Joint Industry Board of the Electrical Industry

Information Security Policy

Effective: June 13, 2025

Confidential and proprietary.

Not for distribution outside of the JIBEI*.

As Adopted by JIB Services LLC

Version: 8

*Confidential. Not for distribution outside of the JIBEI unless approved by CTO

Table of Contents

1. Introduction

Information is one of the Joint Industry Board's ("JIBEI") most important assets. The JIBEI is entrusted with the protection of our participants' personal data such as social security numbers, personal health, and personal financial information. We take this responsibility very seriously.

A valuable asset is you, the JIBEI employee (and consultants performing services on behalf of JIBEI). During the course of performing your duties for the JIBEI, you may be exposed directly or indirectly to confidential information. It is critical that you understand the policies and procedures concerning such information so that the integrity of the JIBEI is not compromised and that the trust of the Local 3 membership and all of our participants is always maintained. We can achieve this through a team effort.

Effective security involves the participation and support of every JIBEI employee who deals with information or information systems. It is the responsibility of all employees to know and understand the guidelines presented in this booklet, and to conduct their activities accordingly.

1.1. Formats of this Document

The authoritative version of this document is located on the IT page of the JIBEI intranet (i.e., the JIBEI's internal website for its employees) http://intranet . Employees should consult the intranet to ensure they have the most up-to-date information.

1.2. Feedback and Questions

If you have questions regarding the JIBEI's security policies and procedures, or if you have suggestions or comments regarding this document, contact the Sr. Manager of Information Security at Ext# 1450 or the IT Help Desk at x1499.

2. Overview

2.1. What is Information Security?

Information security deals with several different aspects of securing information. Information security is not confined to computer systems or to information in an electronic format. It applies to all aspects of safeguarding information in any of its many forms.

Major items involved in information security include:

- Confidentiality. The safekeeping of data and information by restricting access to individuals who have a need, reason, and permission to such data and information.

- Data Security and Privacy. The protection of data in all its forms (electronic, paper, or other), and throughout its life cycle (origination, entry, processing, distribution, storage, and disposal) from unauthorized access, modification, destruction, or

disclosure, whether accidental or intentional.

- Integrity. The accuracy, consistency, and completeness of data.

- Availability. The system and related resources are available to authorized users.

2.2. What Information needs protection?

- Protected Health Information (PHI) (e.g., member's and employee's health records, eligibility information)., as defined by the Healthcare Insurance Portability and Accountability Act (HIPAA)

- Electronic Protected Health Information (ePHI) (Protected Health Information that is transmitted electronically)., as defined by HIPAA

- Personal Identifiable Information (PII) is defined as information:
    - (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, maiden name, biometric data, etc.) or
    - (ii) By which the Joint Industry Board uses to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

- Confidential member or employee information (e.g., social security number and address)
- Other Confidential Data
    - Internal Policy and Procedures
    - Financial Information
    - Internal Communication and documents
    - Payroll information.
    - Account balances
- All non-public JIBEI information needs protection and safeguards as appropriate.

2.3. Information Security is a Group Effort

The primary responsibility for information security resides with end -users (i.e., employees, consultants). All employees are accountable for their actions in the creation, transmission, storage, and use of all information including PHI. Employees are responsible for controlling access to information and information systems, ensuring its integrity, as well as its availability to others who require it for their legitimate business needs.

Consultants are required to sign an information security agreement and the Business Associate Agreement, where if there is a breach of contract, the appropriate action will be taken.

2.4. Security Guidelines for All Users

The user is any person who has been authorized to read, enter, or update information. All users are accountable for their actions in the creation, transmission, storage, and use of all information including PHI, PII and HIPAA data. A user of information is expected to:

1. Access information only in support of their authorized job responsibilities.

2. Comply with Information Security Policies and Procedures and with all controls established by the owner and custodian of the information.

3. Refer all improper disclosures of PHI both inside and outside of the JIBEI to HIPAA Security Officer. Proper disclosures are those related to treatment, payment, or health care operations. In certain circumstances, the Security Officer may specifically delegate the disclosure process to other departments.

4. Keep personal authentication devices (e.g., passwords, Secure Cards, personal identification numbers, etc.) confidential and secure

2.5. Treat Paper Records and Electronic Data Equally

Sensitive information on paper is the same as sensitive information on a computer. Both need to be protected from unauthorized access and should be treated with caution and discretion. In particular, protected health information (PHI) in all forms (called ePHI, or Electronic Protected Health Information, when transmitted via computer or other electronic means) is covered by the HIPAA privacy regulations.

It is sometimes necessary to print out sensitive electronic information on paper and make copies. Do not leave these copies lying around in open areas within your workspace, as this information may be seen or even taken by unauthorized parties. If you would not want someone to read that information on your computer, you probably would not want someone to read the same information on paper.

Keep printouts of sensitive information such as medical records in a secure location, such as a locked desk, locked filing cabinet or a safe. Avoid leaving sensitive documents unattended, especially in high traffic areas. When disposing of copies of sensitive information always shred or place them in a secure recycling bin. Do not simply toss them in the trash.

Remember to shred any printouts containing any information that would be useful to identity thieves, including documents containing any personal, financial, or protected health information. The JIBEI has a contract with a vendor to provide centralized shredding services. The vendor has placed secured receptacles throughout the JIBEI office space where sensitive materials can be discarded. Materials placed in these bins are periodically removed from the premises and shredded. This service is available to

all JIBEI departments.

3. Information Security Policy

3.1. Purpose

This chapter sets forth the policy of the JIBEI with regard to the use of, access to, review, or disclosure of confidential information, particularly information, which is stored and exchanged electronically. The JIBEI's purpose in creating this policy is not to impose restrictions that are contrary to its established culture of openness and trust. Rather, the JIBEI wishes to protect the JIBEI's employees, partners and the JIBEI itself from illegal or harmful actions by individuals, whether those actions are intentional or accidental.

3.2. Scope

This Information Security Policy covers, but is not limited to, the following: internet and intranet systems; computer hardware, software, and operating systems; all digital storage media, including both fixed and removable storage devices; and user access accounts on all JIBEI computer systems, including network, mainframe, electronic mail, secure file transfer protocol , and other user accounts.

This policy applies to all individuals using the JIBEI's computer and network systems, including employees, contractors, and consultants. It is the responsibility of every user to adhere to these guidelines. Remedies for non- compliance are discussed in Chapter 10, Enforcement and Compliance.

3.3. Roles and Responsibilities

The Sr. Manager of Information Security & Networking, under the direction of the Chief Technology Officer, is responsible for establishing and implementing organization-wide information systems security policies, standards, guidelines and procedures.

While responsibility for information security on a day-to-day basis is every user's duty, the Information Security & Networking department is responsible for identifying and implementing security products, procedures and frameworks, which align with JIBEI's operational needs. Information Security monitors systems and services for potential cyber security risks and threats.

All Users are responsible for complying with this and all other JIBEI policies and procedures covering computer and network security measures. Users are required to take security awareness training at least annually, as provided from the Learning Management System by the Information Security & Networking department, and acknowledge this Information Security policy on a periodic basis. In addition, IT and HR will evaluate refresher or supplementary training as needed. All employees will receive emails mimicking common phishing emails, and may be required to take

additional training if they are susceptible to these emails.

Definitions

For the purposes of this policy, the following definitions apply:

1. Confidential information: (a) Information of a private nature that is protected by law from public disclosure, including, but not limited to, personal health information (PHI), electronic personal health information (ePHI), social security numbers, and addresses of JIBEI members and employees; and (b) Information about the business activities of the JIBEI including, but not limited to, financial and technical data, operations and strategies, and lists of Local 3 members or JIBEI employees.

   Personal Identifiable Information (PII) is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, maiden name, biometric data, etc.) or (ii) by which the Joint Industry Board use to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media

2. Electronic communications: Data, which is sent, received, or obtained through the internet, intranet, voicemail, facsimile machine, teleconference, instant message, or online information service.

3.4. Systems Use and Data Ownership

1. Email, internet access, and equipment provided by the JIBEI are intended for JIBEI-related business use. Personal email and Internet should not be accessed from JIB equipment, whether using it onsite or remotely.
   Personal use should not be during working time and should not interfere with job performance. Employees are responsible for exercising good judgment regarding the reasonableness of personal use; however, JIBEI management reserves the right to determine what constitutes reasonable use and to terminate personal usage rights for employees who abuse their privileges. If there is any uncertainty regarding the personal use of equipment, employees should consult their supervisor or manager.

2. All electronic communication is JIBEI property. The JIBEI treats all electronic communications sent, received, or stored as business property, including those for personal use.

3. While the JIBEI's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on JIBEI systems remains the property of the JIBEI. No user shall have any expectation of privacy with respect to any electronic message. The JIBEI monitors all electronic communication and periodically reviews selected messages as part of its audit

and security process.

4. Access to the JIBEI's equipment. JIBEI may monitor equipment, system and network traffic at any time. Remote Access is limited to employees who are on site at the JIBEI or who have been expressly authorized to access its equipment from other locations. When authorized, access from other locations must be through a secure and encrypted communications channel as determined by JIBEI Information Security.

5. The technical staff of the JIBEI strives to deploy equipment in conformance with the wishes of employees whenever possible. Nevertheless, the JIBEI reserves the right to deploy equipment in a manner most suitable for its business operations and retains final authority over its installation and configuration.

6. To ensure compliance with this policy, authorized individuals within the JIBEI may monitor equipment, systems and network traffic at any time, including but not limited to JIB email, file transfers and files stored on JIB equipment or transmitted over the JIB network.

3.5. Privacy & Confidential Information

3.5.1 Data Privacy

Data Privacy overlaps with security and confidentiality. Privacy is at the heart of the "Confidentiality" leg of the CIA triad "Confidentiality, Integrity, Availability", which are the cornerstone principles of an Information Security program. Many administrative, technical, and physical safeguards to ensure security overlap with those to ensure privacy. While Information Security controls contribute to managing privacy risk, privacy risks can also arise by means unrelated to security incidents.

The Participant ID (PID) was created to have an alternate identifier to help protect the privacy of our members. Where possible, PID should be used on forms, etc. instead of the Social Security Number (SSN).

Some of the types of privacy controls we employ at JIBEI include:

- Identity and Access management
- Data Leakage Protection (DLP)
- Encryption
- Incident Response plan
- Third Party risk management
- Policies
- Training.

The above is just a high level of controls that help ensure Data Privacy. Many things we do under the auspices of Information Security, improves our Data Security posture. For example, patching systems reduces vulnerabilities, which reduces the likelihood of a system being compromised, which in turn reduces the likelihood of a data breach.

All employees play an important role in Data Privacy. For example, not sharing data with others (employees or externally) unless authorized and necessary to conduct business, not

discussing confidential information in public places, disposing of confidential documents properly and always being on the lookout for phishing and other malicious attempts in emails or when clicking on links.

Privacy events could arise from system or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal. The problems individuals may experience as a result of data privacy issues range from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm.

JIBEI employees should take members' privacy into account in selecting, designing and deploying systems, practices and services that involve individuals' data. Members' data should only be collected, processed, or shared (where permitted) to the extent that it is necessary to provide the services of JIBEI.

3.5.2 Confidentiality

Understanding how to handle sensitive data, like PHI, ePHI, and PII, is important for safeguarding the confidentiality of information. Regardless of the type of data, the integrity and accuracy of information must be protected. The purpose of this policy is to establish rules and regulations on how to handle protected health information and other sensitive data.

The JIBEI requires that all sensitive or vulnerable information are encrypted before it is exchanged with parties outside of the JIBEI. In addition, Information Security must review the recipients to make sure they have security in place once it is unencrypted on the other end. For further information about data encryption, see Sections 4. Exchanging Confidential Information" and 4.1 Encryption

3.5.3 Employee and Member Records

JIBEI employees are reminded that much information about individual members, individual employees, and most information about health records for either, is considered confidential under federal law and may not be released to unauthorized personnel without permission from the member or employee.

4. Exchanging Confidential Information

Employee and member records must be protected by a level of security commensurate with their confidentiality. Member records should not be maintained on publicly accessible systems (such as the internet).

All sensitive data provided to parties external to the JIBEI (benefit providers, vendors, banks, contractors, etc.) must be encrypted. **Under no circumstances should unencrypted confidential data be sent to anyone outside of the JIBEI.** This policy applies regardless of the method used to transfer the data, such as: file transfer, CD-ROM*, email, or other medium. (*JIB Medical may provide patients with an

unencrypted record of their medical records as long as it is physically handed to them).

Email to certain organizations will be encrypted, by default, using Transport Layer Security (TLS). See Table 1 on next page. TLS encryption is transparent and does not require registration.

To encrypt an email to anyone NOT at an organization on Table 1, simply put [Secure] in the subject or body of your email. Putting [Secure] in the subject line will cause the email to be encrypted by JIBEI's encryption software to recipients outside of the organization. Note that "secure" maybe in upper or lower case, but it must be surrounded by the square brackets. In order to read this email the recipient will be prompted to register for an id.

External parties, who send data to the JIBEI, both through the mail or electronically, are strongly encouraged to encrypt the data.

Table 1: TLS List

List of organizations, which emails are encrypted by default.

Organization Name
Accredo Health Group, Inc.
Active Care Network
Anthem Health Insurance (formally Blue Cross Blue Shield)
Benz Communications/Segal Group
Blood Stone Magazine
Bridgeway (formerly Basys)
Brighton Health Plan Solutions
Care Continuum Partners, LLC
Children's Hemophilia
Christie Digital Systems USA
Cisco
Cohen Weiss and Simon, LLP
Congruity
CuraScript SD
Dell
Deutsche Bank
IBM Support for Data Domain
Electchester Management
Empire BlueCross BlueShield
Empower(formerly Prudential)
Express Scripts
FactorCare Pharmacy, LLC
Freedom Fertility Pharmacy
Great West Retirement
HealthBridge Inc.
Healy Electric
Hemophila Health
Integrity Healthcare
IRS.gov
JWS Software

Lincoln Financial Group
Local 3
Magnacare
Marcus And Pollack LLP
Matrix Oncology
Medco Foundation
Medco Sports Medicine
Microsoft Office 365
Neuberger Berman
Nova Factor Inc.
Novartis
NPC Recruiting
Nutanix
NutrePlection Resources
NYC Department of Buildings
NYC Workers Compensation Board
Optum (formerly Connect your Care)
Optum Workers Comp
Pharmacare Resources Inc.
PMSI Online
Priority Health
Procurri
Proofpoint
Proherant Hospital & Healthcare
RSM US LLP (Audit)
Rx Partnership (Express Scripts)
Segal Marco Advisors
Segal Select Insurance
Seix Investments Advisors, LLC.
State Street
Sunrise HM
SystemED
The Segal Group
Value Health Inc.

Verizon
Virtus Investment Partners

4.1 Encryption

Encryption is use to help protect sensitive information, (ex. PHI/ PII) from disclosure in transit and/or storage ("at rest"). Only approved encryption products, coordinated through the IT Department and Information Security Team, should be use to secure sensitive information.

User/Employee Responsibilities:

Encryption requirements that Employees must be aware of and actively comply with include:

- Confidential Information, as described in Section 2.2, must be encrypted (using a method approved by JIB Information Security) when transmitted outside of the JIBIE network, whether it be via email, VPN, SFTP or any other external transport method
- Any "solutions" (portals, SFTP servers, applications, etc.) that third parties supply or recommend to transfer confidential information must be reviewed and approved by JIBEI Information Security before a JIBEI employee can use them to transfer confidential data
- The use of DropBox, Google Drive and similar applications are NOT permitted, even if the data is encrypted in transit

Email:

- If you need to send an email to an authorized party containing confidential information, TLS encryption will automatically be employed if the organization is listed in Table 1 in Section 4
- To send confidential data via email to an authorized party, not on Table 1, you, the employee, must actively use the Proofpoint Secure Mail option as described in Section 4: Exchanging Confidential Information

Files:

- To transfer files to or from an authorized party for the first time please contact the IT Help Desk so we can:
  (1) Verify that the data will be appropriately secured at the receiving end
  (2) Work with you to determine the most effective method of securely transferring the file(s). Some of our options include:
    a. Solarwinds SFTP/ServU
    b. PGP
    c. Citrix ShareFile
    d. Setting up a Secure VPN Tunnel with the other organization
- The use of thumb drives/usb drives is NOT permitted. Any exception must be approved by the CTO. When used, confidential data must be encrypted when transported by computer-readable storage media, such as magnetic tape, CD-ROM, or any other removable media (i.e., thumb drive or flash cards, etc.).

Websites:

- Always make sure a website is authorized before entering confidential information or credentials
- Encrypted websites usually have "https:\\" not "http:\\" as the beginning of the URL. The "s" stands for secure

- It is best to type in the website directly or use a bookmark rather than using a link that you receive in an email
- employees should not enter SSNs or credentials into third party websites unless vetted (note: Phishing campaigns often lure users to lookalike websites that ask them to enter their credentials or confidential data – always be aware or call IT if not sure)

IT Encryption Responsibilities:

There are many things the IT department does to secure and encrypt data that are transparent to the user. Some of these responsibilities are:

- Setting up encryption options to be used by end users such as TLS, SFTP, VPN Tunnels, Citrix ShareFile, etc.
- Configuring Proof Point Email Security to automatically encrypt emails containing a 9-digit number as a second level defense if employees fail to do so
- Evaluating third parties that we exchange data with for adequate security controls, one of which is encryption
- Regular security reviews of Third parties, including encryption
- Scanning files sent over the internet as a second line of defense to block unencrypted files that contain 9-digit numbers, where possible (this should not be relied upon as the first line of defense. The first line of defense is the employee s should not include SSNs in email attachments, or enter SSNs or credentials into third party websites unless vetted
- Encrypting backups and ensuring we have offline backups that can be restored in the event of a ransomware attack. (Ransomware is when an unauthorized third party encrypts an organization's data so that the organization cannot access it unless they pay "ransom")
- Configuring all JIBEI laptops with full disk encryption before lending to employees for home use or assigning them for onsite use
- Utilizing encryption software for data at rest on the mainframe, AS400 (IBMi) and network.

Please refer to Section 2.2 and 3.5.3 of this Information Security Policy and the JIBEI Data Governance & Classification Policy for further guidance on what information must be encrypted. The authoritative version of this policy is located on the IT page of the JIBEI intranet (i.e., the JIBEI's internal website for its employees) http://intranet

5. Prohibited Activities

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. However, under no circumstances is an employee of the JIBEI authorized to engage in any activity that is illegal under local, state, federal, or international law.

The lists below are not meant to be exhaustive. Instead, they attempt to provide a framework for activities, which fall into the category of unacceptable use.

5.1 Prohibited System and Network Activities

The following activities are prohibited:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the JIBEI.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, e-mail bombs, etc.).

- Using a JIBEI computer or other electronic media to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the employee is not an intended recipient, using another person's password, or logging into a server or account that the employee is not authorized to access, unless these activities are within the scope of regular duties.
- Port Scanning or security scanning, network monitoring, circumventing authentication or security of any host or network are prohibited, except when performed by the IT staff for testing and auditing purposes. (Port scanning is a technique used by hackers to find vulnerabilities in network servers. Normal users of JIBEI computer equipment need not be concerned about unwittingly violating this restriction.)

- Executing any form of network monitoring which will intercept data not intended for the employee's computer, except when performed by the IT staff in the for testing and auditing purposes.

- Circumventing user authentication or security of any host, network or account.

- Using any program, or sending messages of any kind, with the intent to interfere with, or disable computer equipment of any kind.

- Providing personal or work-related information about, or lists of, JIBEI-administered plan participants or JIBEI employees to parties outside the JIBEI.

- The saving of any documents or programs on the local hard drive of any JIBEI computer, unless management authorizes such use.

- Copying data to any external device (floppy drive, CD-ROM drive, USB device), file sharing websites (such as Google Drive, Dropbox, OneDrive) or personal email, etc.on any JIBEI computer, unless the CTO authorizes such use.

- Employees are not allowed to stream music or video (including news or sporting events) from JIBEI computers or from their own devices when connected to any JIBEI wireless network. Streaming music and video consume excessive bandwidth and disrupts business operations that depend on the bandwidth.

5.2 Prohibited Email and Communications Activities

The following activities are prohibited:

- Emailing unencrypted, confidential information to external parties either in the message body or as an attachment. Confidential information shared with external parties must be encrypted as described in Section 4. “Exchanging Confidential Information” and 4.1 “Encryption”.
- Storing social security numbers, dates of birth, or medical information in emails.
- Forwarding emails with attachments containing PII in image files or converting attachments to an unsupported file format to try and bypass security scanning.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, or telephone, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than the sender's, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Automatically forwarding JIBEI email to a third-party email system (i.e., Gmail, Yahoo mail, etc.). Individual messages forwarded to a third-party email system must not contain confidential information.
- Using third party email systems to conduct JIBEI business.
- Do not forward emails that are considered malicious to anyone else except to the IT Department. Use the “Report to IT” button under the Security Actions tab in Outlook to report suspicious emails.
- Use of USB drives are not permitted at the JIB unless previously approved by the CTO.

6. Physical Security

The JIBEI limits physical access to its property and assets to employees and authorized visitors. JIBEI employees are required to observe the following guidelines with respect to physical access to the JIBEI premises and equipment:

1. Employees may not share keys, access cards, or codes for security devices with other employees. If an employee loses a key or access card, or suspects that an access code has been compromised, that employee should contact Human Resources at extension 1400.
2. Employees are prohibited from interfering with any physical security mechanism in place at the JIBEI. In particular, employees are not to circumvent security devices by, for example, propping open security doors or otherwise interfering with their normal operation.
3. Management must approve access to the JIBEI premises, and visitors to the JIBEI must be accompanied by a JIBEI employee at all times. Employees who suspect that an unauthorized person has gained access to JIBEI property should call security at extension 1121.
4. Access to the secured systems area on the fifth floor is limited to those who require access as part of their job responsibilities. The Chief Technology Officer must approve visitor access to the secured systems area.
5. Employees should be aware that access logs to all areas of the building are maintained and periodically audited to ensure compliance with these policies. Employees who violate these policies are subject to disciplinary action as described in Chapter 10, Enforcement and Compliance.

6.1 Environmental Safeguards

Ensuring that all computer, network, and telecommuting equipment is physically protected from security threats is essential in order to reduce the risk of unauthorized access, inadvertent or unintentional disclosure of information, loss, modification, or damage to JIBEI information assets. The following measures should be taken to safeguard against equipment failures and to minimize damage from natural hazards.

This policy outlines physical and environmental controls that are in place within the JIBEI building generally and the data center specifically. These rules are in place to protect the employees and JIBEI data. Inappropriate equipment access exposes the JIBEI to risks including virus attacks, compromise of network systems and service, and legal issues.

1. Drinking and eating in the immediate areas of computers is restricted in accordance with the already established JIBEI policy.

2. Employees should exercise care when cleaning or using solvents on or around computer equipment as it is often very sensitive and can easily damage.

3. Controls are necessary to minimize damage from natural hazards such as fire or excess water. For example, flooding can result from breaks in the cooling system or

water drainage pipes. Computer equipment must be protected against natural disasters such as fire damage, water damage, or electrical surges.

4. Computer equipment must not be located near any combustible or hazardous areas.

5. Smoke detectors and fire extinguishers must be accessible.
6. Care must be taken to keep electronic storage media away from harmful environmental or magnetic influences. For example, a photo-magnet on a desk could damage a floppy disk or a hard drive in the same vicinity.

7. Workstation Security

JIBEI policies are intended to ensure the privacy of its employees and members, and protect their data from unauthorized, illegal, and malicious actions. The JIBEI's Workstation Security Guidelines are meant to ensure the integrity and privacy of protected health and other confidential information.

The purpose of this policy is to outline the acceptable use of workstations at the JIBEI. These rules are in place to protect the employee and the JIBEI. Inappropriate use exposes the JIBEI to risks including virus attacks, compromise of network systems and service, and legal issues.

7.1 Workstation Requirements

- All equipment used at JIBEI must be procured or approved by the JIBEI IT department. Users are prohibited from bringing in their own equipment and peripherals such as computers, laptops, monitors, keyboards, mice, speakers, etc.

- Desktop workstations and laptop computers are for business use at the JIBEI. Non-Business software should not be installed on JIBEI computers. All Software can only be installed by the IT Department.

- All PCs, laptops and workstations must use a screensaver to lock the screen when not in use. Basic instructions for locking computers can be found in Section 7.2, “Workstation Usage Guidelines”.

- All desktop and laptop computers owned by the JIBEI must be equipped with approved Info Sec Software. JIBEI Info Sec Software are up to date and protects all of JIBEI equipment. All non-JIBEI desktop and laptop computers must have a minimum of virus-scanning software with a current virus database whenever they are connected to a JIBEI computing network.
- Since information contained on portable computers is especially vulnerable, laptop users are required to comply with the guidelines set forth in Section 7.3, “Laptops”.

7.2 Workstation Usage Guidelines

- The JIBEI and its employees shall take reasonable and appropriate steps to ensure that workforce members understand which purposes and functions are authorized on their workstations. Employees are not use workstations for unauthorized purposes or to perform unauthorized functions.

- All employees must lock their computer when they leave their workstations unattended for a period of time, such as breaks, visits to the restroom, and any other time they may be called away from their workstations. Computers are locked by using keys Ctrl, Alt, and Delete keys and selecting Lock Computer. Upon returning to the workstation, employees can unlock their computer by using keys Ctrl, Alt, and Delete and logging on by using their desktop password. This will restore the screen to the exact place the user left it when he or she locked the computer. Compliance with this security measure will be monitored, as required by law.

- All employees must log off from their workstations when their shift or day is complete, but leave the workstation powered on so patches can be pushed out by the IT Department.

- All employees are required to report any unauthorized activity at a workstation to the IT Help Desk x1499.

7.3 Laptops

Laptop computers warrant special consideration because they are used off the premises of the JIBEI and are not subject to the same physical safeguards as other equipment. The Director of Administration must grant approval for a laptop being loaned to an employee.

Several security policies apply only to laptops:

- Any employee that is provided a laptop for work and data associated with the JIBEI must adhere to the following:
  The laptop, and the software and data it contains, is the property of JIBEI and must be returned upon request or upon separation from the organization.
- Laptops (in Office or Home) – cannot store sensitive JIBEI information on the hard drive of the laptop. Any sensitive JIBEI data must be stored on a mapped network drive.
- Do not install any software on the laptop.
- Do not store personal data on the laptop.
- Do not leave the laptop unattended in a public location. Do not leave the laptop in a locked car where it could be subject to theft as well as damage from extreme heat.
- You should only access JIBEI data from a wired or secure Wireless connection.
- This device should only be used in accordance with all applicable laws and JIBEI Policies and should only be used in a safe and ethical manner.
- Do not permit others to use the laptop, with the exception of instruction or

demo or JIBEI IT support staff.

- Cannot store any JIB-related data/files on home computers, USB drives or other removable media or personal cloud-based storage or file-sharing services (such as google drive, personal OneDrive, drop box, amazon drive, iCloud, etc.)
- If you need any assistance accessing JIBEI data on this laptop or if the device is not working properly, please call the IT help desk at (718) 591-2000 x1499.
- If this device is lost or stolen, immediately report this to Sanjay Patel at x1566 or the IT Help Desk at x1499.

7.4 Printer/Fax and Document Security

- Printers and fax machines used to print sensitive JIBEI data or PHI must be located in a physically secure area, or the recipient must attend the printer/fax machine during output.

- The sender must make every effort to ensure the recipient of sensitive or private data is advised when it is being sent.

- JIBEI employees must make every effort to ensure that the correct fax numbers are used. For example, information intended for the medical department should only be sent to the fax machine located in the medical department.

- At least one person in every department should be designated to collect confidential faxes several times daily.

- It is the responsibility of the person handling sensitive or confidential documents to ensure the documents are shredded or put in a secure recycling bin when being discarded.

8. Remote Access Guidelines

- Remote Access (for both JIB laptops and personal laptops/ computers)
- Only permitted as approved by Administration and CTO, and must use security tools as specified by Info Security team (such as secure remote portal and 2 factor authentication if accessing JIB network remotely)
- Cannot store any JIB-related data/files on home computers, USB drives or other removable media or personal cloud-based storage or file-sharing services (such as google drive, personal OneDrive, drop box, amazon drive, iCloud, etc.
- Laptops (in Office or Home) – cannot store sensitive JIBEI information on the hard drive of the laptop. Any sensitive JIBEI data must be stored on a mapped network drive.
- You should only access JIBEI data from a wired or secure Wireless connection.
- Do not leave any computer unlocked and unattended while remotely connected to the JIB network
- Printing PII, PHI or HIPAA data remotely is not permitted
- Remote Access of JIBEI- related data via any other means besides Pulse/Duo and MaaS360 is prohibited

8.1 Mobile Device Management (MDM)

In recent years, mobile devices have become ubiquitous for enterprise use. Businesses and their workforces rely on mobile devices like smartphones and tablets for an assortment of jobs. As working remotely has become essential, mobile devices have become an integral part of most organizations—vital tools for productivity and efficiency. Enterprise mobile devices access critical business data, they can threaten security if hacked, stolen or lost. So, the importance of managing mobile devices has evolved. With a mature MDM platform, IT and security departments can manage company data, regardless of device or operating system. It helps keep company data and networks secure while keeping the workforce flexible and productive.

Any JIBEI employee or consultant who wants to access JIBEI email and/or calendar on a mobile phone or tablet must get written approval from the Director of Administration and utilize Maas360 ("Maas"), exclusively, to access JIBEI email and or/calendar. This policy is intended to protect the security and integrity of JIBEI data and technology infrastructure. JIBEI reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

Native email clients (including but not limited to iPhone/iPad and Google Android Mail, Mail, Gmail, Outlook, Apple Mail, Inbox, Yahoo Mail, Samsung Mail, Windows Live Mail) are NOT secure, and are NOT permitted for accessing JIBEI email and/or calendar on a mobile phone or tablet.

Maas360 is a Mobile Device Management (MDM) application. It creates a secure encrypted container on the device that is isolated from all other content on the device. In addition to securing and encrypting the contents of the container, it allows IT to wipe the container if the device is lost, stolen or if the employee separates from JIBEI. It also protects the employee as IT does not have any access to anything on the device outside the Maas container.

By accessing JIBEI email and/or calendar on a mobile phone or tablet, JIBEI employees and consultants agree to the terms and conditions set forth in this policy:

- JIBEI defines acceptable business use as activities that directly or indirectly support the business of JIBEI.
- The Maas360 application may not be used at any time to:
  - Store or transmit illicit materials
  - Store or transmit proprietary information belonging to another company
  - Harass others
  - Engage in outside business activities
  - Engage in unlawful activities
- Employees may use their mobile device to access the following company-owned resources: e-mail, calendars, contacts, documents, etc. only via the Maas application
- Employees and consultants must obey all laws regarding texting or emailing while driving
- JIBEI will install Mobile Device Management (MDM) software on any device used for access to company email system, once the appropriate approval process is complete

- Employees must promptly notify IT if a phone or tablet with Maas installed is lost or stolen, and before it is traded-in, sold, given away or discarded. (Employees are responsible to notify their carrier if they want to stop service on the device)

Devices and Support

- Smartphones including iPhone, Android, and Windows phones are all supported
- Tablets including iPad and Android are supported
- Old versions of devices or operating systems may not be supported
- Connectivity issues specific to our MAAS application are supported by the IT department; employees should still contact the device manufacturer or their carrier for operating system or hardware-related issues.

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to use the MAAS MDM software to access JIBEI network.
- JIBEI password policy is discussed in detail in other sections of this information security policy.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.

9. Passwords

Passwords play an important role in our security strategy. Misuse of passwords, including negligence on the part of authorized system users, provides hackers with an opportunity to compromise the confidentiality, integrity, or availability of our systems.

Always keep your password a secret. Do not share your password with anyone. This includes your supervisor, your subordinates, and the IT staff.
No one from the IT staff will ever ask you for your password. You may be held responsible for any actions taken using your username and password.

Password security depends upon good password selection. Unauthorized access to computing systems can often be achieved through trial and error using common passwords. Select your password carefully using the guidelines for choosing a secure password in Section 9.4 "Password Confidentiality".

If you need to have your password reset, contact the IT help desk at extension 1499. If you suspect your password has been compromised, contact extension 1499 immediately.

The purpose of this policy is to outline the password parameters required and the various controls that are in place regarding system access.
These rules are in place to protect the employee and the JIBEI. Inappropriate use exposes the JIBEI to risks including virus attacks, compromise of network systems and services, and legal issues.

9.1 JIBEI Password Policies

Generally, you will have two separate and distinct passwords. One is for your desktop log-on. This enables you to log on to the various network directories used in your daily job performance. Files that are in such programs as Laserfiche, Traverse, and Filemaker are all located on the network. Your second password is for logging on to the mainframe and accessing System 2.

Employees are required to keep passwords secure and not to share accounts information with anyone, including IT staff. Where passwords cannot be a minimum of 12 characters in length, they must be changed every 45 days at a minimum.

9.2 Desktop Passwords

- Passwords must not consist of readily guessable sequences of letters or numbers, or variations of the work PASSWORD, abc123, etc.

- Passwords must be a minimum of 12 characters in length and consist at least three out of the four of the following types of characters: number, uppercase letter, lowercase letter and symbol, where possible. Create a Passphrase that is easier for you to remember but longer in length. For example, “Myfavoriteseason1sFall”, “MorecoffeePlease!”, “Ihave3greatchildrenBobTomMary”, “DoyouKnowthewaytoSanjose?”, “GoJets!GoGreen”.
- Passwords cannot be the same as the previous 10 passwords
- All accounts must be suspended indefinitely after 3 consecutive invalid log-in attempts. If you forget or lose your password, contact the IT Help Desk at extension 1499.
- Make sure you use a different password for your personal accounts than your JIB account passwords
- Do not share passwords with anyone.

9.3 Mainframe Passwords

Your mainframe password consists of 8 digits and will be automatically assigned to you every 45 days. Several days prior to the date your current password expires, you will be warned that your mainframe password will be expiring. On the 45th day, you will be assigned a new 8-digit password.
It is important that you memorize this password or write it down and keep it in a safe place that is not accessible to anyone else. If you forget or lose your password, contact the IT Help Desk at extension 1499.

9.4 Password Confidentiality

Everyone must understand the need for maintaining confidentiality of passwords. The world's best pass- word is ineffective if it has been compromised. This section defines the specific security measures related to password confidentiality.

1. A password must be treated as JIBEI confidential information at a minimum.
2. Passwords must not be posted or exposed to the view of others. Do not print your password and place it near/under your monitor and/or keyboard. Be sure no one watches you when you are entering your password.
3. A password must be changed immediately if there is any possibility that it was compromised. If you need help changing your password, please contact the IT Help Desk at extension 1499.
4. Passwords must not be written on paper or stored in a computer file unless the paper or file is stored in a place accessible only by the owner of the account(s) protected by the password.
5. Whenever possible, passwords should consist of upper- and lower-case letters, numbers, and punctuation. The password drY:(winDOw)7 is far more secure than drywindow. Also, consider using two or more unrelated words as a basis for a password. The password drY:(winDOw)7 illustrates this technique by combining dry and window with punctuation and numbers.
6. Always log off if you leave your desk – it only takes a moment for someone to steam or change your password.
7. Do not store passwords in your web browser.
8. Do not tell anyone your password. Keep your passwords safe by keeping them to yourself.

10. Email and Related Communication

10.1 Email

Electronic mail (email) is the preferred method of business communication because it is fast, inexpensive, and relatively simple to use. This method, however, is not flawless: Email is one of the leading conduits of viruses across computer networks through infected messages or their attachments.
Email is often used to spread "hoaxes" causing undue concern and insensitivity to real future threats. Email typically makes numerous stops at computers along the route to its final destination. At each stop, it can be intercepted and read by prying eyes.

- The use of JIBEI’s email system is intended for work purposes only and cannot be used for personal use. Do not use JIBEI email addresses to sign up for non-JIBEI notifications, coupons, sales, catalogs, etc.
- You cannot use personal email to conduct any JIBEI business. Do not forward any JIBEI emails to your personal email account.
- You cannot access personal email (such as Gmail, Personal OWA/ Office.com, yahoo, Hotmail, @me, etc.) from a JIB computer or laptop.

The JIBEI has taken several security measures to ensure that all email coming into the company is safe and will not harm your computer, the JIBEI, or the JIBEI's work environment. However, if you suspect any type of virus or unknown program in your email, do not open the email and report it to the IT Help Desk at extension 1499.

10.2 Junk Email (Spam)

The email gateway, which connects the JIBEI to the internet, is equipped with a spam filter to detect and delete junk email. The spam filter is effective at blocking almost all-junk email. Nonetheless, junk email may occasionally find its way into your inbox.

- Employees should be wary of suspicious-looking emails and delete any junk mail they receive without opening it. Questions about whether a specific piece of email is spam should be directed to the IT Help Desk at extension 1499.

- If a JIBEI employee receives more than a few pieces of junk email per month, it may indicate that there is a problem with that user's email settings or with the spam filter. Users who receive spam frequently should contact the IT Help Desk at extension 1499.

- Be cautious of any emails that say they are from JIBEI employees but are marked as [EXT] in the subject. (This indicates that this is coming from an external person.) Do not click on links or attachments from people you do not know. Even if you do know the sender, you should verify the following before clicking on any link or attachment: The email address next to the sender’s name looks reasonable as expected (for example it does not say from Magnacare yet the sender’s email is Bobby@gmail.com.

10.3 Social Media

JIBEI Employees may not post to Social Media any PHI data, JIBEI Financial data or other internal JIBEI data or information about internal policies and procedures. Except for LinkedIn or other professional networking, JIBEI employees are not to represent themselves as JIBEI Employees on Social Media.

11. Suspicious or Unusual Events

This chapter outlines the procedures for reporting suspicious or unusual events and describes certain events that employees should be especially aware of.

11.2 Social Engineering

While users are the most important part of any security program, they are all too often its weakest link. Criminals realize this and strive to get users to drop their guard and share information when normally they would not. Attempting to trick users into providing unauthorized access to information is called social engineering.

Social engineering scams take a variety of forms.

- Examples include email hoaxes designed to induce users into divulging a group of email addresses,
- password generators that entice users into using easily cracked passwords, or
- human insistence that technical problems require that sensitive data be sent unencrypted over the internet or through the mail.

This section discusses some of the most common social engineering scams. Employees should bear in mind, however, that this list is far from exhaustive. Criminals work hard to devise new ways to get users to divulge sensitive information or otherwise thwart security policies and procedures. Always remember that if you see or hear of something that looks suspicious, report it to the IT Help Desk x1499.

11.2.1 Pretexting

A well-designed social engineering scam can be very convincing. Hackers typically conduct research prior to running their scam and often have valid information at their disposal. Using valid information or a plausible ruse to gain access to confidential information is known as pretexting.

- For example, a hacker may try to impersonate a member (and thereby gain access to confidential information) by supplying a legitimate name, address, or date of birth to a JIBEI employee.
- Another common scheme combines pretexting with random calling. Hackers may, for instance, call random telephone numbers claiming to be following up on a technical problem.

Eventually they will find someone with a legitimate technical issue who will be asked to provide system login information so that the technician can solve the problem.

JIBEI employees should understand the nature of pretexting schemes and should follow security protocols to ensure they are not successful. In the scenarios described above, JIBEI employees should only disclose information in conformance with JIBEI policies and should not make exceptions no matter how legitimate the reason may seem. JIBEI employees should further be aware that a JIBEI help desk technicians would resolve all

technical issues. In rare cases, a help desk technician will work with an outside party, but users will always be made aware of this beforehand. Additionally, employees should remember that no one from the IT staff would ever ask them for a password.

11.2.2 Email Hoaxes

Email hoaxes are bogus emails that trick users into providing confidential information or simply attempt to gather a list of valid addresses. Email hoaxes usually come in the form of chain letters containing false or misleading information. They play on the reader's emotions, prompting them to engage in meaningless activity or worse, the compromise of personal information.

Examples of email hoaxes include:

- Prizes for taking surveys, dialing a certain phone number (#77), or forwarding emails to as many users as possible.
- Fake virus alerts or fake security updates.
- Requests to sign email petitions or to contribute to a worthy cause like disaster relief, a search fund for a missing child, or an emergency medical procedure for someone who is gravely ill.
- Fictitious warnings or news releases about the government, companies, institutions, or upcoming events.
- Promises of unlimited financial gain from making a specific investment or joining a "get-rich-quick" scheme.

If you receive what you suspect to be a hoax or an email chain letter do not respond or forward to other users and report it to the IT Help Desk at extension 1499.

11.2.3 Phishing Scams

Phishing scams are usually accomplished by sending out Phishing emails. The Phishing emails are attempting to entice users into divulging sensitive information over the internet is known as "phishing." Typically, users are sent an email message from a source, which appears to be legitimate (a well-known bank, vendor, or existing contact for example). The email usually has an email link attached or states that there is a problem with the user's account and requests that the user log on to a website or click on a link to confirm account information. This bogus website, or link is designed to look legitimate, but provides hackers with the user's confidential account information Please follow-up with the Helpdesk if you are unsure before clicking on any clink that looks malicious. **Use the "Report to IT" button under the Security Actions tab in Outlook if you receive any suspicious emails.**

Phishing emails present a serious threat to all organizations, including JIB.

Many links in emails are sent by bad actors pretending to be legitimate emails and are intended to steal your credentials, gain unauthorized access to sensitive information such as PHI or PII, encrypt JIB data and hold it hostage (ransomware), install viruses, worms or other malicious software that could compromise our systems or network, or make them unusable. **It is extremely important that you do not click on a link in an email until you have taken steps to make sure it is not malicious.**

- Hover over the "From" address in the email to make sure the from address displayed is the from address you see when you hover.
- Make sure there are no typos in the from address – this address should match the email address you have in your files for the sender. If you do not know the sender, or the email address does not match, do not click on the link.
- If an email, or link in the email, requests your username and/or password, do NOT enter it for ANY of your credentials.
- If an email is marked with EXT in the subject line, it is coming from an outside party and is not from a JIB employee, even if the email says it's from an employee.
- Especially if an email is purporting to come from a supervisor/manager at JIB, asking you to transfer funds, cut a check, email sensitive information like W2s or lists of members, do not comply without calling (or a contact method other than email) the supervisor/manager to verify the request. It is very possible an employee's or contact's email may be compromised if they are making unusual requests.

The JIB Information Security team periodically conducts "phishing campaigns" (tests). These phishing campaigns are designed to look like real phishing emails, and are intended to heighten your awareness of phishing emails, and to practice not responding and reporting these emails to IT. If you are opening and clicking links in these test phishing emails, you are not practicing safe cyber behavior – you need to review emails more carefully. There is no way to know if a test email is a real phishing email or a test. **Clicking on links in emails, without proper verification, puts the organization, and our members' data, at serious risk.**
JIBEI employees are never to provide confidential information over the internet. All sensitive information must be encrypted as described in Section 4. "Exchanging Confidential Information". Additionally, employees should be suspicious of any email message, which requests confidential information.

11.3 Reporting Suspicious Events

Employees are asked to report suspicious or unusual events. In addition to the scenarios described above, such events may include (but are not limited to) unauthorized access of the network (from both internal and external sources), compromise of sensitive data, destroying hardware or software, and malicious code such as viruses, worms or any other unauthorized software. Immediate reporting events will help mitigate any adverse impact and minimize current and future vulnerability. You should report even those events that seem trivial.

To report an event immediately, contact the Sr. Manager of Information Security or the IT Help Desk x1499. Department personnel will document the report on a Suspicious or Unusual Event Form. This form is used when you first notice a suspicious or unusual event, use the form to collect all relevant and important details.

12 Security Violations

12 .1 Identification of Security Violations

While there are many systems and logs that may reveal a security violation, vigilant employees and supervisors are our best defense. Any suspected security violation should be reported to the Sr. Manager of Information Security or to Human Resources. It is IT's responsibility to investigate whether there was an actual violation. The Sr. Manager of Information Security is responsible for these investigations. Employees of the IT Department are provided with additional IT Controls Guidelines, which include their additional roles in the identification and handling for security violations.

12.2 Tracking Security Violations

Once the IT department concludes its investigation into a suspected security violation, IT will report any actual security violation to Human Resources. HR is responsible for tracking security violations for specific employee(s) and documenting them in the employee's file.

12.3 Enforcement and Compliance

While IT will consult on the severity of a security violation, HR is responsible for any decision on disciplinary actions. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. If an employee violates this policy for the first time, he or she will be given a written and verbal warning; however, depending on the nature of the violation, a first offense can be grounds for termination. If there is a second violation, the person will be suspended from their job responsibilities and may be terminated based on the nature of the violation. The lengths of suspension will be commensurate with the severity of the incident. If this policy is violated a third time by the same individual, he or she will be terminated immediately.

The Information Security Policy applies to all users of JIBEI information, including employees, medical staff, outside vendors and consultants. Failure to comply with information security policies by employees, medical staff, outside vendors and consultants may result in disciplinary action up to and including dis- missal in accordance with applicable JIBEI procedures, or, in the case of outside vendors and consultants, termination of the affiliation. Further penalties associated with state and federal laws may apply.

Possible disciplinary or corrective action may be instituted for, but is not limited to, the following:

1. Unauthorized disclosure of Personal Health Information (PHI), ePHI, Personal Identifiable Information (PII) or confidential information.

2. Unauthorized disclosure of a user id, sign-on code, or password.

3. Attempting to obtain a user id, sign-on code, or password that belongs to another person.

4. Using or attempting to use another person's user id, sign-on code, or password.

5. Unauthorized use of an authorized password to invade patient privacy by examining records or information for which there has been no request for review.

6. Installing or using unlicensed software on JIBEI computers or laptops.

7. The intentional unauthorized destruction of JIBEI information.

8. Attempting to get access to sign-on codes for purposes other than official business, including completing fraudulent documentation to gain access.

9. Failure to lock a computer when leaving the workstation.

10. Use of a cell phone camera to photograph protected information (such as a picture of the computer screen, reports, medical claims, correspondence, etc.).

13 User Account Creation & Access

- Access to all JIBEI software is secured via passwords. Once the user account is created and the employee logs into the system successfully, access to software functionality is based on the role of the employee. The IT department sets up the credentials for the employee, based on the access requirements provided by HR or the employee's supervisor. Refer to the Access Controls Policy for more details about the guidelines for access controls. The IT Department will also adhere to the "IT guidelines for the use of Privileged Accounts" section of the IT Controls policy. Multifactor Authentication is needed when using (RDP) Remote Desktop Protocol to a server or network device

13.1 Provisioning

IT department will provision access as requested by HR, or by employee's supervisor with approval from Director of Administration. User provisioning is detailed in the "User Provisioning Procedures," found on the IT page of the Intranet.

13.2 Suspension of Accounts

When an employee is terminated, HR will notify the IT department. The IT department will promptly disable access for the terminated employee from all systems.

Table 2 Summary of Changes

Section	Date	Description
	2025	
1	6/13/25	Language cleanup
2.2	6/13/25	Added line addressing all data
2.4	6/13/25	Added word secure
3.3	6/13/25	Language cleanup
3.51	6/13/25	Sentence clarification
4	6/13/25	Added word confidential
4 Table 1	6/13/25	Update TLS Companies
5.2	6/13/25	Removal of the Usenet newsgroup reference Clarification of USB approver
10.1	6/13/25	Clarification on forwarding email
10.2	6/13/25	Language cleanup
11.2	6/13/25	Change scheme to program.
	2024	
4 Table 1	3/4/24	Update TLS Companies
4.1	3/4/24	Update ProofPoint information
5.1	3/12/24	Add prohibited file share examples.
11.2.3	4/11/24	Elaborated on risks of phishing emails.
	2023	
3.2	2/23/23	Update to Secure File Transfer
3.3	2/23/23	Update frequency of training and phishing campaigns
3.4	2/23/23	Update file transfer process
Table 1	2/23/23	Update Additional TLS Companies
11.2.3	2/23/23	Add Additional information on phishing emails
	2022	
	4/15/2022	Re-Ordered and reorganized sections
3.5	4/15/2022	Update Data Security & Confidentiality section
5.2	4/15/22	Update Prohibited Email Activities
9	4/15/2022	Update Password Policy
Table 1	4/15/2022	Update additional TLS companies
4.1	2/17/2022	Added Encryption Section
8.1	2/17/2022	Added Mobile Device Management Section

	2021	
1.1	6/4/2021	Update the URL for the security policy
2.1	6/4/2021	Added Availability
2.2	6/4/2021	Update what information needs to be protected section
2.3	6/4/2021	Added Business Associate agreement
3.3	6/4/2021	Added Roles and Responsibilities
3.4	6/4/2021	Updated system use and data ownership section
3.5	6/4/2021	Updated workstation and password requirement section
3.8.1	6/4/2021	Updated #12
3.8.2	6/4/2021	Updated #12
5.2	6/4/2021	Updated Laptop section
5.3	6/4/2021	Created Remote Access Guideline section
6.1	6/4/2021	Updated Desktop password section
8.1	6/4/2021	Updated email section
10.1	6/4/2021	Updated Identification of security violations section
11	6/4/2021	Updated User Account Creation & Access section
	2020	
1.1	2/21/2020	Updated new intranet website URL
3.8.1	2/21/2020	Updated wireless usage for employees
3.8.2	2/21/2020	Update to not send social security numbers in emails, and do not forward spam or malicious emails.
6.1.1	2/21/2020	Update password security on Desktops and have different passwords for separate accounts.
6.2	2/21/2020	Do not print passwords, log off when leaving your desk, do not save passwords in the browser, do not tell anyone your password, and change your password periodically.
6.1.3	2/21/2020	Update password security confidentiality
7.2	2/21/2020	Updated TLS vendor listing
8.1.1	2/21/2020	Update spam section
10	2/21/2020	Change the section to security violations
11	2/21/2020	Reference IT Controls Policy for the use of privilege accounts
11.1	2/21/2020	Reference User Provisioning procedure document.
	2019	
11	4/29/2019	Added User Account Creation & Access
3.8.2	4/29/2019	Added restriction on forwarding or using 3rd party email systems.
1.2	4/29/2019	Deleted section – no longer relevant
7.2	4/29/2019	Expanded section to include email encryption
2.2, 3.3, 10	4/29/2019	Added reference and definition of Personal Identifiable Information
5.2	4/29/2019	Added Laptop acceptable use policy

References

- Access Controls Policy
- Data Governance & Classification Policy
- IT Controls Policy & Procedures
- User Provisioning Procedures

ACKNOWLEDGMENT OF RECEIPT OF INFORMATION SECURITY POLICY

I acknowledge that I have received the Information Security Policy Handbook.

I understand that it is my responsibility to read and understand the policies and procedures contained in this Handbook and that if I should have any questions regarding the Handbook, I will consult Human Resources.

NAME (printed): _____

SIGNATURE: _____

DATE: _____