

TTHM Vendor Security Policy Handbook 2026

From: Ian Cerveney, Operations Director
TTHM Security & Privacy Officer

To: All TTHM Employees, Vendors and Subcontractors

The current members of the TTHM Compliance Committee (CC) are:

Ian Cerveney – Security and Privacy Officer
Erin Konz – Compliance Manager
Allison Court – Confidentiality Officer
Preston Underwood – Director of Meeting Operations

This TTHM Security Policy Handbook includes critical sections of the TTHM Security Policy. For additional details, refer to the TTHM Security Policy itself. If you have any questions, concerns or are lacking the requirements detailed in this Handbook and in the Security Policy, reach out to a member of the Compliance Committee immediately for assistance.

APPROVED ANTIVIRUS SOFTWARE

Norton Antivirus
Avast Antivirus
CrowdStrike Falcon
ESET Antivirus
McAfee Antivirus
XProtect (Mac Only)

APPROVED VPNS

Private Internet Access
Express VPN
Mozilla VPN
Nord VPN

APPROVED PASSWORD MANAGEMENT

Google Chrome
Mozilla Firefox



TTHM Vendor Security Policy Handbook 2026

NordPass

Norton Password Manager

1Password (CrowdStrike Marketplace)

ESET Password Manager

McAfee Password Manager

APPROVED HARDWARE ENCRYPTION

Bitlocker (PC)

Filevault (MAC)

APPROVED FILE SHREDDING SOFTWARE

Microsoft File Shredder (PC)

Shredo (MAC)

TTHM DATA MANAGERS & REPORTING TECHNICIANS

TTHM employees that receive, transmit or otherwise process potential PHI/PII/CI require a more stringent security environment. TTHM Data Managers and Reporting Technicians must use Endpoint Security on devices used to render services to clients that transmit Confidential Information.

Protected, Secure & Confidential Information Handling (TTHM Security Policy Definitions)

Access to Confidential Information provided by clients or event participants to facilitate TTHM outreach events and services will be granted to TTHM employees and vendors as-needed. All Confidential Information received directly or cultivated as a result of producing events or providing services must be protected in accordance with the TTHM Security Policy and HIPAA.

Confidential Information can include Protected Healthcare Information (PHI), Personally Identifiable Information (PII), Controlled Unclassified Information (CUI) and Protected Proprietary Information (PPI) provided by a client to TTHM in order to facilitate outreach.

Importantly, all Confidential Information must be protected before and during event production and/or as services are rendered. Then all digital and physical copies of that information must be destroyed within one (1) week of completion of the related event or service, except reporting data which must be destroyed within thirty one (31) days. Employee and Vendor Non-Disclosure Agreements specify this tenet of our policy.



This document is for use by current TTHM Staff only and should never be distributed outside of Telephone Town Hall Meeting.



TTHM Vendor Security Policy Handbook 2026

Security Policy Basics (TTHM Security Policy Sections 1.1, 1.2, 1.3)

The policy provides sales, executive and production staff within Telephone Town Hall Meeting (TTHM) with policies and guidelines concerning the acceptable use of TTHM technology equipment, e-mail, Internet connections, voicemail, facsimile, future technology resources and information processing.

Included are definitions of terms and roles, scope of the policy, and applicable regulations. Please familiarize yourself with the terms defined in Section 1.3 – Acronyms/Definitions.

This handbook should be considered supplemental to the full Security Policy, not a suitable replacement for reading and comprehending that policy in full. It is recommended that TTHM employees familiarize themselves with the Security Policy sections referenced in this Handbook.

Notification of Confidential Information (TTHM Security Policy Section 2.1)

TTHM Schedulers will note events and services where Confidential Information will be distributed to TTHM employees and/or vendors. Distribution of that information will be prefaced by the following notice:

Data and documents provided to facilitate this outreach event or service contain Confidential Information. Protection and subsequent destruction of this information in all physical and digital formats is required in accordance with the TTHM Security Policy, section 2.1.2.

Data Access & Removal Notes (TTHM Security Policy Section 2.1.1)

Policy - Only the Security Officer or designated individuals may authorize and grant sensitive data such as EPHI access to workforce members, technical support personnel, and other entities. The organization will define the information a user can access by granting or limiting access to systems, workstations, applications, files, records, fields, etc.

When non-workforce members require access to computers (i.e. for hardware installation, etc.), or to locations where sensitive data such as EPHI may be accessed, such entities are required to sign and date a Vendor Non-Disclosure Agreement. If a non-workforce member is intentionally provided access to sensitive data such as EPHI in order to perform a service for the organization, a Vendor Non-Disclosure Agreement must be established with the entity prior to sensitive data being disseminated.

Procedure - All access requests for current employees and subsequently for new hires must be preceded by the



TTHM Vendor Security Policy Handbook 2026

reading and signing of an Employee Non-Disclosure Agreement. All access requirements for vendors and contractors involved in event production and service delivery must be preceded by the reading and signing a Vendor Non-Disclosure Agreement, both by the vendor and by the individual(s) providing services in their capacity as an employee or subcontractor of that vendor.

The Security Officer will grant access to sensitive data such as EPHI based on the minimum amount of Confidential Information needed by each individual to complete his or her assigned tasks in consultation with management personnel. The Security Officer will either grant access to information systems him/herself or will delegate the responsibility to a designated individual (e.g., IT personnel or service provider). The Compliance Manager will maintain documentation of compliance with this policy through signed NDA's and notification of completion of required annual training.

Password Guidance (TTHM Security Policy Section 2.4)

User Account Passwords – User IDs and passwords are required in order to gain access to all TTHM/BA networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length and Complexity – Passwords/Passphrases are required to meet the following complexity requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least eight characters in length
- Contain characters from three of the following four categories:
 1. English uppercase characters (A through Z)
 2. English lowercase characters (a through z)
 3. Base 10 digits (0 through 9)



TTHM Vendor Security Policy Handbook 2026

4. Non-alphabetic characters (for example, !, \$, #, %)

Complexity requirements are enforced when passwords are changed or created.

Change Frequency – Passwords must be changed every 180 days. Compromised passwords shall be changed immediately.

Reuse - The previous six passwords cannot be reused.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are stored in an encrypted format using an approved password storage software or service.

Telecommuting (TTHM Security Policy Section 5.1)

Telephone Town Hall Meeting - TTHM is a 100% remote based organization. Telecommuting has become a required capability for many organizations, including TTHM. The advantages of telecommuting are critical for an organization such as TTHM. Telecommuting allows TTHM to work with only the best in our industry. TTHM considers telecommuting to be the primary work arrangement with its employees.

With this in mind this policy is applicable to all employees and business associates, contractors and sub-contractors who work with TTHM. It applies to all users who connect to TTHM employee or Business Associate networks, from any location.

While telecommuting is an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to TTHM employee or Business Associate networks become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. TTHM expects that the minimum standards listed below will be met by all employees and business associates of TTHM.

General Requirements (TTHM Security Policy Section 5.1.1)

All workforce and business associates are required to follow all corporate, security, confidentiality, HR, or Code



This document is for use by current TTHM Staff only and should never be distributed outside of Telephone Town Hall Meeting.



TTHM Vendor Security Policy Handbook 2026

of Conduct policies that are applicable to other employees/contractors.

- Need to Know: Users will have the access based on 'need to know'.
- Password Use: The use of a strong password, changed at least every 180 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- Contract Specific: There may be additional requirements specific to the individual contracts to which an employee or business associates is assigned.

Data Security Protection (TTHM Security Policy Section 5.1.2)

Access and Transfer: Access to and transfer of client-protected data, TTHM proprietary information (including production processes and related documents), and contract details (such as BAAs, MSAs, and SOWs) are strictly limited to employees' Google Workspace email accounts, designated Google Drive folders and Microsoft OneDrive. These are the only approved platforms for accessing and transferring such information. TTHM may modify or update the list of approved platforms at its discretion.

Any employee who accesses or transfers client-protected data, TTHM proprietary information, or other confidential client or contract details through unapproved platforms, methods, or channels will be considered in violation of this Security Policy and may be subject to disciplinary action or sanctions as outlined in Section 7.

Transferring Data: Transferring of data containing PHI/PII to TTHM requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. FTP other than through Google Workspace email, Google Drive folders and Microsoft OneDrive, may be established by TTHM and employees will be notified of any change in FTP. Employees are prohibited from circumventing established procedures when transferring data to TTHM.

External System Access: If employees require access to an external system, they should contact their supervisor. The Security and Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Employees should not send any Confidential Information (CUI, PHI or PII) via e-mail unless it is encrypted. Employees should contact the Security and Privacy Officer or appropriate personnel if they have questions/issues using email encryption.



TTHM Vendor Security Policy Handbook 2026

Non-TTHM Networks: Extreme care must be taken when connecting TTHM equipment to a public network. Although TTHM actively monitors its security status and maintains organization-wide protection policies to protect the data, TTHM has no ability to monitor or control the security procedures on non-TTHM networks.

(See Section 6.1 for details.)

Protect Data in Your Possession: Employees should view or access only the information they have a need to see to complete your work assignment. If your computer has not been set up with hard drive encryption technology, contact the Security and Privacy Officer or appropriate personnel for assistance.

Data Entry When in a Public Location: Employees should not perform work tasks that require the use of Confidential Information when they are in a public area, i.e. airports, airplanes, hotel lobbies.

Minimum Hardware Security Protections (TTHM Security Policy Section 5.1.3)

Virus Protection: Any computer connecting to TTHM must be equipped with TTHM-approved, commercial up-to-date Antivirus and Virtual Private Network (VPN) protection products.

Operating System and Updates: TTHM requires the use of supported operating systems kept up to date by automatic updates to connect to TTHM resources.

VPN and Firewall Use: Established procedures must be rigidly followed when accessing TTHM information of any type. TTHM requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Lock Screens: No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected or may contain Confidential Information. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

Multi-Factor Authentication (MFA) - TTHM utilizes Multi-Factor Authentication to access TTHM system resources. Employees and business associates are prohibited from overriding, disabling, or otherwise circumventing this critical security system.

Approved Software & Services - For a list of currently approved Antivirus, VPN, Password Management, and Hardware Encryption software and services see page one of this document.



TTHM Vendor Security Policy Handbook 2026

Required Equipment (TTHM Security Policy Section 5.1.4)

Employees and business associates must understand that TTHM will not provide all equipment necessary to ensure proper protection of information to which the employee has access. To avoid the need for a paper shredder and lockable file cabinet/safe, keep all documents digitally secure and do not print them. The following lists define the equipment and environment required by TTHM:

TTHM Provided (TTHM Security Policy Section 5.1.4.1.1)

Virus Protection

VPN Software

Hardware Encryption

File Shredding Software

Employee Provided (TTHM Security Policy Section 5.1.4.1.2)

Broadband connection and fees

Paper shredder

Secure office environment isolated from visitors and family

A lockable file cabinet or safe to secure documents when away from the home office.

Additional Employee Requirements (TTHM Security Policy Section 5.2)

Non-Solicitation Agreements - As a condition of employment, all employees are required to sign an Employee Non-Disclosure and Non-Solicitation Agreement with TTHM at the time of hire. TTHM updates its employment agreements from time to time and requires employees to sign and abide by the most current employment agreement as a condition of continued employment. This is typically provided to the employee at the time of employee's performance appraisal. Pay increases and incremental changes to other TTHM-provided benefits may be withheld for employees who do not have a signed current employment agreement on file. As outlined



TTHM Vendor Security Policy Handbook 2026

in this handbook and in the TTHM IT Security Policy, nothing in this provision changes the “at will” nature of the employee’s employment relationship.

Workforce Member Responsibility (TTHM Security Policy Section 5.2.1)

Workforce members shall be responsible for:

Ensuring compliance with privacy policies applicable to the performance of their duties;

- Participation and completion of compliance related training as outlined in Section 5.10
- Participation and completion of any supplementary compliance related training provided by the Compliance Manager (section 1.8);
- Maintaining the confidentiality of all sensitive information including protected health information;
- Assisting individuals with inquiries regarding the office's privacy policies and procedures; and
- Informing the Compliance Manager of any privacy problems as well as suggestions for enhancing privacy policies and procedures. Reports made in good faith shall not result in any retaliatory actions against a workforce member.

Additionally, all workforce members will review the organization's confidentiality statement and sign a confidentiality agreement, regarding sensitive data including protected health information that is used in the performance of their duties.

Work Performed on Personal Devices (TTHM Security Policy Section 5.12)

In the modern era it is quite common for employees to use their own personal devices to perform company business. This is referred to as BYOD (Bring Your Own Device). With this in mind, employees who use their personal devices (cell phones, laptops, etc.) to perform Company business should be aware that electronic data related to such company business is the sole and exclusive property of the Company, just as with the electronic data accessed, created, or stored on Company-issued devices, and is subject to all policies and procedures concerning Company property, including the Company’s right to demand access to that information at any time for any reason.

TTHM Vendor Security Policy Handbook 2026

This policy does not give TTHM the right to review ANY personal information stored on BYOD devices, but rather only company-related information which is not accessible by other means. If such personal device containing ANY company data or assets is lost or stolen, such an incident must be reported to the Security Officer within a 24-hour window from the data or asset loss.

1. Acceptable Use
 - a. Require use of Approved VPN
 - b. Required Use of Approved Antivirus Software
2. Permitted Devices
 - a. PC with Windows 11 Pro or newer
 - b. Android mobile device with most current operating system available for device
 - c. Apple computer with most current macOS available for device
 - d. Apple mobile device with most current iOS available for device
3. Security Threats
 - a. Phishing
 - i. Number one mobile security threat
 - ii. Email or Text that appears to be from legit source
 - iii. Contains minor spelling or address errors
 - iv. Attempting to steal credentials or other Confidential Information
 - b. Malware & Ransomware
 - i. Undetectable software created to disrupt, or gain illegitimate access to, a computer, server or network.
 - ii. Ransomware threatens to destroy data unless ransom is paid to decrypt files and restore access.
 - iii. Cryptojacking:
 1. Uses company or personal computing power to mine cryptocurrencies, decreasing a device's processing abilities and effectiveness.
 - c. Outdated Operating System
 - i. Vulnerabilities in older operating systems have already been exploited.
 - ii. Manufacturer updates often include critical security patches to address vulnerabilities that can be actively exploited.
 - iii. Keeping software up to date is crucial for staying ahead of these threats.
 - d. Excessive App Permissions
 - i. Mobile apps compromise data privacy through excessive permissions.
 - ii. App permissions determine an app's ability to access a user's device.

TTHM Vendor Security Policy Handbook 2026

- iii. Apps can be compromised, and sensitive data can be funneled through to untrustworthy third parties.

Workforce/Employee Termination (TTHM Security Policy Section 5.14)

Policy - The Security Officer will implement procedures for terminating access to sensitive data such as EPHI when the employment or contract with a workforce member ends or their assigned duties change their need to access sensitive data such as EPHI. The same will be performed if a business associate or subcontractor relationship is terminated.

The objective is to prevent access to sensitive data such as EPHI by those who are no longer authorized to access the data (i.e., they may have left the organization or have been reassigned to another position). The organization will document and provide communication of each termination to the Security Officer who will ensure that termination procedures are followed. It is important to clearly define and then document the responsibilities of designated staff members to ensure that termination procedures are carried out completely and in a timely manner.

Procedure - The Security Officer will ensure that there is timely communication from supervisors, the personnel department, and others, regarding the termination of workforce members and entities with access to the organization's sensitive data such as EPHI.

For example, when a staff member's employment is terminated, their unique identification or other means of access will be disabled so that they or someone else cannot gain access to sensitive data such as EPHI with that user ID and password. The Security Officer will also coordinate with management to ensure the termination of an individual's ability to access company emails, shared documents and sensitive data.

Sanctions (TTHM Security Policy Section 7.7)

Policy - Appropriate sanctions will be applied when workforce members (including management and officers) fail to comply with the security policies and procedures established by the organization.

Sanction policies are the penalties that would be imposed on individuals for failure to comply with the organization's security policies and procedures. The severity of a penalty is based upon the potential risk to the organization's sensitive data such as EPHI. Other considerations such as repeat offenses, intent,

TTHM Vendor Security Policy Handbook 2026

and actual impact of the violation are also considered when determining the penalties to be imposed.

Sanctions or penalties can range from verbal correction, to written reprimand, to suspension from work (for a period of time), to dismissal from the organization and/or termination of employment.

Notice of the organization's sanction policy is provided to all workforce members to ensure their understanding of consequences for non-compliance with the organization's policies. Notice is included in the confidentiality statement that each workforce member is asked to sign, as well as the Workforce Member HIPAA Training Handbook.

Procedure – When a violation of the security policies and procedures established by TTHM has occurred, the incident will be investigated by a member of the Compliance Committee, or other party that TTHM may designate. A member of the Compliance Committee or designated party will review the facts and circumstances relevant to the violation and make a determination on whether sanctions or other disciplinary action is appropriate. The sanctions or penalties will be imposed on a workforce member after taking into consideration the severity of the incident, the intent of the workforce member, and the number of prior incidents in which the individual has been involved.

Specific sanctions or penalties shall be imposed for security incidents that place sensitive data such as EPHI at risk and/or are identified as a violation of the organization's security policies and procedures. Sanctions shall be reviewed and updated, as necessary.

7.7.1 Sanction Examples

The Security Officer, Compliance Manager and other management personnel shall impose the sanction(s) that they determine to be appropriate, considering the severity of the incident, the intent of the workforce member, and the number of prior incidents in which the individual has been involved.

- A verbal reprimand shall be imposed for incidents that are deemed to be minor, and for first occurrence of an incident by an individual.
- A written reprimand shall be imposed for incidents that are a repetition of an incident, or a different incident that involves the same individual.
 - 1) Detail the specific violation
 - 2) Identify personnel involved
 - 3) Detail previous warnings related to the specific violation
 - 4) Explain expectations and timelines for improvement



TTHM Vendor Security Policy Handbook 2026

- 5) Include potential next steps for non-compliance
 - (a) Two written reprimands
 - (b) Suspension without pay
 - (i) A workforce member may be temporarily suspended from work to prevent him/her from accessing Confidential Information, for a length of time to be determined by the Security Officer or Compliance Manager. The length of the suspension will be dependent upon the type and the severity of the incident and/or the repetition of offenses by the individual.
 - (c) Termination of employment
 - (i) A workforce member may be terminated from the organization for malicious or other serious failure to follow HIPAA policies and procedures implemented by the organization.
 - (d) Date & Sign by Security Officer and Employee

Remote Work Policy for the United Kingdom (TTHM Security Policy Section 7.8)

Purpose – This defines the security requirements and responsibilities for employees authorized to perform remote work while physically located in the United Kingdom (UK) consisting of England, Scotland, Wales and Northern Ireland.

Scope – This policy applies to all employees, contractors, and third-party vendors who access company systems, data, resources or services remotely from the UK. TTHM employees, contractors and third-party vendors operating remotely from the UK must follow all applicable US laws and regulations along with all tenets of the GDPR.

Policy Statement:

Authorization - remote work in the UK is permitted for employees who have received prior written approval from their department head and IT Security Manager. (Use TTHM Remote Work Authorization Form)

Secure Access Requirements:

- All remote connections must use company-approved VPN services with multi-factor authentication (MFA).



TTHM Vendor Security Policy Handbook 2026

- The use of public internet networks to perform work tasks for TTHM or when utilizing devices containing TTHM client data, documents or resources is forbidden.
- Devices used for remote work must comply with company endpoint protection standards, including antivirus, disk encryption, and regular patching.
- Access to sensitive systems or data must be logged and monitored.

Travel and Temporary Relocation – All employees temporarily or permanently working in the UK must notify the Compliance Committee at least 14 business days in advance, providing travel dates and intended access needs.

Data Protection Compliance – Remote work from the UK must comply with applicable data protection laws. Employees must avoid storing or transferring sensitive data outside of approved systems.

Incident Reporting – Any suspected security incident while working remotely must be reported immediately to the Security team via the designated incident response method. Further actions will be determined by the Compliance Committee.

Enforcement – Failure to comply with policy standards or violations of this policy deemed irresponsible may result in suspension of remote access privileges and disciplinary action, up to and including termination.

