	Information Privacy and Security Program	No. EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page: 1 of 8
		Effective Date: 10-27-16
		Retires Policy Dated: 09-16-13
		Previous Versions Dated: 12-22-04; 11-06-00

I. PURPOSE:


Define standards of application development, operation and management to provide a stable and secure application environment. The control of software, application, and database security on all Tenet information assets is essential to maintaining data integrity.

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. **“Product Security Life-cycle Program”** refers to the Corporate Information Security Department’s program to manage the entire life cycle of a product introduced into the Tenet network
- 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. The **“Systems Development Life Cycle”** or **“SDLC,”** also referred to as the **“Application Development Life-cycle,”** is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.
- F. 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.
- G. Additional capitalized terms used herein are defined in the Information Privacy & Security Glossary of Definitions.

III. STANDARD:

All Tenet applications, whether developed internally or purchased from a third party, must conform to access configuration, integrity and functionality controls. Depending on the type of application and implementation, different processes must be followed.

	Information Privacy and Security Program	No. EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page: 2 of 8
		Effective Date: 10-27-16
		Retires Policy Dated: 09-16-13
		Previous Versions Dated: 12-22-04; 11-06-00

- A. Both new as well as upgrades to existing applications are subject to the process for review and approval for information systems and software development as discussed in Administrative Policy AD 2.01 Authorized Financial Approval Limits for Capital Expenditures and Administrative Policy AD 2.05 Authorized Financial Approval Limits for Disbursements.
- B. Applications must be reviewed by appropriate Corporate Information Systems personnel to determine if Data Sharing Review is required, and if so, if the data sharing in the project is appropriate.
- C. Based on certain qualifications determined in the aforementioned information systems approval process, Third-Party application requests must include an Information Security Questionnaire (ISQ) review by the Corporate Information Security Department and an Information Security Agreement (ISA) to be reviewed by the IT Contract Sourcing team.
- D. All new or existing applications must register with the Corporate Information Security Department's Product Security Life-cycle Program to maintain compliance.
- E. Information security must be addressed throughout the Application Development Life-cycle.
- F. The EC.PS.04.05 Technical Control Security Standard must be followed throughout the Application Development Life-cycle. In each life-cycle step (listed below) Tenet must consider:
 1. Requirements Specification: Assuring security requirements are identified and addressed in planning the application.
 2. Design and Development: Assuring the security requirements outlined in the specification process are built into the product.
 3. Testing: Assuring the testing process validates the adequacy of the security specifications.
 4. Implementation: Assuring the planned security features are implemented and not bypassed.
 5. Maintenance: Assuring the security features are maintained.
- G. The following information security issues must be considered during the application specification process.

	Information Privacy and Security Program	No. EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page: 3 of 8
		Effective Date: 10-27-16
		Retires Policy Dated: 09-16-13
		Previous Versions Dated: 12-22-04; 11-06-00

1. Security Compliance

Security issues must be addressed at the beginning of the application development process (when establishing specifications). A risk analysis must be performed on a case-by-case basis.

2. Security Functionality

Applications must have information security functionality and administrative procedures appropriate to the sensitivity of the information processed. This includes a combination of network, system and application controls. Refer to EC.PS.04.00 Information Security Policy for more information.

a. Authentication can be handled at the server level, by the application, or both. If authentication is handled at the application level, then Administrators must follow the “UserID Controls” noted in EC.PS.04.05 Technical Controls Security Standard and conform to the following:


- (1) Any transmission of passwords must be encrypted.
- (2) Passwords must not be included on system reports, including user access lists and audit trails.

b. Authorization of an authenticated User to access various resources, functions, tables, etc. must require:


- (1) The application to read the UserID provided by the authenticating entity and to link it to the appropriate level of privilege in its security table.
- (2) Levels of access to be granted on a “need to know” or “least privilege” basis.
- (3) A “segregation of duties” when specifying security controls within an application.

c. Information may be directly accessed without going through the security mechanisms provided by the applications.

- (1) Direct access to any production application or database must be highly restricted (System Administrators only).

	Information Privacy and Security Program	No. EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page: 4 of 8
		Effective Date: 10-27-16
		Retires Policy Dated: 09-16-13
		Previous Versions Dated: 12-22-04; 11-06-00

- (2) Direct access must be logged. See EC.PS.04.04 Activity Logs and User Monitoring Standard for further details.
- d. Whenever feasible and cost-effective, developers must use existing system level services for security functionality rather than incorporating such functionality into applications. Examples include operating systems, network operating systems, database management systems, and access control packages. However, if these services cannot be utilized, this functionality must be built into the application and must include application specific logging and auditing capabilities as outlined in EC.PS.04.04 Activity Logs and User Monitoring Standard.
- e. Production data must only be modified in predefined ways that preserve or enhance its integrity.
 - (1) Applications must allow the User to access, read and edit the data in a manner consistent with the User's approved access level.
 - (2) When possible, data entry formats must be restricted to ensure the data is reasonable, accurate and valid.
- f. As referenced in EC.PS.04.00 Information Security Policy, developers and system administrators must protect Tenet's information and information assets against accidental or deliberate modification or destruction. Application Integrity must be addressed through proper application of the following:
 - (1) Change Management Controls;
 - (2) Access Controls;
 - (3) Backup Controls;
 - (4) Logging and Auditing;
 - (5) Segregation of Duties; and
 - (6) Integrity Controls (integrity can be enhanced by the incorporation of check-sum or encryption technology into the applications).
- g. Developers and third parties must ensure that the message received is the same as the message sent. Messages in this context refer to

	Information Privacy and Security Program	No. EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page: 5 of 8
		Effective Date: 10-27-16
		Retires Policy Dated: 09-16-13
		Previous Versions Dated: 12-22-04; 11-06-00

both E-Mail messages and to messages between applications, servers and clients. This can be accomplished by the application of:

- (1) Digital Signatures;
- (2) Check Sums;
- (3) Encryption; and
- (4) Web based access using authentication and Transport Layer Security (TLS).

3. Software Provided by a Third Party or Developed Internally

As part of the Information Security Questionnaire Review process, third-party vendor products or vendors requesting access to the Tenet network, must be reviewed by the Corporate Information Security Department. The Corporate Information Security Department will review the application, solution and/or connectivity to ensure the it is secure and compliant with audit and compliance policies.


Both third-party and Internally developed applications should be reviewed to ensure that the software follows Tenet Information Security Policies and do not:

- a. Contain undocumented features.
- b. Contain hidden mechanisms that could be used to compromise the software's security.
- c. Modify, negate or bypass the security features of the system on which it resides, other applications or databases.
- d. Contain any alternative access methods (back doors).

H. Development

Tenet's Corporate Information Security Department must be involved in the development process to ensure that the development and production environments are physically or logically separate and the developers incorporate security functionality necessary for the particular application and its use.

I. Implementation

	Information Privacy and Security Program	No. EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page: 6 of 8
		Effective Date: 10-27-16
		Retires Policy Dated: 09-16-13
		Previous Versions Dated: 12-22-04; 11-06-00

Prior to implementation, EC.PS.04.05 Technical Controls Security Standard must be reviewed to assure requirements are met.

J. Maintenance

In accordance with the Product Security Life-cycle Program, Information Asset Administrators must periodically review the maintenance records for all systems, networks and applications under their control. Additionally, all existing and new applications and products must register with the Product Security Life-cycle Program.

1. Unnecessary Features

Features that are unnecessary in the Tenet computing environment must be disabled at the time software is installed.

- a. This paragraph does not apply to standard commercial software (Microsoft Word, Excel, etc.).
- b. This paragraph applies both to software developed specifically for Tenet by third parties or developed internally by Tenet staff.
- c. The Corporate Information Security Department is the final authority on this subject.


2. Unauthorized Access Paths

Prior to moving software that has been developed in-house to production, programmers and other technical staff must remove all special access paths so that access may only be obtained via normal secured channels. Refer to EC.PS.04.05 Technical Controls Security Standard for more information.

3. Major Application Revisions

If a change to an application or its methodology significantly alters the initial security evaluation, the product must be re-evaluated by the Corporate Information Security Department and the implementation of those revisions must meet or exceed the above noted security standards. Refer to EC.PS.04.05 Technical Controls Security Standard for more information.

K. Information Security Testing

	Information Privacy and Security Program	No. EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page: 7 of 8
		Effective Date: 10-27-16
		Retires Policy Dated: 09-16-13
		Previous Versions Dated: 12-22-04; 11-06-00

Tenet's Corporate Information Security Department and Tenet Facility Information Security Officers may periodically test the production information assets for information security vulnerabilities that may be new or inadvertently introduced.

IV. IMPLEMENTATION:

A. Information Privacy and Security Program


1. Tenet Facility WITHOUT Regional Privacy Officer

- a. The Tenet Facility Compliance Officer, Tenet Facility Information Security Officer, the Tenet Facility Compliance Committee, and Tenet Facility Leadership are responsible for distribution and oversight of Information Privacy and Security Program (the "Program") Standards at the facility level.
- b. Tenet Facility Leadership will:
 - (1) Adopt this standard and where necessary develop specific written procedures in order for the Tenet Facility to operationalize this standard;
 - (2) Develop appropriate methods to monitor adherence to the written procedures; and
 - (3) Report monitoring activity to the Tenet Facility Compliance Officer.

2. Tenet Facility WITH Regional Privacy Officer

- a. The Regional Privacy Officer, Tenet Facility Information Security Officer, Tenet Facility Compliance Committee, and Tenet Facility Leadership are responsible for distribution and oversight of Program Standards at the facility level.
- b. Tenet Facility Leadership, in coordination with the Regional Privacy Officer and Tenet Facility Compliance Committee, will create specific policies and procedures as necessary in order for the Tenet Facility to operationalize the Program.
- c. Tenet Facility Leadership will report Program monitoring activity to the Regional Privacy Officer.

3. Corporate Office (Dallas/Nashville) and Region/Market Offices

	Information Privacy and Security Program	No.	EC.PS.04.06
	Title: APPLICATION SECURITY STANDARD	Page:	8 of 8
		Effective Date:	10-27-16
		Retires Policy Dated:	09-16-13
		Previous Versions Dated:	12-22-04; 11-06-00

- a. Tenet's Information Privacy/Security Office will work with the Regional Privacy Officers, Tenet Facility Compliance Officers, Tenet Facility PIRTS, Tenet Facility Information Security Officers, Tenet Facility Compliance Committees and Tenet Facility Leadership to develop, maintain, and update policies, 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.
- b. Tenet Corporate Office and Tenet Region/Market Offices must incorporate these standards into their specific policies and procedures where necessary.

V. REFERENCES:

- Administrative Policy AD 2.01 Authorized Financial Approval Limits for Capital Expenditures
- Administrative Policy AD 2.05 Authorized Financial Approval Limits for Disbursements
- 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.04.04 Activity Logs and User Monitoring Standard
- EC.PS.04.05 Technical Controls Security Standard
- Information Privacy & Security Glossary of Definitions