TECHNOLGY PLAN

2023-2026

Information Technology Policy and Procedures

Technology Overview:

**POLICY:** It is the policy of Equitable Solutions to inform and train all users regarding the acceptable use of technology equipment, information, responsibilities, and security. Initial and ongoing related training and competencies will be documented. The main objectives for acceptable use ensure:

1. The **confidentiality and security** of data and information are protected against unauthorized misuse or disclosure (or that prompt reporting occurs).
2. The **integrity** of data and information to protect from unauthorized or accidental modification.
3. The **availability and accessibility** of technology balanced against the need for use.

**INTENT:** The use of technology is meant to enhance services for persons served, personnel, and other stakeholders so that we can implement our mission.

**GENERAL INFORMATION:** The following information is to be used as an outline of what is expected regarding information technology (IT). It defines terms, identifies standards, and supports IT implementation. The policies and procedures for IT use will address the following topics:

1. **Acceptable Use of Technology and/or Equipment** which may include business computers, tablets, cell phones, USB drives, email, and internet, Wi-Fi, network access, Information and Communication Technology (ICT) for service delivery, or use of other applications.
   1. The acceptable use of all technology is implemented to support business processes, therapeutic service deliver, and **information systems** including how information is collected, processed, stored, and communicated.
   2. Guidelines for using the internet, Wi-Fi, and/or the network as well as other resources are specified regarding business computers, laptops, phones, tablets, and/or personal devices.
   3. The control and use of technology including bringing or using **personal devices** on the business network or for business purposes will also be addressed.
   4. See separate policy and procedures for, *Remote Service Delivery Using Information & Communication Technologies*
2. **Backup and Recovery Practices** refers to backing up data and the setting up of systems that allow data recovery. Additionally, the type of back up method used (on-site or off-site device or system) will be identified and evaluated. Regular monitoring and testing of the backup processes will be performed to verify they function as expected. Data retention timeframes, copies of data, as well as distribution of data will be addressed in backup and recovery planning.
   1. This policy and procedure will set rules and regulations for the backup and secure storage of all critical data and electronic information in the case of system damage/failure or other events such as natural disasters, data corruption, faulty data entry, espionage, or operation errors.
   2. It will also address technology utilized for areas like payroll, billing, scheduling, electronic health/medical records, financial collection methods, as well as other portable devices that may be used for data transfer.
3. **Business Continuity and Disaster Recovery** is used to help the business recover from a disaster, accident, or emergency, and continue operations.
   1. **Business continuity** will address the availability of essential business functions and may include replacing personnel, service availability issues, [business impact analysis](https://www.fema.gov/media-library-data/1388776348838-b548b013b1cfc61fa92fc4332b615e05/Business_ImpactAnalysis_Worksheet_2014.pdf) otherwise known as a BIA.
   2. **Disaster recovery** processes may include server and network repair, replicating backup data, and supplying backup systems.
4. **Security** awareness seeks to educate users about the consequences of their actions regarding security and privacy. The policy and procedures for security address:
   1. **Access management** refers to initial access to IT systems, information access, user ID’/Passwords as well as the password policy.
   2. **Audit capability** refers to the record or audit log showing who has accessed a computer system and what operations have been performed during a given time frame.
   3. **Data export or transfer capabilities** will address what data is proprietary and secure as well as how or if data may be exported or transferred back and forth from business to personal device and from personal to business device.
   4. **Decommissioned hardware and data destruction** refer to the removal of active hardware to inactive status and how the hardware will be disposed of without risking access to the data that was stored on it.
   5. **Malicious activity protection** includes security features such as firewalls, spam filtering, and other systems designed to prevent abuse or unauthorized use.
   6. **Remote access** will define our standards for connecting the business network to any internal and/or external host (i.e., someone off site, a telecommuter, and/or someone traveling). These standards are created to identify what equipment can be used to perform company business and what kind of access is allowed.
   7. **Configuration management/updates** follow the hardware, software, or other related technology to track versions and updates installed on computer systems and network addresses belonging to hardware devices used.
   8. **Change control** is meant to ensure that all changes made are managed, verified, approved, and tracked i.e., new technology, software updates, operating system updates, and firmware updates. Testing and analyzing these areas will help the business to understand the impact of the changes and ensure a smooth and orderly transition.

**SCOPE:** The policies and procedures apply to all business systems and those working at or for our organization including personnel, contractors or sub-contractors, or services purchased or contracted. Additionally, all vendors must meet the security and privacy rules to be utilized.

**ORIENTATION:** All new staff and other stakeholders, as appropriate, will be provided an Orientation or Onboarding Session regarding the various IT systems and practices.

1. New staff must read and acknowledge the “Acceptable Use of Information Technology” located within their staff handbook or policy and procedure manual.
2. Staff must confirm they have read and agree by signing and dating the appropriate document.
3. All training and competencies will be documented and filed in their personnel file or stored in our cloud-based system.
4. Various introductory activities include:

* Being assigned Log On information and gaining access to the Internet, Network, as well as our (Wi-Fi).
* Using their Network Username and Password to log into their workstation equipment.
* Microsoft Outlook/Web Mail and the Cloud System.
* Printing, Faxing, Calls, or mobile device.
* Accessing various websites, software, and hardware specific to their position.
* Technology Security such as Ransomware, Cybersecurity, and other current technology practices.
* The Physical Environment regarding IT safety and security practices.
* As applicable to the staff position, utilization of ICT in service delivery.

**INFORMATION COLLECTION:** Maintaining the security and integrity of collected information is crucial to our business viability. Administrative and clinical information is collected in a legal, ethical, and uniform manner per the guidelines and timeframes identified in relevant policies and procedures (refer to individual policies guiding each of these functions). Information is reviewed and analyzed for use in our strategic planning, various decision-making events, and quality improvement, Information is collected in accordance with our mission, vision, values, and program goals. Overall, the data collected is meant to:

1. Enhance quality clinical care and identify unmet needs.
2. Improve efficient business functions (health and safety, workforce management, strategic planning, risk management, performance improvement, etc.).
3. Increase productivity and foster effective communication among all stakeholders.

**TECHNOLOGY DEMONSTRATION:** The use of information technology services will be demonstrated in the following ways:

1. **The Website:** Stakeholders can become familiar with services, staff, beliefs, common misconceptions, scheduling, payments, job openings, surveys to determine quality of services or corporate compliancy, appointment requests, and online assessments with resources for accessing special accommodation requests, if needed.
2. **Hardware and Software:** The telephone systems, training software, intrapersonal file sharing, email, business accounting software, file management, billing software, electronic health record, payroll services, ICT delivery of services, online assessments, insurance, fee collection systems, and other technology services required by contracts or based on need.
3. **PR Material:** Newsletters, social media, and other electronic media will be used for marketing.

**INFORMATION DISSEMINATION:** Technology information will be disseminated to staff, persons served, and other stakeholders as appropriate and in accordance with individual policies. The above types of demonstration will be performed based on the type of input, outcome, and audience.

**TELEHEALTH SERVICES:** We do **not** provide any [telehealth services](https://www.integration.samhsa.gov/operations-administration/telebehavioral-health) and therefore do not use any telehealth platforms. If, at some point we provide this service, the appropriate policies and procedures will be implemented. (Note: If you have added telehealth through ICT service delivery, see *Accreditation No*w! Group Two, General Program Standards, the section addressing *Service Delivery Using Information & Communication Technology.*

**RESPONSIBILITY:** The CEO is responsible for coordinating the security and privacy of protected health information, the assessment and planning of technology needs, as well as ensuring appropriate training.

*Acceptable Use of Technology*

**GENERAL USE AND OWNERSHIP:** Proprietary information stored on electronic and computing devices whether owned or leased, remains the sole property of the business. Personnel must ensure through legal or technical means that proprietary information is protected in accordance with the data protection standard.

# HARDWARE:

# POLICY: Personnel are responsible for the technology resources entrusted to them. Due diligence and care should be exercised to ensure the security and integrity of these business resources including, but not limited to computers, monitors, modems, hard drives, keyboards, cell phones, mobile devices, tablets, mice, printers, and scanners.

**PROCEDURE:** Reasonable and prudent steps should be taken to protect agency-provided technology equipment or resources. At no time should safety toward hardware be compromised or circumvented.

1. Agency-provided hardware and other information systems should only be used as authorized by executive management.
2. Requesting, purchasing, or obtaining hardware must be approved by the appropriate staff member and follow the purchasing policy.
3. Use of agency-provided technology should conform to an individual’s job function and/or specific job description.
4. Any action which breaches, evades, or circumvents reasonable and prudent methods of hardware use; should be immediately reported to the appropriate management.
5. Failure to report these actions is a violation of policy and subject to disciplinary action.

**COMPUTERS:** Company owned computers are for business use only. The use of personal electronic devices i.e., smart phone, tablet, desktop computers, or laptops is **prohibited** for business use, unless authorized by the Executive Team or designee.

1. Security verification will be performed on the device to ensure the security of the device.
2. All computers must be password protected and only those persons who are authorized can use or have access to approved devices.
3. Each person authorized is assigned a security code or password and must sign a confidentiality statement. Security codes or passwords shall be changed periodically, and information must be backed up regularly.
4. If you are using a personally owned device for company, use, the device must have appropriate security software installed and meet minimum requirements for maintaining security. This verification will have to be performed by management and documented.

*.*

**PORTABLE DEVICES:** The purchase of portable devices such as cell phones, tablets, and laptop computers must meet the guidelines for purchasing equipment under the financial policy.

1. Portable systems must run a Windows and integrate with existing hardware.
2. The minimum capacity of the portable system must be:
   1. 3.50 to 4.2 speed of device.
   2. 16GB RAM size.
   3. 2 USB ports

3. The portable system must be able to run the following applications/software:

1. Internet Browser: Google Chrome, Firefox, Safari/iOS.
2. Most current version of Microsoft and Office 365.
3. Cloud Storage such as Professional Dropbox.
4. Security: Anti-Malware such as McAfee or Malwarebytes.
5. Adobe Acrobat, JAVA, Brother Printing/Scanning or other equipment .
6. If applicable, QuickBooks or billing collections software such as PayPal; Electronic Medical Records; and other publishing applications (Canva, MailChimp, Constant Contact).

**EXTERNAL DEVICES:** This may include modem, routers, monitors, keyboards, mice, printers, scanners, fax machines, projectors, phones, shredder, mailing equipment, and other security devices.

1. Purchase and use of all other computer peripherals can only be authorized by appropriate staff.
2. External devices must be compatible with the company’s current hardware and software systems.
3. Mobile device(s) must be purchased through the business account The request for accessories (hands free kit, additional scanner, label maker/printer, etc.) must be included with initial request for purchase.
4. All purchases of devices must be supported by 1–2-year manufacturer warranty or other guarantee.

**BRING YOUR OWN DEVICE:** This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets, for business purposes. All staff who use or access our business technology equipment and/or services are bound by the conditions of this policy.

1. Staff must register their device for business use and report what applications that are being used for business purposes on personal devices.
2. Staff will register their devices when completing their onboarding and/or orientation to the Technology Standards. The following can be used for business purposes:
   1. Approved device for the use for email access using appropriate security measures.
   2. Approved device for the use of business internet access using appropriate security measures.
   3. Approved device for the use of business telephone calls (VOIP) using appropriate security measures.
   4. Approved use of the Electronic Medical Record using the appropriate security measures.
3. All staff who have registered personal devices for business use acknowledge that the business:
   1. Owns all intellectual property created on the device.
   2. Can access all data held on the device.
   3. Will regularly backup the data held on the device.
   4. Will delete all data held on the device in the event of loss or theft.
   5. Has the first right to buy the device if the staff member wants to sell.
   6. Will delete all data held on the device upon termination of the staff member.
   7. Has the right to deregister the device for business use at any time.
4. Each staff member that utilizes personal devices agrees:
   1. Not to download or transfer business or sensitive information to the device. Sensitive information includes business or personal information sensitive to the business such as intellectual property, personnel details, client information, etc.
   2. To maintain the device with current operative and security software.
   3. Not to share the device with other individuals to protect the business data access through the device.
   4. To abide by the internet policy for appropriate use and access of the internet.
   5. To notify the business immediately in the event of loss or theft of the registered device.
   6. Not to connect USB memory sticks from an untrusted or unknown source to equipment.
5. To keep devices secure, the following must be observed:
   1. Devices must never be left unattended in a public place, or in an unlocked home, vehicle, or even if it locked. Wherever possible, staff should keep device on their person or securely locked away.
   2. Devices should be carried on as hand luggage when traveling.
   3. Passwords and encryption should always be utilized for device access.

**SOFTWARE:**

**POLICY:** Staff may be required to use a company owned computer to complete the responsibilities of their position. The CEO is the only person authorized to approve software use, changes, or purchases.

**INTENT:** Ensure that all software used is appropriate, has suitable value regarding cost vs. need, and integrates with other used technology.

**OVERVIEW:** There are typically three classifications of software. This includes Systems Software which aids the user and the hardware to function and interact with each other, Programming Software, as well as Application Software.Unauthorized software applications may be removed as all software needs to be approved and evaluated on an individual basis and implemented using the appropriate configuration procedure.

**APPROVED SOFTWARE:** The following is a list of software programs that are authorized to be on Business Computers**:**

* Operating Systems like MS Windows, Macintosh Operating System, iOS, or Android.
* Device Drivers such as Printer Drivers, USB Drivers, Display Drivers, VGA Drivers, Keyboard/Mouse Drivers, or other Virtual Devices.
* Licensed Microsoft Office Suite, OpenOffice.org or Outlook.
* Java and Adobe Acrobat Reader.
* Internet Web Browsers like Microsoft Edge, Internet Explorer, Mozilla Firefox, Safari, or Chrome.
* Anti-Virus, Malware Software, or Firewall Protection like McAfee, AVG, Microsoft Security Essentials, or Windows Firewall.
* Data Backup Systems such as SOS Online Backup or SpiderOak One.
* Bookkeeping systems such as Quick Books, PayPal, Ivy Pay, or Bench.
* Practice Management and Electronic Health Records like Simple Practice, DaVinci Milan, CounSol, Therapy Partner, Therasoft, Theranest, or Therapy Notes.
* Internet Phone/VOIP Operating Systems like Ring Central, iPlum, RingRx, or Spruce.
* Secure Email Systems like Hushmail for Healthcare, G-Suites, Microsoft 365, GoDaddy, or Paubox Encrypted Email.
* Telehealth Video Conferencing Systems like Zoom, Simple Practice, Thera-link, CounSol, Spruce, or Doxy.Me
* Cloud Systems such as G-Suites or Dropbox Professional.
* Document Collaboration such as Dropbox Professional, Theranest, RingCentral, Microsoft 365 Teams, G-Suites.
* Form Development and Electronic Signature Software such as LuxSci SecureForm, IntakeQ, or Cognito Forms.
* Note Taking Software or Note taking Devices with Apps such as Notability or Livescribe Smart Pen by Anoto.
* E-Prescribing Software such as WRS Health.
* Visitor Check in Software such as Medical Check-In or the Receptionist.
* Tech Assisted Supervision Tools such as Dreamaker.io.

**PROCEDURE:** Reasonable and prudent steps should be taken to protect agency-provided technology equipment and resources. At no time should safety toward software be compromised or circumvented. Software procedures are outlined below:

1. Agency-provided software and other information systems should only be used as authorized by executive management.
2. Requesting, purchasing, or obtaining software must be approved by the appropriate staff member and follow the purchasing policy prior to the use or download of such software.
3. All software that is purchased must be sold by reputable software sellers and meet relevant security rules so that configuration can be implemented smoothly.
4. All purchased software must be supported and compatible with the operating system identified below.
5. Any changes from the requirements must be authorized by the Executive Team or designee.
6. Use of agency-provided technology should conform to an individual’s job function and/or description.
7. Any action which breaches, evades, or circumvents reasonable and prudent methods of software use; should be immediately reported to the management.
8. Failure to report these actions is a violation of policy and subject to disciplinary action.

**SOFTWARE USAGE:** All personnel must receive training relevant to their job description and use prior to the use of any software. This will be the responsibility of the appropriate management team member. Staff is prohibited from bringing software from home and loading it onto company hardware.

1. Unless express approval is obtained from the CEO*,* software cannot be taken home and loaded on personal devices.
2. When a staff member is authorized to take home a company device, the use of all software or hardware must be business related unless previously approved.
3. Illegal use, reproduction, or duplication is strictly forbidden and may be subject to civil and criminal penalties including fines and imprisonment.

**SOFTWARE AUDIT:**  There will be periodic audits of all company owned PC’s, including laptops to insure we follow software licenses. Audits will be conducted using McAfee software*:*

1. Software for which there is no supporting registration, license, and/or original installation will be removed from the user’s computer.
2. A search for viruses and any other unknown software will also be implemented.
3. Full cooperation of all users is required.
4. The company reserves the right to audit networks and systems on a periodic basis to ensure compliance with acceptable use policy.

**BROWSER AND OPERATING SYSTEM (OS) BEST PRACTICES:**  To guarantee the best experience, get the most out of our electronic systems, and ensure security and performance, the following best practices are to be applied:

1. Keep your OS and browser updated.
2. Enable JavaScript and cookies.
3. Utilize AdBlock and other security protections.
4. Disable Autofill.
5. Remove browser extensions.

**OPERATING SYSTEM OVERVIEW:** The Operating System (OS) has 3 basic functions: (1) managing the computer’s resources like the central processing unit, memory, disk drives, and printers, (2) establishing a user interface, and (3) executing and providing services for software applications. To keep the browser working smoothly, it is best to make sure the OS is up to date and current with business standards. System updates can fix performance issues for the browser, internet connection, and other key features. To update the OS, use the following links:

1. [Operating System-Mac OS](https://support.apple.com/en-us/HT201541)
2. [Operating System-Windows](https://support.microsoft.com/en-us/help/4027667/windows-10-update)

**BROWSER:** Your browser is the program used to navigate the World Wide Web. Each browser update comes with improvements, installs new features, and fixes performance issues that keep your browser running smoothly, safely, and error-free. The minimum requirements for successfully using our software technology include:

1. A reliable internet connection with a bandwidth of at least 10 mbps which will minimize connection issues and provide the best quality interactions.
2. Newer devices purchased in the last 3-5 years.
3. A computer that has at least 2.5 GHz processor and 4 GB or more of RAM.
4. For Apple Computers the [latest version](https://www.apple.com/macos/catalina/) is recommended.
5. For Windows Computers [Windows 10](https://www.microsoft.com/en-us/windows/get-windows-10), 8, or 7.
6. Web Browsers such as [Google Chrome](https://www.google.com/chrome/) version 71, [Mozilla Firefox](https://www.mozilla.org/en-US/firefox/new/) version 64, and [Apple Safari](https://support.apple.com/en-us/HT204416) version 12.
7. For Mobile devices (iOS or Android) use at least iOS 12 or newer.

**INTERNET:** The following guidelines are for accessing and utilizing the internet through the company’s network. Internet services are authorized to staff based on their job description and to enhance services provided. The internet is a great tool but comes with security implications we must guard against. For that reason, staff are granted access only as a means of providing support when fulfilling their job responsibilities.

1. Internet accounts are approved for designated staff members by their supervising manager.
2. Each person is responsible for the account issued to them as well as ensuring the security of their issued accounts.
3. Sharing of one’s User Id or Password is prohibited.
4. Use of the internet must reflect the business mission and support company goals and objectives for providing services.
5. No staff member may use the business’ internet to deliberately propagate any virus, worm, trojan horse, or other malicious malware.
6. The following constitutes inappropriate use of the internet and is not permitted:
   1. Accessing, uploading, downloading or distributing pornographic or sexually explicit material
   2. Violating state, local, or federal laws.
   3. Vandalizing or damaging the property of any other individual or of the company.
   4. Invading or abusing the privacy or rights of others.
   5. Violating copyright or using intellectual property without permission.
   6. Using the network for financial or commercial gain.
   7. Degrading or disrupting the network performance.

**EMAIL:** The use of email must be consistent with Company policies and procedures for ethical conduct, safety, and in compliance with applicable laws and proper business practices. The Company email account should be used primarily for business related purposes. Personal communication is permitted on a limited basis, but non-related commercial uses are prohibited.

1. All data contained within an email message or attachment must follow the secure data transfer protection standards.
2. Personnel must use extreme caution when opening email attachments received from unknown senders, which may cause malware.
3. Email messages should be retained if they qualify as a business record. Email messages are considered a business record if there is a legitimate and ongoing reason to preserve the information contained in the message.
4. The email system shall not be used for the creation or distribution of any unacceptable usage including disruptive messages, offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practices, political beliefs, or nation origin. Personnel who receive any emails with this content form other staff members should report the matter to their supervisor immediately and utilize the grievance reporting system, if warranted.
5. Users are prohibited from automatically forwarding business email to personal accounts or 3rd party email systems. Individual messages which are forwarded by the user must not contain any confidential or private information.
6. Personnel is prohibited from using 3rd party email systems and storage servers such as Google, Yahoo, and MSN Hotmail, etc. to conduct business, to create transactions, or to store/retain information.
7. Personnel shall have no expectation of privacy in anything they store, send, or receive on the company’s email system.
8. Email accounts and messages may be monitored without prior notice or warning.

**BACKUP PRACTICES:**

**POLICY:** All business-critical data will be backed up daily using One Stop Back Up Solutions to protect and ensure data integrity. An offsite data storage facility, backup hard drives, and other cloud-based systems will be utilized to ensure business continuity.

**INTENT:** Ensure continuity of services through regular backup of all technology and data. This provides the assurance that the use of systems will be available and ensures the safe and effective storage of critical information. Additionally, our intent is to minimize risk by implementing a set of processes to recover from a disaster and continue or resume business.

**PROCEDURE:**  The organization is responsible for the backup of data held in **central systems** and related databases. The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the organization falls entirely on the user.In the event of a disaster, daily backups would restore all applications and information. Once the restore is complete, full access will be available.

The procedures below are used to ensure backups between servers occurs so that if one server becomes unavailable, access is available through another avenue or separate location until a full restoration is complete.

1. The staff/contractor/vendors shall have backup servers that will back up nightly with recovery software that is built into the approved operating system or programs.
2. Network data and programs are backed up daily and archived off site in the case of emergency, this is to minimize risk in the following disasters:
   1. Critical computer systems.
   2. User vulnerability and/or user area vulnerability.
   3. Loss of building, loss of key staff, loss of IT Network, loss of power.
   4. Weather related incident.
   5. Security issue.
   6. Software or Hardware failure.
   7. Virus or other Security breach.
   8. Website Disruption.
3. Data and software on your PC may not be backed up. If you want to protect data and files used on your PC, the following measures should be taken:
   1. Save the data onto the Cloud System-Dropbox, EMR, or relevant program.
   2. Copy the data to the appropriate network server and store it within your personal file folder specifically set up for this purpose. This will ensure the important data is saved and archived in the daily backup process.
4. Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or re-purposed, data must be certified or deleted, or disks destroyed consistent with industry best practices for the security level of the date.
5. To validate the backup can be created completed within a timely basis, a test database is verified using the daily backups.
6. Some backups may be stored using backup hard drives which will follow security storage rules and guidelines.
7. Ongoing assessment of Technology will be performed, and planning will occur annually. It will be updated as needed.

**BUSINESS CONTINUITY AND DISASTER RECOVERY:**

**POLICY:** The company is committed to ensuring that regular business services can be maintained in the event of a disaster (ranging from weather-related to catastrophic) using key technologies and disaster preparedness measures.

**INTENT:** Ensure we are better prepared in the event of a disaster by having basic technology services available or by utilizing a plan to support resuming business.

**PROCEDURE:** Since we utilize virtual services in a variety of ways, disaster preparedness methods will be maintained using key IT services employed through the following methods:

1. **Phone Systems**: In the event of a disaster rendering the phone systems unusable, cell phones will become the primary method of contact for key office personnel. A list of cell phone numbers and home phone numbers is maintained and updated regularly. Office calls will be forwarded to the appropriate person’s phone to manage business calls.
2. **Internet Servers/Networks:** Alternative secure internet access could be established if the office server or network is down. A secure “Hotspot” could be implemented in the event of an office disaster. This will be used for essential services only, until the network is restored.
3. **Data Storage:** All data is backed up daily utilizing our secure cloud-based system and will be virtually restored when necessary.
4. **Remote Connectivity**: If a disaster has prevented work from the administrative office another device and/or location will serve as a backup for connectivity.
5. **Equipment/Computers**: Additional laptops could be made available for personnel to work remotely from home following remote device guidelines. Necessary equipment would be transported overnight, configured and replaced.
6. **Security and privacy management:** All policies and procedures for security and privacy management are to be followed. If it is a security breach that has caused the disaster, appropriate risk measures (for reporting) will be taken according to the breach.
7. **Business Continuity Plan:** The disaster recovery plan will be developed in conjunction with a [Business Continuity Plan](https://www.ready.gov/business-continuity-plan).

**SECURITY:**

**POLICY:** Reasonable and prudent steps should be taken to protect business data and information systems. At no time should these steps be breached, evaded, bypassed, or circumvented. Any action which breaches, evades, or circumvents these reasonable and prudent steps should be immediately reported to management. Failure to report these actions is a violation of policy and subject to disciplinary action.

**INTENT:** Every staff member or service contractor employed is responsible for the business resources entrusted to them. Due diligence and care should be exercised to ensure the security and integrity of all resources including safeguarding and protection of data and other IT systems.

**PROCEDURE:** Data and information systems should only be accessed according to one’s respective job function and description. Approval and use must be authorized by Executive Staff and/or designated person. Threat prevention must be utilized to protect against negligent and/or intentional damage. Business continuity and recovery from this damage is imperative if the business is to operate without interruption.

1. **Security Overview:** Please see the [McAfee Fact Sheet](https://www.mcafee.com/enterprise/en-us/assets/fact-sheets/fs-mcafee-fact-sheet.pdf) for a full description of the security features.
2. **Access Management:** Access to the network, servers, and other systems will require individual unique logins for authorization to the system. Authentication includes the use of passwords to gain access to the system.
   1. **Passwords:** System level and user level passwords must comply with the password policy outlined below. Providing access to another individual, either deliberately or through failure to secure access, is prohibited. All computing devices must be secured with a password protected screensaver with the automatic activation feature set to 10 minutes or less. Personnel must lock the screen or log off when the device is unattended.

* Passwords must consist of a minimum of eight (8) characters and must contain three of the four following attributes – upper-case letter, lower-case letter, number or symbol.
* Passwords are required to be changed every 75 days and not to be shared with anyone.
* New passwords must be significantly different than the previous five used passwords.
* When a staff member forgets their password or is locked out after 3 unsuccessful attempts, then the appropriate staff member will be authorized to reissue a new initial password that will be required to be changed upon successful log in.
  1. **Physical Access:** For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through keypad lock. All devices must be securely locked in offices with appropriate password protection and/or encryption measures in place.
  2. **Encryption:** Policies, procedures, scenarios and processes shall identify confidential information or PHI that must be encrypted to protect against persons or programs that have not been granted access. Apple offers built-in encryption for both mobile iOS and the desktop OS X systems, Microsoft Windows offers BitLocker, and Android also supports encryption out of the box.
  3. **Technology Access:** Authorization of technology use will be performed upon new hire orientation/onboarding and completion of technology training relevant to one’s job role. Deactivation or de-authorization will be implemented upon termination, security issue, or other policy breach.

1. **Audit Capabilities:** Audits will be performed of servers, firewalls, websites, log history, and other technology on a regular basis using McAfee Endpoint Security tasks. These reviews will include monitoring access logs, results of intrusion detection software, and web security. Vulnerability and risk assessment will be virtually conducted on a weekly or monthly basis depending on the type of audit and the results of the report. The program used for this is [McAfee and there are multiple free tools that can be used](https://www.mcafee.com/enterprise/en-us/downloads/free-tools.html) including anti-malware tools and encryption tools. Relevant reports will be utilized for resource planning.
   1. All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain enough audit-logging information to answer the following questions:

* What activity was performed?
* Who or what performed the activity, including the system the activity was

performed from?

* What the activity was performed on (object)?
* When was the activity performed?
* What tool(s) was the activity performed with?
* What was the status (such as success vs. failure), outcome or result of the

activity?

* 1. If Log Results yield suspicious or malicious activity or any of the detection prevention systems are implemented automatically using predetermined McAfee Safeguards, relevant reports will be immediately reported to management so that appropriate actions are taken.
  2. Any staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.
  3. Audit Logs will be stored in the McAfee Dashboard and relevant reports will be shared as appropriate.

1. **Data Export and Transfer Capabilities:** The company must protect restricted, confidential, or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our stakeholders. The protection of data is critical, yet flexibility to access data to work effectively is also critical. The primary objective is user awareness in order to avoid accidental loss scenarios, data leakage, or malicious threats.
   1. Data may be exported or transferred in the following cases:
      * Email exchange
      * Video conferencing
      * Billing, Payroll, or other Financial transactions
      * Fax, Phone Call, or other communication methods
      * Record sharing
   2. Data is defined as:
      * Credit card details, bank account numbers, and other financial identifiers
      * Email addresses, names, addresses, and other combinations of personally identifiable information
      * Documents that have explicitly marked with “Confidential” information
      * HIPAA information including all elements of the medical record
2. **Data Transfer Capabilities:** *.*
3. **Decommissioning of Physical Hardware and Data Destruction:** Technology equipment often contains elements which cannot be thrown away. Therefore, proper disposal of equipment is both environmentally responsible and usually required by law. In addition to hard drives, USB drives, CD-ROMs, and other storage media that may contain carious types of IT data, some of this data is sensitive. To protect our stakeholder’s data, all storage mediums must be properly erased before being disposed of. Deleting or formatting data is insufficient because it can still be accessible until it is overwritten by a new file. Consequently, special tools shall be used to securely erase data prior to equipment decommissioning or destruction. Best practices for data destruction include:
   1. **Creating and Utilizing a Metadata Standard:** Metadata summarizes basic information about data which can make finding and working with specific data easier. For example, a clinical metadata standard may include a unique identifier that identifies the file type, the start of services, the type of services, the conclusion of services, as well as the legal destruction date
   2. **Establishing and Maintaining a Records Retention Schedule:** The retention of health care records must follow [HIPAA policies and procedures and documentation requirements](https://www.law.cornell.edu/cfr/text/45/164.316) which states that information must be **retained** for a minimum of 6 years from when the document was created or the date when it was in effect, whichever is later. **Utilize Appropriate Processes:** Establish the destruction process to address physical and electronic records that complies with relevant information management policies.
   3. **Manage Vendors:** Ensure appropriate documentation is in place by Completing the *Destruction and Release Log Form* as well as ensuring a *Certificate of Destruction* has been received to verify compliance with relevant state and Federal rules, guidelines, and/or laws.
   4. **Monitor, Adjust, and Analyze**: Implement quality performance measures to ensure the destruction process meets the current needs of the business.
4. **Malicious Activity Protection:** McAfee is the tool used for Virus Protection, Endpoint Security, Cloud Security, and as a Common DLP Engine. This is employed to ensure the integrity of all operating systems including Windows, macOS, Android, and iOS so that we can defend ourselves against viruses, malware, spyware, and ransomware attacks while staying on top of privacy and security.
   1. **Security Protection:** McAfee protects against security threats by utilizing anti-virus protection, protecting and shredding sensitive files, deleting cookies, safe web browsing, performance optimization, multi-device compatibility, encrypted storage, and more.
   2. **HIPAA rules** continue to apply with the use of personal computers including password protection as well as the use of anti-virus and firewall protection. Tablets, smartphones, or other mobile devices shall have Malware installed. All electronic devices must have up to date operating systems.
5. **Remote Access:** These policies are meant to provide guidelines for appropriate use of remote access capabilities to the company’s network, business applications, and technology systems. This policy applies to all staff, contractors, vendors, and other agents with a company owned or personally owned device used to connect to the company network. Activities include reading or sending email, viewing intranet web resources, utilizing the electronic medical record, or any other applications used for business. The same type of security measures must be implemented for remote access.
6. **Configuration Management:**
7. **Training:** Data security and client confidentiality procedures are an indispensable and integral part of the system policies and procedures therefore, training will occur for new staff, upon the use of new technology, and as needed or warranted. This will be performed by appropriate staff and with HIPAA compliance in place.
   1. *Accreditation Now, Inc*. Technology Training
   2. HHS Technology Training
   3. Other listed.

**HIPAA, PRIVACY, AND CONFIDENTIALITY:**

**POLICY:** The business information systems, data, and technology assets, which include but are not limited to computers, computer networks, printers, and other related pieces of equipment and/or systems, are the property of the agency and are valuable company assets.

**INTENT:** Individuals using and having access to this technology must take reasonable and prudent steps to preserve the integrity of the systems, the data, and to protect the information. These assets are to be used for appropriate business-related functions only.

**GENERAL INFORMATION:** All communications made and transmitted within the agency shall be professional in nature as they represent the agency, our culture, and the individuals we serve. Prior to the use of the agency data and telecommunication systems, the staff member or company/individual hired by the agency is required to read the information policies and sign an acknowledgment statement.

Information and technology assets include but are not limited to the hardware, software, equipment that makes up workstations, local area networks, wide area networks, telephone, and other communication systems. All changes, modifications, and alterations to computing assets must be made and/or approved by the Executive Team.

**PROCEDURE:** Confidentiality of all treatment information and records shall be kept, recorded, released, maintained, and provided to requesting parties, in accordance with all applicable state and federal laws.

1. The “Minimum Necessary” rule is required of all personnel to ensure only the minimum protected health information necessary to carry out treatment, payment, and healthcare operations are released via any technological system. Refer to the policies concerning Confidentiality for additional information.
2. Reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure will be maintained by the following safeguards:
3. Shredding documents containing PHI before discarding them.
4. Securing clinical records with lock and key or pass code.
5. Limiting access to keys or pass codes.
6. Passwords are established through the Management Team.
7. Sharing of passwords between staff members is forbidden.
8. New or change of current password is available upon request.
9. Personnel must set up their workstations to automatically log off after a predetermined time of inactivity, i.e., a screensaver with a password.
10. Individually identifiable information shall not be transmitted via email.
11. A “Security Officer” will be designated by the agency director and will function as the security officer for safeguarding the records and billing data.
12. A “Privacy Officer” will be designated by the agency director to ensure compliance with all HIPAA requirements.

**PHI STORAGE:** The storage of any protected health information (PHI) is prohibited on any personal electronic device i.e., smart phone, tablet, laptop, flash drives or any other device capable of storing electronic information. The company may issue encrypted flash drives for use or data can be saved in approved software-based cloud systems or other medical record systems.

# ASSISTIVE TECHNOLOGY

**POLICY:** The agency will attempt to provide appropriate assistive technology to staff and persons served with disabilities. We are committed to training staff on how to most effectively use assistive technology to improve quality services. Training is accomplished via in-person, one-on-one, group presentations, or on your own through work or home study.

**INTENT:** Multiple methods of assistance for staff, clients, and other stakeholders will be available upon reasonable request, ability to meet request, and options available. Cost will be a factor upon ability to meet need.

**GENERAL INFORMATION:** Assistive technology is defined as any item, piece of equipment, or product, whether acquired commercially, off the shelf, modified, or customized, that is used to increase, maintain, or improve the functional capabilities of individuals with disabilities.

**PROCEDURE:** The need for assistive technology must be determined on a case-by-case basis. Reasonable Accommodation Requests are to be made to the next level of management. The Executive Team or designated staff member has deciding vote on request. If it is determined that assistive technology item is required for personnel to be provided a reasonable opportunity to perform the responsibilities of job or to meet the needs of persons served, the technology will be provided.

Examples of assistive technology include:

* Customized office furniture or supplies.
* Specialized keyboard (ergonomic or large key).
* Voice recognition software.
* Large monitors.
* Video phones.
* Screen magnifiers.
* Optical character recognition (OCR) scanning software.

Additionally, other safety accommodations such as wide hallways/walkways, wheelchair ramps and strobe/vibrating alarm systems are common to all offices.

**RIGHTS RESERVED BY THE BUSINESS:** Violation of policy or misuse of business assets is subject to disciplinary action up to and including termination. Failure to report violations constitutes a violation in policy and is therefore subject to disciplinary action. These policies are intended to augment existing State, Federal, and copyright laws. Failure to comply with applicable State, Federal, or copyright laws is considered a violation in policy and may be subject to criminal prosecution. The agency reserves the right to monitor, audit, screen, and preserve data as the agency deems necessary in to maintain compliance with company policy.

**ELECTRONIC MEDICAL RECORDS:**

**POLICY:** Provide a comprehensive set of resources designed to support the organization in areas critical to obtaining and maintaining accreditation and funding.

**INTENT:** Make use of supportive technology to run throughout all sections of the policy manual, including both the administrative and clinical sections, and to ensure a perpetual state of improvement.

**PROCEDURE:** Implement new and improved technology to maintain and improve our commitment to quality standards.

**Personnel Acknowledgement Form:**

1. You need to complete the security awareness training and agree to uphold the acceptable use policy.

2. If you identify an unknown, un-escorted or otherwise unauthorized individuals in you need to immediately notify .

3. Visitors must be escorted by an authorized employee at all times. If you are responsible for escorting visitors you must restrict them to appropriate areas.

4. You are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by. For example, the use of external e-mail systems not hosted by to distribute data is not allowed.

5. Please keep a clean desk. To maintain information security you need to ensure that all printed in scope data is not left unattended at your workstation.

6. You need to use a secure password on all systems as per the password policy. These credentials must be unique and must not be used on other external systems or services.

7. Terminated employees will be required to return all records, in any format, containing personal information. This requirement should be part of the employee onboarding process with employees signing documentation to confirm they will do this.

8. You must immediately notify in the event that a device containing in scope data is lost (e.g. mobiles, laptops, etc.).

9. In the event that you find a system or process which you suspect is not compliant with this policy or the objective of information security you have a duty to inform so that they can take appropriate action.

10. If you have been assigned the ability to work remotely you must take extra precaution to ensure that data is appropriately handled. Seek guidance from if you are unsure as to your responsibilities.

11. Please ensure that assets holding data in scope are not left unduly exposed, for example visible in the back seat of your car.

12. Data that must be moved within is to be transferred only via business provided secure transfer mechanisms (e.g. encrypted USB keys, file shares, email etc.). will provide you with systems or devices that fit this purpose. You must not use other mechanisms to handle in scope data. If you have a query regarding use of a transfer mechanism, or it does not meet your business purpose you must raise this with.

13. Any information being transferred on a portable device (e.g. USB stick, laptop) must be encrypted in line with industry best practices and applicable law and regulations. If there is doubt regarding the requirements, seek guidance from .