization's current IT configuration and processes as well as detail a plan for the growth of IT capabilities to support the organization's strategic plan.

Information Technology Department Description and Policies: Recovery Technology's IT Department is under the direction and supervision of the agency's Chief Executive Officer. The department is comprised of one on-site full-time IT specialist. He is responsible for day-to-day operations, administration, application, and infrastructure support, and maintaining Recovery Technology's compliance HIPAA, CARF and all other standards. This Specialist is required to support the full scope of IT department functions from hands-on desktop support to systems administration and infrastructure support.

Information Confidentiality (Updated for 2026)

Recovery Technology maintains and protects all Electronic Protected Health Information (ePHI) and Proprietary Business Information (PBI) in accordance with HIPAA, HITECH, MDHHS requirements, and current security best practices. All systems, devices, and users accessing ePHI must comply with Recovery Technology's Zero Trust-aligned security controls.

Definitions

- **Electronic Protected Health Information (ePHI):** Any individually identifiable health information stored or transmitted electronically, including demographic data, treatment details, payment information, and any information that can be used to identify a client or employee.
- **Proprietary Business Information (PBI):** Company financial data, employee information, contracts, policies, and internal strategic materials requiring restricted access.

Security & Access Requirements

1. **Minimum Necessary Access:** Staff may only access ePHI required for their treatment, payment, or operations role.
2. **Multi-Factor Authentication (MFA):** All remote access, Microsoft 365/Entra ID logins, and privileged accounts require MFA.
3. **Encryption Standards:**
 - ePHI must be encrypted at rest and in transit (AES-256 / TLS 1.2+).
 - Mobile devices accessing ePHI must use full-disk encryption.
4. **Device Compliance:**
 - Only IT-managed, encrypted devices may store or transmit ePHI.

- Personal devices may not store ePHI unless specifically approved and enrolled in Intune device compliance.
- 5. **Prohibited Storage & Transmission:**
 - ePHI may not be stored on local PC hard drives, USB drives, personal cloud accounts, or unencrypted storage.
 - ePHI may not be emailed externally unless encrypted or transmitted through an approved secure platform.
- 6. **Audit Logging & Monitoring:**
 - All access to ePHI is logged, monitored, and retained.
 - Unauthorized access attempts trigger IT review.
- 7. **Annual Security Risk Assessment (SRA):**
 - Recovery Technology conducts a full HIPAA risk assessment annually with quarterly follow-ups.
- 8. **Data Transmission Rules:**
 - All ePHI transmitted electronically must use IT-approved secure applications (e.g., encrypted email, secure file transfer, Microsoft 365 protected sharing).
 - ePHI may not be transmitted via personal email, text messaging, or unapproved third-party apps.
- 9. **Incident Reporting:**
 - Any suspected privacy breach or unauthorized access must be reported immediately to IT and leadership.
 - Incidents are managed under HIPAA breach notification guidelines.

Failure to follow these confidentiality standards may result in loss of access privileges, disciplinary action, or termination.

Storage: Confidential electronic information that must be saved by staff is to be stored by all users with registered Microsoft 365 accounts in OneDrive. Documents and files are to be stored in a user's "My Documents" folder on Windows-based workstations, which is automatically re-directed to the Corporate OneDrive or by using the Recovery Technology OneDrive Shortcut. These folders may only be accessible from password-protected User accounts and a secure browser. Employees may not store confidential electronic information in their personal computers' local hard drives or non-encrypted local drives.

System Security: All access to electronic records maintained by Recovery Technology is restricted by the use of strong passwords. All use of company IT resources on the local area network (LAN) and Microsoft 365 OneDrive is secured by the use of strong passwords.

Company IT resources include but are not limited to: a) Company owned computers, smartphones, and all data and files stored on them, b) Company owned Removable Devices and hard drives and all data and files stored on them, c) Networked Public or private folders on the Company Servers and all data and files stored on them and/or Cloud

Drives (OneDrive, Google Drive, etc.), d) All email and contact information on the Company Exchange Server and/or transmitted across Company Network Infrastructure, f) All Internet usage via Company Network Infrastructure, g) All Instant Messaging transmitted across Company Network Infrastructure using MS Teams, Skype, etc.

All company-owned computers are Domain/Entra ID joined and are secured from unauthorized access in the following manner:

- A. Computers from which it is possible to access confidential client or business information are located within a secure location, with at least one locking door between the computer's location and the public areas of the facility.
- B. Computers from which it is possible to access confidential client or business information are configured with the requirement of a strong password upon startup of the PC and upon exiting the screen saver on a running PC.
- C. Remote access to Company IT Resources shall be granted only to registered Domain Users at the discretion of the Information Technology Staff or Leadership. All access will be protected by strong passwords and VPN Technology or MFA via browser by Microsoft 365/Entra ID.
- D. Windows-based workstations and servers are protected by Trend Micro Antivirus/Antimalware and/or Microsoft Defender Antivirus. Definition updates and regular scanning are centrally managed and performed regularly. Managed Microsoft Patching is also implemented, and updates/rollouts of critical patches and updates will occur regularly.
- E. Managed Content Filtration services are implemented, and we continue to monitor and specify anything we wish to block/report on using Microsoft Intune, Ubiquiti Unifi firewall and networking equipment.
- F. Managed Network Firewall is in place with 24/7 Monitoring with HIPAA/PCI Compliant cloud management service.
- G. In 2025 a Security Risk Assessment was completed (see attached), and Recovery Technology completed implementing the findings and recommendations from this report.

While Recovery Technology IT Department personnel seek to provide a reasonable level of privacy to users of company IT resources, all persons utilizing the system/accessing records on the system must be aware that all data or files created or stored on the Recovery Technology system are the intellectual property of Recovery Technology. The single exception to this standard is any electronic information concerning clients and their treatment, which is adjunct to their medical records and, therefore, the property of the

clients themselves. Electronic information concerning clients and their treatment belongs to the client. However, Recovery Technology maintains custody of this information and, therefore, the security standards included in this report.

Failure to adhere to the standards in this report, inappropriate use of company IT resources, and/or actions that place the security of Recovery Technology IT resources and/or electronic records at risk may result in a) Revocation of access privileges, b) Possible disciplinary action up to and including termination of employment.

Inappropriate use of company IT resources includes:

- A. Access and/or viewing of client records without a need to know for business, payment, or treatment purposes.
- B. Access and/or viewing for personal gain.
- C. Access and/or viewing for reasons that are counter to the best interests of Recovery Technology and/or its clients.

Upon separation of employment with Recovery Technology, the IT Department personnel must be notified immediately to ensure that the individual's access to IT resources is immediately disabled. The IT Department must be notified regardless of the reason for the employees' separation from Recovery Technology. If access to IT resources is not immediately disabled, access to IT resources by a former employee is unlawful and subject to legal action.

System Backup: All Recovery Technology servers are automatically backed up every weeknight. Backups include a) system volume information, b) system state data, c) application data, d) exchange mailboxes, e) the content of all user folders. Backups are stored at a secure data center. No user workstations are backed up.

Disaster Recovery: It is the responsibility of the Information Services Department to implement and maintain the following measures to protect against catastrophic loss of data: redundant backups in more than one location off-site using a mixture of technologies of Acronis local and cloud storage.

Use of Assistive Technology (Updated for 2026)

Recovery Technology is committed to ensuring that all clients, guests, and staff with disabilities have equal access to our services, technology, and electronic systems. Our approach to accessibility aligns with current ADA, Section 508, and WCAG 2.2 accessibility standards.

Assistive technology is provided to support individuals with physical, sensory, or cognitive limitations. Recovery Technology maintains, supports, and evaluates a range of accessibility tools, including:

1. Built-In Windows 11 Accessibility Features

- **Voice Access** for full voice-controlled operation of the workstation
- **Narrator** screen reader
- **Magnifier** and color/contrast filters
- **Live Captions** for audio and video content
- **Adaptive input tools** (on-screen keyboard, eye-control settings)

2. Microsoft 365 Accessibility Tools

- **Immersive Reader** for reading comprehension support
- **Dictation and speech-to-text** capabilities
- **Real-time captioning** in Microsoft Teams meetings
- **Accessibility Checker** integrated into Microsoft apps
- **Reading Mode** and simplified layouts for cognitive easing

3. Additional Supported Assistive Technologies

- Professional screen readers (e.g., **JAWS, NVDA**)
- Alternative input devices (adaptive keyboards, trackballs, switches)
- Cognitive support tools (focus mode applications, reading aids)

4. Telehealth Accessibility

- All telehealth platforms must support:
 - Captioning
 - Screen reader compatibility
 - Multiple communication modalities
 - Device-agnostic access (smartphones, tablets, laptops)

5. Ongoing Evaluation & Accommodation Process

- Recovery Technology reviews new assistive technology quarterly to assess compatibility with organizational systems.
- Staff and clients may request additional accommodations at any time.
- Training is provided for staff who require or support accessibility tools.

Recovery Technology will continue to invest in technology and training to ensure equitable access for all individuals who interact with our organization.

Summary of Current Technology and Spending: When the Information Services Department was started, Recovery Technology had a small handful of Desktop Computers. Currently, we have expanded to a mix of laptop computers, Chromebooks and smart phones for all clinical staff. These computers must be refreshed based on performance, hardware age, and warranty status to prevent the computers from falling into a state of disrepair, causing downtime for the staff and lost productivity and dollars. We are currently in a PC refresh cycle based on performance, hardware age, and warranty status.

Goals: As growth continues, we must focus our goals on several areas listed below that will be critical toward achieving and sustaining our Strategic Plan and growth.

Goal #1: Computer Hardware: Recovery Technology will continue to purchase Laptop Computers for clinical staff to access the Electronic Medical Record and Microsoft 365.

Priority Level: High priority/ongoing

Responsible Staff/Department: IT Administrator, CEO

Goal #2: Software and Licensing: As we acquire new computer hardware, we will ensure all devices include the most current version of Windows 11 Professional and are fully integrated with Recovery Technology's cloud-based services, with the ability to join our Active Directory domain and Microsoft Entra ID environment.

Priority Level: Medium/ongoing

Responsible Staff/Department: IT Administrator, CEO

Goal #3: Network Infrastructure: LAN with a high-speed internet connection, seven wireless access points, three primary network printers, and supporting equipment have been implemented and will be upgraded based on performance, hardware age, and warranty status to optimize network speed and access.

Priority Level: Low/ongoing

Responsible Staff/Department: IT Administrator/CEO

Goal #4: Disaster Recovery: Experience has revealed that the most common threat we face daily is the loss of our connectivity to the Internet. When we lose access to the Internet and to Electronic Medical Records, email, etc., this leaves us "dead in the water" and severely impacts our ability to function. This results in a very unfavorable situation for our staff and our clients. We will be investigating a bonding network appliance with packet

level load balancing, WAN aggregation and internet failover technology. We will continue to enhance wireless performance and reliability throughout the building, maintaining our existing segmented network structure, which includes the 'RT-Guest' network for visitors and the secure 'Recovery Technology' network for staff and organizational operations.

Priority Level: High/ongoing

Responsible staff/Department: IT/CEO

Electronic Medical Record Implementation: eHR Thomas, from Genius Solutions, was implemented in the first quarter of 2019. We continue to fine-tune our ability to use this system to its fullest capacity. We are continuously adding enhancement requests and preparing new forms to use. This is an ongoing project that requires quarterly review with the leadership team and feedback from the users. Our current Electronic Health Record system continues to meet our needs in 2026.

Lifeways CMH, whom Recovery Technology contracts with to provide an array of services, implemented "Lifeway's Electronic Organizer" or LEO. Currently, LEO is fully functioning. All documentation, authorization for services for CMH clients and billing are currently being completed in LEO.

Telehealth: To maximize productivity and provide superior service we were tasked with creating a mobile workforce and providing Telehealth services to our clients. Telehealth continues to assist us in the ability to expand our services and expand access for clients. Groups have continued to be conducted primarily via telehealth. We also use Doxy.me, Secure Video and Microsoft Teams services while leveraging our existing MS Teams enabled workstations and cellular phones which can run all the same software as our laptops/workstations. All of our telehealth solutions meet the requirements for HIPAA privacy and MDHHS standards. We will continue to get feedback from clients and staff to improve the hardware, software, and processes to provide