	Information Privacy and Security Program	No. EC.PS.04.05
		Page: 9 of 19
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

I. PURPOSE:

The purpose of this standard is to provide standards for the management of networks, applications and systems, standards for the use of encryption, data backup, configuration management, access control, and audit controls.

II. DEFINITIONS:


- A. **“Administrators”** means the individuals responsible for the technical administration of information assets, including networks, systems, applications, and databases.
- B. **“Confidential Information”** shall have the same meaning as Proprietary Information.
- C. **"Exception Request Process"** means Tenet's exception request process which documents Tenet Cybersecurity's approval or denial for any exceptions to Tenet Policy and (unless otherwise specified) shall require an annual renewal of such approval for any such exceptions.
- D. **“Proprietary Information”** means any trade secret, know-how, invention, software program, application, documentation, schematic, procedure, contract, information, knowledge, data, process, technique, design, drawing, program, formula or test data, work in progress, engineering, manufacturing, marketing, financial, sales, supplier, customer, patient, employee, investor, or business information, whether in oral, written, graphic or electronic form.
- E. A **“User”** means an individual that inputs/outputs data to/from Tenet information assets. These individuals are collectively referred to as Users, and may include, but are not limited to, employees, students, physicians, contractors, agents, consultants, clients, vendors, business partners and electronic (web site) visitors.
- F. Additional capitalized terms used herein are defined in the Information Privacy & Security Glossary of Definitions.

III. STANDARD

- A. Asset Access Controls

User access controls are required to secure access to Tenet information assets.

- 1. Access controls must include at a minimum:
 - a. A User ID and password per EC.PS.04.02 User Security and Conduct


	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

Standard;

- b. Be put in place at the network (firewalls, network login) level, system (operating system) level, and when appropriate, at the application (database) level;
 - c. Automatic Logoff;
 - d. If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session;
 - e. Remote Access, in accordance with IS.PRO.04.13 Remote Access;
 - f. Secure all individual non-console administrative access to the Cardholder Data Environment (CDE) using multi-factor authentication;
 - g. Restrictions for Vendor Support, in accordance with IS.PRO.04.11 Remote Vendor Support;
 - h. Restrictions for Individual User Dial-Up Connections (Modems); and
 - i. Restrictions for Systems Accepting In-Coming Dial-Up Connections.
2. The use of advanced technologies for identification and authentication are to be used where appropriate. The implementation of these technologies must be coordinated with the Corporate Information Security Department.
 3. Tenet information assets must not be open to “PUBLIC,” “GUEST” or “WORLD” access unless that information asset has been specified to allow public access.
 4. Programmers, administrators and other technical staff must not install “back doors” that circumvent the authorized access control mechanisms found in operating systems and/or access control platforms.

B. User ID Controls

1. Creation of User IDs for individual use is restricted to the appropriate procedures as outlined in EC.PS.04.02 User Security and User Conduct Standard.
2. Each User ID must be unique to each User.
3. Generic User IDs, User IDs not identifiable to an individual User, are not permitted, except with the following and as set forth in the IS.PRO.04.04.

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

Service Account Procedure.:


- a. Generic User IDs are permitted for network/desktop operating system access in shared environments, where:
 - (1) The operating system password does not in itself provide any access to Confidential/Proprietary Information; and
 - (2) Each User uses his/her own unique User ID to gain access to the systems and applications on that workstation.
- b. Application User IDs - A User ID employed by one information asset to access another asset (often used for batch or other processing).
 - (1) Interactive access is not allowed.
 - (2) The User ID must contain information that relates it to the name of the application (*e.g.*, S2K###), where technically feasible within the system.
- c. System User IDs - System User IDs may be either interactive or non-interactive and are used by an operating system to run the asset (*e.g.*, server, router).
 - (1) User IDs loaded by the vendor, such as root, system, field, etc.; pose a security risk; and:
 - (2) Must be disabled and/or renamed before being placed into production.
 - (3) Must be restricted to their specific job function.
 - (4) Must be documented, logged, monitored and audited on a routine basis.
4. Concurrent Logons - Networks, systems, and applications must be configured to disallow more than three concurrent logons for a single User ID, if possible. If more than three concurrent logons are required, approval must be granted through the Exception Request Process.

C. Administration of Passwords


Administrators of Tenet information assets are responsible for configuring systems under their control to enforce compliance with Tenet's password standards.

1. Password Configuration

- a. Proper configuration must include the following for all Active Directory or network/domain level passwords. Other systems technically able to comply with the requirements for accounts must also be configured as follows:
 - (1) Passwords must be at least eight (8) characters long.

	Information Privacy and Security Program		No.	EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page:		9 of 19
		Effective Date:		07-15-19
		Retires Policy Dated:		02-13-15
		Previous Versions Dated:		07-13-17; 09-16-13; 12-22-04; 11-06-00

- (2) Passwords must contain three (3) of the four (4) following characteristics:
 - (a) At least one upper-case alphabetic character (A-Z)
 - (b) At least one lower-case alphabetic character (a-z)
 - (c) At least one numeric character (0-9)
 - (d) At least one special character (e.g., “@”, “#”, “\$”, “%”, “>”, “<”, “!”, “*”, and “?”)
 - (3) Users must not be able to use one of their previous five passwords.
 - b. Passwords that are not able to meet the complexity requirements must be configured to require the strongest password possible within the system. Those systems must also be configured to access to the application by first logging into an Active Directory or network/domain password that has the strong password requirement prior to logging into the application with the less strong password.
2. Password Expiration
 - a. Passwords for all Users for Active Directory or network/domains must expire at least every 90 days.
 - b. User passwords for other systems are encouraged to be configured to expire at least every 90 days. However, that timeframe is not required if access to the application requires a login to an Active Directory or network/domain password that has the 90-day requirement. For applications meeting that criteria, passwords must be set to expire at least every 180 days.
 - c. Passwords must be changed manually when:
 - (1) The password is lost or stolen; and
 - (2) The password is provided to System Administrators or the Helpdesk.
 - d. Passwords for generic accounts approved through the IS.PRO.04.04 Service Account Procedure must be manually changed at least every 180

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

days or have approval through the Exception Request Process.


3. Password Security

Within system limitations, the following guidelines must be implemented:

- a. The number of consecutive attempts to enter an incorrect password must be limited, with excessive attempts causing the User ID to be locked until reset by the appropriate authority.
 - (1) The number of unsuccessful password attempts to be entered before the User ID is disabled must be set appropriately for the system.
 - (2) If a system does not meet the minimum requirements noted in section III.C.1., the User ID must be locked after five (5) unsuccessful attempts to enter a password.
- b. Failed login attempts must be logged in accordance with EC.PS.04.04 Activity Logs and User Monitoring Standard.
- c. Passwords must be encrypted when held in storage or when transmitted over networks. Password storage files must not be retrievable by unauthorized Users.
- d. The display and printing of passwords must be masked, suppressed, or otherwise obscured.
- e. Whenever a system has been compromised, or is suspected of being compromised, the immediate change of every password and re-verification of all User IDs must be considered.
- f. All vendor-supplied default passwords must be changed before any computer or communications system is put into production.
- g. Strong passwords/pass-phrases (*i.e.*, maximum number of characters, mixed characters and numbers) must be used with all vendor supplied default User IDs.

4. Responsibilities Concerning Passwords

Administrators and Service Desk personnel receiving requests for password changes must positively identify the individual requesting the change in accordance with the IS.PRO.04.08 Service Desk Procedures.

	Information Privacy and Security Program	No.	EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page:	9 of 19
		Effective Date:	07-15-19
		Retires Policy Dated:	02-13-15
		Previous Versions Dated:	07-13-17; 09-16-13; 12-22-04; 11-06-00


- a. Users requesting password changes must be able to prove their identity to the service desk. Verification of identity must follow the process set forth in IS.PRO.04.08 Service Desk Procedures.
 - (1) If there is reason to suspect deception on the part of the caller, the request must be refused pending further investigation. The Corporate Information Security Department must be notified in order that they may conduct an investigation.
 - (2) If the User cannot provide proper identification, THE REQUEST MUST BE REFUSED.
 - (3) An abusive, demanding or threatening User is justification to deny a password change request.
- b. The initial passwords must be valid only for the initial logon session.
 - (1) Each time a password is reset, a unique password must be provided.
 - (2) Accounts must never be created without a password or with a password that matches the User ID.

D. Encryption Control

Tenet information assets must be secured to ensure that data is not accessed or modified by unauthorized users. Administrators and Users of Tenet information assets must only use secure methods when transmitting Confidential or Proprietary Information. The following methods must be used to encrypt information that is stored and/or transmitted over un-trusted networks.

1. Email Encryption

- a. Internal or Secure Transmissions Via Email - Email is considered to be a secure transmission method when:
 - (1) the email is transmitted wholly between Tenet email addresses,
 - (2) the email and its attachments are encrypted;
 - (3) Emails transmitted from a tenethealth.com (or other Tenet managed email) address to one or more tenethealth.com (or other Tenet managed email) addresses, and no outside email addresses,
- b. External Email

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

Emails transmitted from tenethealth.com (or other Tenet managed domains) addresses to external email accounts are only to be considered secure transmissions if the following procedures are followed:


- (1) must be encrypted by using the secure email solution approved by the Corporate Information Security Department if:
 - (a) the email subject and/or body contains Confidential Information,
 - (b) the email body and/or an attachment contain Confidential Information,
 - (c) the email body does not contain Confidential Information, but at least one attachment does
- (2) in accordance with the EC.PS.04.01 Record Processing & Information Handling Standard
- (3) in accordance with the IS.PRO.04.05 Email Use Violation Procedure
- (4) Alternatively, if the email body does not contain Confidential Information, but at least one attachment does:
 - (a) the email may be sent without encryption, with the attachment protected using a Data Encryption method outlined below.
 - (b) In this case, the password or decryption key must be distributed to the recipient in a separate email, or preferably through a different means of communication

2. Data Encryption

Confidential Data must be encrypted for storage and/or transmission as required below. Refer to the IS.PRO.04.08 Device Encryption Control Procedure for more information.


a. Encryption Technologies

- (1) Proven encryption technologies that apply industry standard algorithms (*i.e.*, AES, RSA) must be used to protect data. These algorithms represent the actual cipher used for an approved application (*i.e.*, PGP, GPG, etc.).
- (2) Symmetric cryptosystem key lengths must be greater than 128 bits, while asymmetric cryptosystem keys must be of a length that yields equivalent strength.
- (3) **Password-protected files** may be used to safeguard data when proven encryption technologies could not reasonably be

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00


applied.

- (a) The use of password-protected files (*i.e.*, Excel file with password protection) instead of encryption must be approved in the Exception Request Process.
 - (b) If this method is used, the password or decryption key must be distributed to the recipient in a separate email, or separate means of communication.
- b. Data in Transit** - The transmission of data from Tenet information assets must be protected against unauthorized access and modification.
 - (1) Encryption of Confidential Information over secure transmission channels is recommended, but not required. Encryption of Confidential Information over non-secure transmission channels must be secured by using Data Encryption in accordance with this security standard.
 - (2) Secure vs. non-secure transmission channels
 - (a) Secure channels
 - (i) Transmission within the Tenet Trusted Network - Transmissions where the originating point, the receiving point, and all network paths traveled are inside a Tenet trusted network
 - (ii) Dedicated Circuits - Dedicated circuits for data transfer between a Tenet trusted network and a third party, managed with a signed Information Security Agreement between Tenet and the dedicated circuit service provider.
 - (iii) Tunnel Connections - VPN and other tunnel connections between a Tenet trusted network and a third party
 - (b) Non-secure channels
 - (i) Transmissions outside the Trusted Network - Transmissions where the originating point, the receiving point, and/or at least one network path traveled is outside a Tenet trusted network
 - (ii) Dial-up Connections - only be considered secure transmission methods if the Confidential Data is traveling using another secure transmission method noted above.
 - (3) Secure File Transfer Methods - The transmission may be considered secure if a secure file transfer method (*i.e.*, HTTPS,

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

SFTP) is used and user authentication complies with this security standard.

- a. **Data at Rest** – The storage of Confidential Data on Tenet information assets must be protected against unauthorized access and modification.
 - (1) Confidential Data must be stored on secured drives on Tenet or business partner IT-managed servers located in approved secured facilities on the Trusted Network. These are drives that are only accessible by using a password and other required User security controls.
 - (2) Confidential Data stored on servers not located in approved secured facilities must be encrypted.
 - (3) This provision includes but is not limited to application databases, network and computer databases, reporting replication servers, departmental databases and spreadsheets.
 - (3) Data cannot be stored on “public” drives (e.g. O: Drive in a hospital, H: Drive in Dallas).
 - (4) Certain Confidential Data must be encrypted, even in secured facilities. These data elements include:
 - (a) Passwords
 - (b) Full Social Security Numbers
 - (c) Cardholder Data
 - (5) PHI stored in secured facilities should be evaluated for encryption according to risk and feasibility during the risk assessment process and stored encrypted, where appropriate.
3. **Hard Disk Encryption** - The hard disk(s) of information assets must be encrypted using one of the following methods. Assets not technically able to meet this standard should follow the process detailed in the IS.PRO.04.07 Device Encryption Control Procedure.
 - a. **Full disk encryption** technologies that apply standard algorithms (*i.e.*, AES) to encrypt the entire hard disk, including the operating system, may be utilized. These solutions must include pre-boot authentication and provide complete power off protection. Cryptosystem key lengths must be at least 128 bits, but 256-bit encryption or above is recommended.
 - b. **Virtual disk encryption** technologies that apply standard algorithms (*i.e.*, AES) to encrypt a portion of the hard disk may be utilized where full disk encryption would not be feasible. If virtual disk encryption is employed instead of full disk encryption, special attention must be paid

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00


to ensure that the operating system passwords for all users meet the guidelines outlined in EC.PS.04.02 User Security and Conduct Standard. Cryptosystem key lengths must be at least 128 bits, but 256-bit encryption or above is recommended.

4. Media Encryption - All information assets must be deployed with the standard/approved software solution to encrypt data on removable media devices (*e.g.*, USB drives, CD/DVDs).
 - a. Devices must be encrypted using the solution described in the IS.PRO.04.00 Tenet Asset Security Requirements.
 - b. Assets not technically able to meet this standard should follow the process detailed in the IS.PRO.04.07 Device Encryption Control Procedure.
5. Wireless Encryption - Encryption must be enabled for wireless transmissions. Wireless transmissions are considered secure when established in accordance with this standard.
 - a. The 802.11 standard must be used as the preferred security architecture for wireless, and encryption must be enabled on all such implementations.
 - b. Where implementation of 802.11 is not feasible, WPA2 may be used to provide wireless encryption, preferably together with an application layer Virtual Private Network (IPSEC VPN or SSL VPN).
 - c. A minimum 128-bit key strength must be implemented, and unique key encryption (per individual) must be implemented instead of shared key (one for everyone) encryption.

E. Digital Certificates

Any Tenet information asset used to access Confidential/Proprietary Information over the Internet must use digital certificates to ensure confidentiality and integrity of information being transmitted over a network.

1. Certificates used must be issued by a certificate authority approved by the Corporate Information Security Department.
2. Certificates at the User end must be employed in conjunction with standard technologies such as Transaction Layer Security (TLS) to provide continuous authentication to eliminate the risk of session hijacking.
3. Access to digital certificates stored on personal computers must be protected

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

by passwords or pass-phrases. All policies for password administration must be followed. Digital certificate private keys must be 16 characters or more in length and follow the current minimum complexity standards for password creation.


F. Malicious Software Control

Administrators of Tenet information assets must configure those assets to resist and detect malicious software infection.

1. Standard Malicious Software Detection Software

The Corporate Information Security Department has determined the appropriate commercially available anti-malware (including anti-virus) software to be installed on information assets and Tenet Entities must use the designated vendor-product(s).

- a. In accordance with the IS.PRO.04.06 Patch Management Procedure, product file enhancements must be updated periodically (e.g., weekly, monthly) or when new malicious software threats are reported and supported by a new product enhancement.
- b. This software must be updated, to be kept within a supported version, as new versions or patches are released.
- c. An information asset that cannot be supported by the standard anti-malware protection program must be protected by one that can support it.
- d. Information assets that are vulnerable to malware attack or that store files for those systems that are vulnerable to attack, must have an anti-malware protection program active at all times and not be capable of being disabled by standard users.
- e. Disabling or removing anti-malware detection software is prohibited.
- f. All software media must be scanned for malware prior to installation.
- g. All assets must have a Fast and Full Scan run at regular intervals.
- h. All assets must have SMTP and FTP blocked by default.

	Information Privacy and Security Program		No.	EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19		
		Effective Date: 07-15-19		
		Retires Policy Dated: 02-13-15		
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00		

2. Core Software Protection

Anti-malware protection software must be configured to monitor and protect operating system and application software running on workstations to prevent unauthorized modifications, to include not being alterable by the user of the device.

3. Malware Scanning Logs

Malware scanning logs must be recorded and made available for review when appropriate and available.


IV. IMPLEMENTATION:

A. Tenet Entity

1. The Tenet Entity Compliance Officer, Tenet Entity Information Security Officer and Tenet Entity Management are responsible for distribution and oversight of Information Privacy and Security Program Standards at the entity level.
2. Each Tenet Entity must
 - a. Adopt this standard and where necessary develop specific written procedures in order for the Tenet Entity to operationalize this standard;
 - b. Develop appropriate methods to monitor adherence to the written procedures; and
 - c. Report monitoring activity to the Tenet Entity Compliance Officer.

B. Home Office

1. Tenet's Information Privacy/Security Office will work with the Tenet Entity Compliance Officers, Tenet Entity Information Security Officers and Tenet Entity Management to develop, maintain, and update procedures and standards for protecting the privacy of Protected Health Information (PHI) and other Confidential/Proprietary information and affording patients their rights with respect to their PHI.
2. Tenet Home Office and Tenet Regional Offices must incorporate these

	Information Privacy and Security Program	No. EC.PS.04.05
	Title: TECHNICAL CONTROLS SECURITY STANDARD	Page: 9 of 19
		Effective Date: 07-15-19
		Retires Policy Dated: 02-13-15
		Previous Versions Dated: 07-13-17; 09-16-13; 12-22-04; 11-06-00

standards into their specific policies and procedures where necessary.

- C. Exceptions - Exceptions to this standard should be approved through the Exception Request Process.

V. REFERENCES:

- EC.PS.01.00 Information Privacy and Security Administration Policy
- EC.PS.01.01 Information Privacy Security Incident Handling Standard
- EC.PS.04.00 Information Security Policy
- EC.PS.04.02 User Security and Conduct Standard
- IS.PRO.04.00 Tenet Asset Security Requirements
- IS.PRO.04.04 Service Account Procedure
- IS.PRO.04.05 Email Use Violation Procedure
- IS.PRO.04.06 Patch Management Procedure
- IS.PRO.04.07 Device Encryption Control Procedure
- IS.PRO.04.08 Service Desk Procedures
- IS.PRO.04.11 Remote Vendor Support Procedure
- IS.PRO.04.13 Remote Access Procedure
- Information Privacy & Security Glossary of Definitions
- Human Resources HR.ERW.22 Security Inspection
- Federal Information System Controls Audit Manual (FISCAM)