Status Active PolicySat ID 16963879

Origination	06/2020	Owner	Tom Mockus: Director of Information Servic
Last Approved	10/2024	Area	Information Technology
Effective	10/2024		
Last Revised	10/2024		
Next Review	10/2026		

Information Systems Acceptable Use Agreement

Mount Desert Island Hospital **Information Systems Acceptable Use Agreement**	
Mount Desert Island (MDI) Hospital (*which shall be referred to as* MDI, MDIHO, or the **organization**) is committed to protecting the information assets of our patients, our customers, our employees, our partners and the Hospital itself. Today's environment of connected technologies offers many opportunities for cybercriminals from all over the world to anonymously attack, damage and corrupt vital information; and to disrupt our ability to communicate effectively and accomplish our mission statement: "To provide compassionate care and strengthen the health of our community by embracing tomorrow's methods and respecting time-honored values". Effective security is a shared responsibility, and a team effort involving the participation and support of every employee, board member, contractor, vendor, student intern or volunteer who deals with information and/or information systems. It is the responsibility of every employee and affiliate to know, understand and adhere to these policies, procedures, standards and guidelines, and to conduct their activities accordingly. Based on best practices and HIPAA regulations, we have endeavored to create policies which are clear, concise and easy to understand. Thank you in advance for your support as we do our best to maintain a secure environment, and fulfill our obligations and our mission.	
Distribution	Current employees will receive a copy of this agreement upon hire and annually thereafter. Members of the Board of Trustees will receive a copy of this agreement at appointment and annually thereafter.
Acceptable Use Agreement	• I certify that I have read and fully understand the Information Systems Acceptable Use Agreement set forth in this document. I understand and acknowledge my obligations and responsibilities. • I understand that MDI Hospital reserves the right to monitor system activity and usage. My signature on this document means I have consented to this monitoring.

	• I agree that I will not purposely engage in activity that may: harass, threaten or abuse others; take actions that will impede or reduce the performance of Information Resources; deprive an authorized MDI Hospital user access to an MDI Hospital resource; obtain extra resources beyond those allocated; or in any way circumvent MDI Hospital computer security measures. • I further understand that violation of these policies is subject to disciplinary action up to and including termination without prior warning or notice. Additionally, individuals may be subject to civil liability and criminal prosecution. • None of the requirements of this agreement are intended to infringe on your legal rights under federal and state labor laws, including your right to engage in protected activities under the National Labor Relations Act. If you have any questions about this policy, we encourage you to consult with your supervisor or Human Resources.
Acknowledged & Agreed to by	____ User Signature Date ____________________________________ Printed Name

MDI Hospital - Information Systems Acceptable Use Agreement

Access Control	
Access to MDI Hospital information will be limited to those persons who are reasonably required to know such information in order to accomplish our legitimate business purposes or as is necessary for compliance with state or federal regulations.	
Data Classification	• MDI Hospital data classifications include Protected, Confidential and Public. • All data is required to have data classification applied.
Data Handling	• In accordance with regulatory and contractual requirements, each type of classification has specific data handling requirements. • All personnel are expected to handle, store, or use data in accordance with the requirements. • **Reference the MDI Hospital Data Handling Matrix for instructions, included in this Acceptable Use Agreement.**
Authentication	
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may compromise MDI Hospital's entire corporate network. As such, all users are responsible to take the appropriate steps, as outlined below, to select and secure their passwords.	

Password Requirements	• Passwords must be unique, at least 14 characters long, and be comprised of a minimum of 3 out of the following 4 types of characters: numbers, lower-case letters, upper-case letters, and special characters (i.e., #, &, *, etc.). • The password must not include the users first or last name and should not contain dictionary words or names like those of children, pet, or favorite hobby. • Passwords must be changed at least every 365 days. • Users are not permitted to reuse any of their last 5 passwords when selecting a new password. • Accounts will be locked out (disabled) after 5 consecutive failed log-on attempts. Network accounts will remain locked out until unlocked by an administrator or authorized staff member. • All user passwords must expire and will be deactivated after 30 days of inactivity.
Password Protection	• Every user is responsible for any actions performed using their network or application account. Therefore, it is important that users protect their passwords by not writing them down on paper or storing them in a text file on their computer in an unencrypted form. • Passwords must never be shared with anyone, including IT staff. No member of the organization (e.g., IT Staff, the CEO, Management, etc.) will ever call and ask an employee to share their password. • Systems, applications, and internet browsers must never be configured with the "Remember Password" feature enabled. Users must not set the remember password feature. • Work passwords must never be re-used for other types of accounts such as Gmail, Amazon, an ISP e-mail account, etc. These passwords can be easily intercepted and can result in compromising MDI Hospital's network security. • Users must report all password compromises or attempted compromises to the Information Security Manager. • Passwords must be changed if there is any suspicion of compromise.
Email	
This section applies to all users who have been granted permission to use MDI Hospital's email system.	
Email Use	MDI Hospital's email system is a communication tool designed to deliver and receive electronic messages. It is not a record keeping system and should not be used as a database for storing memoranda and other electronic documents. All email messages must be treated as any other MDI Hospital correspondence and be retained in accordance with MDI Hospital's Record Retention Schedule. Email use is subject to the

following:

- MDI Hospital owns the email system and the information transmitted and stored within it. **Users will have no expectations of privacy**.
- Users must use the MDI Hospital approved email encryption solution when sending any email (with or without attachments) that contains Protected or Confidential data.
- Users must add the word [secure] (with brackets, case not sensitive) to the subject line on any email containing protected data.
- Users must be cautious about the type of information communicated by e-mail.
- The following activities are **prohibited**:

- Sending email that is intimidating or harassing.
- Using email for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending or receiving email, except when authorized to send messages for another when serving in an administrative support role.
- The following activities are **prohibited** because they impede the functioning of network communications and the efficient operations of electronic mail systems
    - Sending or forwarding chain letters.
    - Sending unsolicited messages to large groups except as required to conduct MDI Hospital business.
    - Sending excessively large messages.
    - Sending or forwarding email that is likely to contain computer viruses.

- Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of MDI Hospital unless authorized to do so.
- Individuals must not send, forward or receive protected or confidential information through non-MDI Hospital email accounts. Examples of non-MDI Hospital email accounts include, but are not limited to, Gmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).
- MDIHO requests users not access personal email accounts (i.e., non-MDI Hospital email accounts) from MDI Hospital provided equipment.
- Individuals must not send, forward, receive or store protected or confidential information utilizing non-MDI Hospital approved mobile devices. Examples of mobile devices include, but are not limited to, smartphones, laptops, Personal Data Assistants and cellular telephones.
- E-mail messages and Internet site, cache accessed are not private but are

property of MDI Hospital. MDI Hospital may review e-mail messages and Internet sites accessed by a user.

- Users should not use MDI Hospital email for regular personal use (*see also Incidental Usage*).
- Users should be cautious when receiving emails containing attachments; users should examine the email and refrain from opening or downloading any suspicious file.
- Users should not click on URL links in email.

Telephone and voice mail usage

This section applies to organization-wide expectations regarding the use of telephone and voice mail, as well as expectations regarding the timely return of phone calls.

Telephone and Voicemail

Use of Telephone

- It is expected that employees will limit personal calls and will not make long distance calls unless given permission to do so by their supervisor.
- It is expected that employees will provide callers with their direct extensions and the voice assisted operator number (207-288-5082) whenever possible to limit calls coming to reception, and to limit the number of overhead pages.
- It is expected that employees will provide their first and last names when leaving messages outside the organization to limit confusion when the party returns the call.

Timely Response

- It is expected that employees will return phone calls from external customers (excluding vendors and solicitors) within one (1) business day, even if the response is to just acknowledge receipt of the call and to establish a timeline for follow-up.
- It is expected that employees will return phone calls within the organization within two (2) business days, unless the caller requests otherwise.
- It is expected that employees who are unable to meet a one-day response for external customers and/or a two-day response from internal calls due to time off, limited availability, part-time schedule, etc. will set their voice mail greeting to indicate when a response can be expected given their out-of-office conditions.
- It is expected that employees will use temporary voice mail greetings to indicate vacations and other extended absences

Digital Badge and Images

This section applies to all users employed by MDI Hospital. The use of digital photo badges enhances our security protocols by providing a modern, efficient means of identification. Just as physical badges facilitate secure interactions with other employees and patients, digital photos embedded in emails and Microsoft 365 communications serve a similar purpose in the digital realm..

Microsoft 365 / Email

MDI Hospital will be adding your photograph to your profile within our Microsoft Office 365 environment for internal business purposes. Digital photos in Microsoft 365 profiles facilitate instant recognition, reducing the chances of miscommunication and ensuring streamlined interactions. By including a visual identifier in digital communications, we enhance security by minimizing the risk of impersonation and unauthorized access.

Scope of Use: Your photograph will be used for identification, internal communications, organizational charts, and internal directories within Microsoft 365. It will not be shared externally without your explicit consent.

Security Measures: MDI Hospital is committed to protecting your privacy and will implement strict security measures to ensure your photograph is stored securely and accessed only by authorized personnel.

Consent: By signing this form, you agree to the following:

1. **Consent to Use Photograph:** I grant permission to upload and use my photograph within the Microsoft 365 environment for internal business purposes as described above.
2. **Duration of Use:** This consent remains in effect for the duration of my employment with MDI Hospital, or until I withdraw my consent in writing.
3. **Privacy and Security:** MDI Hospital will take all necessary steps to ensure the privacy and security of my photograph, in accordance with applicable laws and company policies.

Internet Use

This section applies to all users who have been granted permission to access the Internet using MDI Hospital's computing resources.

Internet Use

The internet is an excellent resource for information and a revolutionary way to communicate with the world, however, the Internet is also a rapidly changing and volatile place which can introduce threats to MDI Hospital and its ability to achieve our mission. As such, in order to protect our environment and allow use of the internet, the following rules apply when users access the internet:

The following is prohibited:

Websites/Access/Use:

- Use the Internet for any illegal purpose.
- Knowingly visit Internet sites that contain obscene, hateful, violent, or other objectionable materials.
- Attempt to access blocked sites or attempt to circumvent or otherwise changes settings that prohibit access to blocked sites (e.g., shopping, gambling, streaming, social media, or malicious known sites).
- Use the Internet including webmail, messaging, chatbots, etc. for offensive or vulgar messages such as messages that contain sexual or racial comments

or for any messages that do not conform to MDI Hospital's policies against harassment and discrimination.

- Access the Internet via any means other than an approved connection provided for that purpose.

Software/Downloads/Settings:

- Download or install any software or electronic files without the prior approval of the Information Security Manager.
- Download images or videos unless there is an approved business-related use for the material.
- Download entertainment software or games or play games against opponents over the Internet.
- Change any security settings in their internet browser unless under the direction of the Information Security Manager.
- Upload, download, or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of MDI Hospital, or the Hospital itself.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic, which substantially hinders others in their use of the network.

Activities/Communication:

- Perform any actions on behalf of MDI, unless authorized.
- Solicit non-MDI Hospital business for personal gain or profit.
- Participate in unauthorized political or religious activities.
- Represent personal opinions as those of MDI Hospital or purport to represent MDI Hospital when not authorized to do so.
- Make or post indecent remarks, proposals, or materials.

Data:

- Reveal or publicize protected, or confidential, information which includes, but is not limited to financial information, confidential patient, customer or employee information, marketing strategies and plans, databases and any information contained therein, client lists, computer software source codes, computer/network access codes, and business relationships

Social Media

This section applies to all users of MDI Hospital Information Resources.

Social Media Use	Social media, such as Facebook, Twitter, and blogs, is largely a personal communication medium. Even LinkedIn, as well as other "professional" social media sites, are used by individuals in their personal capacity. If MDI Hospital elects to participate in social media, any MDI Hospital communications will be subject to review and approval by Senior Management of MDI Hospital. *Personal* use of such media needs to be conducted in compliance with the following:

- Under no circumstances will Protected or Confidential Information be posted on social media sites.
- Under no circumstances will Protected or Confidential Information be uploaded or sent via social media messaging (i.e., chat or email functions).
- The personal use of Facebook, Twitter or social networking web sites must not interfere with working time. Personal use of social networking web sites from MDI Hospital provided equipment is monitored and restricted.
- Any messages that might be construed as the "voice" or position of MDI Hospital must be approved in advance by the Hospital.
- Any identification of the author, including usernames, pictures/logos, or "profile" web pages, must not use logos, trademarks, or other intellectual property of MDI Hospital, without approval of Hospital.
- A message must not disclose any protected or confidential information of MDI Hospital.
- Written messages are, or can become, public. Use common sense.
- In addition, *if a user identifies himself or herself on the site as an officer or employee of MDI Hospital:*
- Any comments on any aspect of MDI Hospital's business practices must include a disclaimer in his or her "profile" or "bio" that the views are his or her own and not those of Hospital.
- The user must avoid any use of profanity, racist or other discriminatory language, or any other communication that could be expected to reflect negatively on MDI Hospital.
- Any information a user (or former user) posts to the web that identifies their relationship to MDI Hospital must be and remain accurate. For example, listing in an online profile a current role as "Vice President, MDI Hospital" must be deleted or clarified ("Vice President, MDI Hospital: 2009-2013") promptly when it is no longer accurate.

Instant Messaging

This section applies to all users of MDI Hospital Information Resources.

Instant Messaging Use

MDI Hospital's instant messaging system is a communication tool designed to enhance productivity and facilitate internal communications in order to provide excellent customer service. Only instant messaging applications approved by MDI Hospital are permitted. Policies governing the acceptable use of email and the Internet apply to Instant Messaging.

- Employees have no reasonable expectation of privacy when using the company's IM system. The company reserves the right to monitor, access and disclose all employee IM communications.
- The IM system is intended for business use only.

	• Employees will use professional and appropriate language in all instant messages. • Employees should refrain from sending memes or other photos that may appear offensive or unprofessional. • Sending documents using MDI Hospital's instant messaging platform is prohibited unless in company approved IM. • All IM conversations are retained for a minimum of one (1) year.
Removable Media	
The following section applies to all users of MDI Hospital computing resources.	
Removable Media Requirements	To minimize the risk of loss or exposure of sensitive information maintained by MDI Hospital and to reduce the risk of acquiring malware infections on computers operated by the Hospital, the following restrictions on removable media apply: • Authorized hospital staff may only use MDI Hospital removable media on MDI owned equipment (e.g., computers). • Removable media may not be connected to or used in computers that are not owned or leased by MDI Hospital without explicit permission of the MDI Hospital information security staff. • All approved media requires encryption. • Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies.
Mobile Devices	
This section applies to all users who have been granted permission to access MDI Hospital's internal information resources via the use of a mobile device (e.g., smartphone, tablet).	
Mobile Device Policy	Use of mobile devices to access MDI Hospital information must abide by these requirements: • Execute the MDI Hospital *Mobile Device Agreement*. • Approval by the Information Security Manager and the employee's manager. • Conform to MDI Hospital security standards.
Mobile Device Requirements	Smartphones and tablets are a great convenience and becoming more and more a part of doing business. They also come with many risks including ease of theft, operation in unsecured environments, and easily intercepted wireless communications. In order to protect our valuable information; it is important that users of portable computing equipment follow these rules of use:

	• Only MDI Hospital approved mobile devices may be used to access MDI Hospital information resources. • The theft or loss of a mobile device must be reported to the Information Security Manager immediately. • Mobile devices will be configured with screen savers that lock after two (2) minutes of inactivity. • Mobile devices require a powered-on password and will lock after two (2) minutes of inactivity. • Mobile devices will be configured to be wiped after five (5) failed password attempts. • Mobile devices must be updated. • MDI Hospital data residing on mobile devices must be encrypted. • Mobile devices must be physically secured at all times.
Laptops	
This section applies to all users who have been granted a laptop computer to access MDI Hospital internal information resources.	
Laptop Use	Laptops are a great convenience and becoming more and more a part of doing business. They also come with many risks including ease of theft, operation in unsecured environments, and easily intercepted wireless communications. In order to protect our valuable information; it is important that users of laptops follow these rules of use: • Only MDI Hospital approved laptops may be used to access MDI Hospital information resources. • Laptops are subject to the same MDI Hospital controls as workstations, including patch requirements, malware protection, firewall rules, screen saver timeouts, password requirements, etc. • Laptops must be full-disk encrypted requiring a separate password than the users MDI Hospital network account. • Laptops must be physically secured at all times. • The theft or loss of a laptop must be reported to the Information Security Manager immediately. • Protected and/or Confidential company data cannot be stored on laptops unless specifically authorized by the Information Security Manager
Remote Access	
This section applies to all users who have been granted permission to access MDI Hospital's internal computing resources from a remote location.	
Remote Access Policy	Remote access to the MDI Hospital network will be provided to users authorized by Mangers with IT approval Any devices used for remote connectivity to the MDI Hospital network must conform to hospital remote access standards.

	Termination of authorized user's Remote Access is handled through the standard employee termination process upon employee termination or at management's request.
Remote Access Systems	Users requiring remote access based upon job function have a responsibility to protect MDI assets and information in the same manner as if working onsite. • No MDI Hospital data is to be stored on / saved to the remote workstation. • Remote access connections must use the authorized Citrix Secure Gateway or VPN. • Remote access connections require two factor authentication. • The remote workstation will: ◦ Be kept physically secure and not be used by anyone other than an MDI Hospital workforce member while connected to the MDI Hospital network. ◦ Have security controls in place: ▪ Antivirus Software installed and virus definition files updated. ▪ Desktop Firewall Software. ▪ Updated and current with operating system and application patches. ▪ No critical vulnerabilities or malware are present that could negatively affect the health of the MDI Hospital network. • Sessions will be automatically disconnected after 45 minutes of inactivity.
Physical Access	
The section applies to all facilities operated by the MDI Hospital and all employees, Board members, contractors, vendors, and any other person who may come in physical contact with resources that affect MDI Hospital's information assets on the Hospital's premises.	
Physical Access Policy & Requirements	Physical Security is the process of protecting information and technology from physical threats. Physical access to information processing areas and their supporting infrastructure (communications, power, and environmental) is controlled to prevent, detect, and minimize the effects of unintended access to these areas (i.e., unauthorized information access or disruption of information processing itself). The business of MDI Hospital requires that facilities have both publicly accessible areas as well as restricted areas. • All personnel (i.e., employees, contractors, volunteers, etc.) are required to where name / photo identification badges upon entering MDI facilities. • All personnel should only access areas permitted based upon job

	function. • All individuals that enter any of MDI Hospital's secured / restricted areas must be verified as authorized to do so. • Individuals are required to notify a Manager if they notice improperly identified visitors. • Access will be restricted to controlled areas of the facility (e.g., record retention areas, computer room, etc.). • Third-parties must not be given access to the Computer Room unless specifically authorized by the Information Security Manager, Security Officer or a member of Senior Management. • After-hours access within facilities by support personnel (e.g., cleaning crews, building maintenance, etc.) must be approved. • Protected and confidential data and/or information systems containing confidential or protected data must be physically secured when not in use. Files must be stored in controlled areas or locked vaults and access is limited to appropriate users based on job function. • Shredding bins must remain locked at all times. • All personnel must lock their computer when unattended regardless of location; the only exception to this is the operating room. • Individuals no longer requiring access (e.g., termination) are prohibited from accessing any non-public areas of the Hospital.
Training and Awareness	
The section applies to all facilities operated by the MDI Hospital and all employees, Board members, contractors, vendors, and any other person who may require access to MDIHO resources.	
Training and Awareness Policy & Requirements	All users are required to participate in ongoing cybersecurity training and awareness programs to maintain compliance with our acceptable use policies. The following mandatory training sessions are in place: • Quarterly Awareness Training: Focused on current threats, best practices, and emerging cyber risks. • Cybersecurity Training: Periodic, role-specific sessions that provide deeper insights into protecting information assets and maintaining a secure environment. • Annual Compliance Training: Comprehensive review of all policies, including acceptable use, information security, and privacy standards, ensuring continued adherence. Failure to complete the required trainings may result in restricted access to systems, disciplinary action, or other appropriate measures.
Incident Reporting	

The section applies to all facilities operated by the MDI Hospital and all employees, Board members, contractors, vendors, and any other person who may require access to MDIHO resources.

Incident Reporting Policy & Requirements

All users are required to promptly report any suspected or confirmed security incidents to ensure swift identification, escalation, and resolution. The following guidelines apply:

- Immediate Reporting: Users must report all security incidents, such as physical intrusion, phishing attempts, data breaches, system vulnerabilities, or policy violations as soon as they are identified.
- Confidentiality and Cooperation: Users are expected to maintain confidentiality regarding incidents and fully cooperate with the incident response team throughout the investigation process.
- Designated Reporting Channels: All incidents must be reported through the organization's official channels (e.g., incident response team, help desk, or security portal) to ensure proper tracking and response.
- No Exceptions: Failure to report an incident may result in disciplinary action, restricted access, or other corrective measures to ensure organizational security.

Incidental Use of Information Resources

The following section applies to all users of MDI Hospital computing resources.

Incidental Use

As a convenience to the user community, incidental use of Information Resources is permitted. Only brief and occasional use is considered to be incidental.
The following restrictions on incidental use apply:

- Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and so on, is permitted only to approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to MDI Hospital.
- Incidental use must not interfere with the normal performance of a user's work duties.
- Incidental use of information resources must not involve solicitation in any form, must not be associated with any outside business or employment activity, and must not potentially injure the reputation of MDI Hospital, its Board Members, or its Employees.
- All messages, files and documents – including personal messages, files and documents – located on information resources are considered to be owned by MDI Hospital and may be subject to open records requests, and may be accessed in accordance with this agreement.

Termination

The following section applies to all users and contractors whose employment or affiliation is terminated either voluntarily or involuntarily.

Termination Policy & Controls	Upon termination all assets (physical and digital) must be returned to MDI. • The terminated user must immediately surrender the following: all keys, equipment, IDs, access codes, badges, business cards and similar items that are used to access MDI Hospital's premises or records; • The terminated user's voicemail access, e-mail access, Internet access, passwords, and any other physical or electronic access to personal information will be disabled immediately; and • The terminated user must return all records to MDI Hospital that contains protected or confidential information, which at the time of termination is in the terminated user's possession. Such records include all personal information stored on laptops or other portable devices or media, and in files, work papers, etc.

MDI Hospital Data Handling Matrix

Data Handling Category	**Protected Information**	**Confidential Information**	**Public Information**
Data Definition	Protected information is defined as information that requires the highest level of protection; which if modified or disclosed would have legal, regulatory, and financial or negative public perception impact. Disclosure or modification of protected information could adversely impact business partners, patients, customers and/or the MDI Hospital workforce. Protected information includes patient, customer, or company information that is protected by law, regulation, contract or agreement.	Confidential information is defined as information that is restricted to MDI Hospital employees, volunteers, contractors, auditors, regulators, vendors, and affiliates on a "need-to-know" basis. It is information that is used in the normal course of MDI Hospital's business for which unauthorized access or disclosure could adversely impact the company or its employees. Confidential information also includes employee specific information such as salary, payroll and performance appraisals.	Public information is defined as information which is not classified as protected or confidential, and would not cause harm to MDI Hospital, its patients, vendors or business partners if made generally available. Public information must be authorized by management for release to the public.
Data Examples	Social Security number, driver's license number, account number, non-public financial information, loan applications, credit reports, account	Reports, proposals, RFPs, general business information. Files that contain network or business critical passwords, personnel records, sensitive legal	Marketing materials, portions of the company website, or published reports.

	statements, credit card numbers.	documents, password reset communications, network and systems information, internal vulnerability assessments, revenue, expenses, and other financial data, budgets, etc.	
Patient / Customer Telephone Identification Procedure	Full Patient Name and Account Number or Social Security Number Plus one of the following: • Last **4 digits** of Social Security number (if not already used as listed above) • Full birthdate	Not applicable.	No special requirement.
Electronic File Transfer	Encryption required.	Encryption required.	No special requirement.
Data Storage (Servers)	Allowed as required for business purposes.	Allowed as required for business purposes.	Allowed as required for business purposes.
Data Storage (Workstations – Internal)	Not allowed.	Not allowed.	No special requirement.
Data Storage (Mobile Devices & Removable Media)	Encryption required.	Encryption required.	No special requirement.
Data Storage (Workstations – Working Remotely)	Not allowed.	Not allowed.	No special requirement.
Smartphones & Tablets	Encryption required.	Encryption required.	No special requirement.
Data Retention	See Records Retention Policy.	See Records Retention Policy.	See Records Retention Policy.
Electronic Data Disposal/ Destruction	Physical destruction for permanent disposal. For internal reuse media sanitization performed based on NIST guidance.	Physical destruction for permanent disposal. For internal reuse media sanitization performed based on NIST guidance.	Physical destruction for permanent disposal.

Paper Document Disposal	Use confidential / locked shred bins.	Use confidential / locked shred bins.	No special requirement.
Paper Document Storage	Use secure / locked storage area.	Use secure / locked storage area.	No special requirement.
External Mail Carriers	Commercial carrier or courier service. Envelope/box to be sealed in such a way that tampering would be indicated upon receipt.	Commercial carrier or courier service. Envelope/box to be sealed in such a way that tampering would be indicated upon receipt.	No special requirement.
Fax	Incoming faxes containing protected information will be removed immediately.	Incoming faxes containing confidential information will be removed immediately.	No special requirement.
Internal Email	Allowed.	Allowed.	No special requirement.
External Email	Encryption required – Use [SECURE] in subject line.	Encryption required – Use [SECURE] in subject line.	No special requirement.
Internal Instant Messaging	Allowed.	Allowed.	No special requirement.
Suspected Breach or Unauthorized Disclosure of Data Must be Reported to:		Tom Mockus, Director of IT and Cyber, Privacy Officer	
Data Handling Questions Must be Directed to:		Will Houston, Network Security Manger	

All Revision Dates

10/2024, 06/2020

Attachments

Information Systems Acceptable Use Agreement

Approval Signatures

Step Description	Approver	Date

CEO Approval	Chrissi Maguire: President & CEO	10/2024
	Tom Mockus: Director of Information Servic	10/2024