	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

## I. PURPOSE:

The purpose of this standard is to provide direction on the appropriate methods to protect the confidentiality, availability, and integrity of Tenet information assets through control of User access and conduct.

## II. DEFINITIONS:

- A. “**Administrators**” mean 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. “**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.
- D. 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.
- E. Additional capitalized terms used herein are defined in the Information Privacy & Security Glossary of Definitions.


## III. STANDARD

The information Tenet uses and controls may be accessed via a variety of methods. The information might be displayed by an application, accessed via a PC, mobile device or mainframe computer, printed for viewing or inclusion in a record or accessed via the Intranet.

### A. User Privacy

Users must not expect privacy with regard to Tenet’s information assets. Any email, fax or voice-mail message that is created, sent, or received, and any file on the computer network, on local PCs, portable computers, or on disks located on Tenet property may be read or listened to at any time. *Every time a User logs on to these information assets, the User consents to such action.* Tenet expressly reserves the right to:

1. Intercept, read, review, access, and disclose all email messages;

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

2. Intercept, read, review, access, and disclose all fax communications;
3. Intercept, listen to, review, access, and disclose all voice-mail messages; and
4. Intercept, read, review, access, and disclose all computer files including, but not limited to, Internet usage and websites that have been accessed.

Email is not a private form of communication. Deleting email messages and computer files does not necessarily mean there are no copies on the network or in storage, or that the information cannot be retrieved. It is possible Tenet could choose or be compelled to produce email and computer files in litigation.

#### B. User Security Access Types

##### 1. Individual Access

Except as provided below in Section III.C.1 of this standard, access to Tenet information assets is granted on a need to know basis, to specific individuals, not entire classifications of individuals.

- a. Each request for access must be authorized by Tenet Facility Management or a delegate of Tenet Facility Management.
- b. All access to Tenet information assets must be accomplished using a unique User ID that can be traced to one single User.


##### 2. File and Directory Level Access

Sharing or assigning access to any file or directory containing Tenet Confidential/Proprietary Information must be restricted to individual Users. Establishing file access to ALL Users requires Tenet Facility Compliance Officer and Information Security Officer approval.

- a. Access must be enforced at both the User ID level (privileges) and at the file level (access lists or files privilege settings).

##### 3. Emergency Access

Access controls may have to be bypassed when an information security incident, disaster, or other emergent event occurs. Emergency Access to networks, systems or applications where Confidential/Proprietary Information may be exposed, can be granted only with the approval of Tenet Compliance Officers and Information Security Officers. Refer to EC.PS.01.05 Contingency Planning Program Standard.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

- a. Any emergency access must be logged, audited, and documented and a copy of that documentation must be maintained at the facility.
- b. Emergency access rights must be removed as soon as the emergency is concluded.

**C. Access Privileges**

Access to Tenet information assets must be authorized.

**1. Management Responsibility**

Tenet Facility Compliance Officers and Information Security Officers must approve specific written standards regarding the categories of people who are granted permission to access various types of information and reevaluate the privileges granted to certain Users of systems containing Confidential Information, as detailed below, at least annually as part of the Information Privacy and Security Risk Management process.


- a. In-scope SOX applications – all Users with the ability to edit any field, server, or database.
- b. Applications containing PHI – all Users with the ability to view, edit, and/ or print PHI.
- c. Applications containing PII:
  - (1) All Users able to view, edit, or print full SSN, full date of birth, payroll data, or human resources data.
  - (2) Users with administrative, database, or server rights to systems storing unencrypted SSN, date of birth, payroll data, or human resources data.
- d. In-scope PCI systems – all Users with access to credit card number.

**2. Revocation of Access Privileges**

Tenet reserves the right to revoke the privileges of any User at any time. Conduct that interferes with the operation of Tenet information assets, which adversely affects the ability of others to use these information assets, or which is harmful or offensive to others is not permitted and may result in privilege revocation.

**D. Unauthorized Access**

Users of Tenet information assets are prohibited from gaining access to any information asset for which they are not authorized. Users are also prohibited from damaging, altering, or disrupting the operations of any information asset. Unless specifically authorized by Tenet, Users are prohibited from capturing or otherwise obtaining passwords, encryption keys, or any other access control mechanism that could permit unauthorized access. Unauthorized access is considered cause for

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

immediate disciplinary action, up to and including termination.

1. Information Asset Penetration Tools Prohibited

Unless specifically authorized by the Corporate Information Security Department, Tenet information asset Users may not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or disrupt information assets. Examples of such tools include those that discover or ‘trap’ passwords, identify security vulnerabilities, or intercept or copy information. The unauthorized use or possession of tools of this nature is considered cause for immediate disciplinary action, up to and including termination.


E. Access Request, Modification Procedure and User IDs

Granting or modifying access to Tenet information assets requires completion of Tenet’s Electronic ID (eID) Security Request Form to ensure appropriate access is provided to each information asset User. Actions taken under a User ID and password are the responsibility of the User ID owner. User IDs and passwords must not be shared.

1. Granting Access

Systems not supported by the eID Security Request Form process must use a Security Request Form ensuring:

- a. A Security Request Form is developed and utilized for all information assets not administered by the eID Security Request Form;
- b. The Security Request Form is accurately completed and routed for processing;
- c. Access is provided only to those Users that have a need to access Tenet Information assets and that such access is limited to the minimum necessary information for the user to perform required functions (see EC.PS.02.01 Uses, Disclosures and Minimum Necessary Standard);
- d. Requested User access does not conflict with the User’s job responsibilities or with previously assigned access;
- e. The Security Request Form contains the proper approvals;
- f. The Security Request Form is routed for appropriate approval, including corporate approval if required;

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page:</b> 4 of 14
		<b>Effective Date:</b> 10-27-16
		<b>Retires Policy Dated:</b> 02-13-15
		<b>Previous Versions Dated:</b> 09-16-13; 12-22-04; 11-06-00

- g. The Security Request Form is routed to the appropriate party for processing;
- h. A copy of the Security Request Form is maintained by the system administrator responsible for establishing the access. Forms must be maintained as required by Administrative policy AD 1.11 Records Management and its Records Retention Schedule; and
- i. Timely production and review of security reports to determine if User access assigned reconciles to User access requested.

## 2. User ID Assignment Standards

The following standards apply when assigning User access to Tenet information assets:

- a. The login name must be unique. Each User must have his/her own User ID that is unique from the User IDs of other Users.
- b. A consistent naming convention must be used when entering user data for a new User ID.
- c. The initial password for the account must not be a standard password given to all new accounts. The new account password must be unique, and must not be the same as the User ID.
- d. The new account password must expire the first time it is used, requiring the User to change the password as part of the initial login procedure.


## 3. Modification Requests

Modifications to User ID access privileges must be performed as described in Section III.E.1 "Granting Access."

- a. Individuals who change their names may have their name changed on their existing user accounts, but may not have the actual User ID changed due to tracking considerations.

## 4. Special Requests

- a. Generic User IDs are generally prohibited on production systems. These include application, system, training and test User IDs. These User IDs must not be assigned without approval of the Corporate Information Security Department.
- b. Bulk User ID loads are generally prohibited without documentation.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

These include any process where multiple users are granted access to a system without following Section III.E.1. “Granting Access” process (*e.g.*, loading all risk managers into a new risk management system). Bulk User ID loads must not be performed without approval of the Corporate Information Security Department. Documentation of the bulk load must contain the following for each user:

- (1) User ID;
- (2) Full name;
- (3) Facility, department, and title;
- (4) Date User ID will be activated; and
- (5) Reason why this individual is eligible to receive access via bulk load.


## 5. Access Termination Procedure

When a User’s relationship to Tenet changes, it may be necessary to change the User’s access privileges. These changes must be accomplished timely when the User’s relationship to Tenet is being terminated.

### a. Types of User Status Change

There are five types of User status changes that require termination of access to Tenet information assets:

- (1) Voluntary terminations (User’s choice).
- (2) Involuntary terminations (Tenet’s choice).
- (3) Hostile terminations (voluntary or involuntary). These terminations may include:
  - (a) Any situation where the individual is being terminated “with cause.”
  - (b) Any situation where the individual is considered disgruntled.
  - (c) Any situation where Tenet management judges the individual would pose a threat to Tenet information assets.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

(4) Transfers

Transfers involve Users changing departments, jobs, or facilities. The User's access privileges must be reviewed and approved as part of the transfer process.

(5) Third party user terminations

The access privileges for third party Users must be terminated at the time the User's relationship with Tenet is terminated. This applies to contractors, students, physicians, volunteers, and other third parties.

6. User ID Administration

When a User ID has not been used for a period of ninety days, that User ID must be disabled, except when allowed as below:

- a. Special consideration will be given for User IDs and data that belong to employees who are on a leave of absence or extended deployment outside of their normal operating environment (and expected to return).
- b. When an eID has been approved to keep access through the eID inactivity request type.
- c. For Active Directory/ network accounts that are tied to an active account within Tenet's identity and access management system.

F. Schedule for Retention of Files

Unless the System Administration staff has received instructions to the contrary, four (4) weeks after a User has permanently left Tenet, all files held in that User's directories must be archived or deleted according to Administrative policy AD 1.11 Records Management and its Record Retention Schedule.


G. User Passwords

1. Password Use

Users who require access to an information asset storing Confidential/Proprietary Information must use a unique password. If the system or asset does not require the User to set a password, the User must set a password that complies with this procedure.

2. Password Structure

- a. Do not use your first or last name or eTenet ID as part of the password.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

- b. All user-chosen passwords must meet the password configuration standards as set forth in this EC.PS.04.05 Technical Controls Security Standard.

### 3. Recording Passwords

Users must not display or store passwords in areas accessible to others. If the password is written down, it must be disguised and retained with personal possessions at all times (*i.e.*, wallet, purse, etc.).

### 4. Password Sharing is Prohibited

Regardless of the circumstance, Users must never share or reveal passwords to anyone other than the authorized User. If a User shares a password, any actions taken under the password will be the responsibility of the authorized User.

If password security has been compromised, the password must be changed immediately and proper incident reporting procedures must be followed (EC.PS.01.01 Information Privacy Security Incident Handling Standard). Withholding information related to Information Privacy or Security incidents or compromises may subject a User to disciplinary action, up to and including termination.

### 5. Password Use by Information Systems Personnel


Information Systems may need access to Users' passwords in order to perform support/maintenance in emergency or abnormal cases. In these scenarios, *i.e.*, when deemed necessary to resolve an issue related to support, installation and /or remediation, IS uses the following process:

- a. IS informs the user regarding the support/maintenance services that will be provided using the User's User ID.
- b. IS resets the User's password and assigns a new unique password.
- c. IS performs the required support/maintenance.
- d. IS resets the User's password and notifies the User that his/her password has been reset.
- e. User changes his/her password during next logon to the system.

### 6. Automating Password Entry

Tenet information asset Users must never hard-code (incorporate)



	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

passwords into software, workstation function keys, or any shortcut procedure. However, single sign-on mechanisms that forward password authentication from one system to another are permitted.


7. Confidential Information and the Use of Different Passwords

Users may consider employing two passwords to access systems when one or more holds Confidential/Proprietary Information (*e.g.*, one password for network access and another password for patient accounting system access).


8. Advanced Authentication

Advanced or multi-factor authentication must be used for remote access to the Tenet VPN environment. When advanced authentication methods are used, the following standards should be applied:

- a. SMS Verification or a push verification must be used as standard method of two-factor authentication. Some users will also be allowed to use voice or hardware tokens, according to user type and/ or work location.
- b. Tokens - Tokens are hardware items used for advanced authentication (beyond simple User ID and password access).
  - (1)
  - (3) Users are responsible for safe handling and storage of all company authentication devices. Tokens must not be stored with the information asset that it is used to access. If a token is lost or stolen, the user must immediately report the occurrence to the Tenet Facility Compliance Officer and Information Security Officer so the device can be disabled.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

H. User Conduct

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

Tenet information assets are provided to support the achievement of Tenet's mission and objectives.

1. All authorized Users must use Tenet's information assets in support of Tenet's business objectives. Incidental personal usage is permissible at the discretion of the employee's supervisor if the use does not interfere with the performance of the User's job, the performance of the Tenet Facility or Tenet as a whole, nor does the use damage Tenet's assets.
2. All information asset Users are responsible for their conduct when using Tenet information assets.
3. Violations of Information Privacy and Security Program policies and standards may result in disciplinary action up to and including termination of employment.
4. Licensing of Computer Software

Any software added to Tenet information assets must be approved by Tenet Facility Information Security Officer and meet all software licensing requirements.


5. Portable Computers and Workstation Responsibilities

Each User of Tenet information assets is responsible for the security of their mobile device or workstation. Authorized Users of Tenet information assets must take appropriate steps to ensure these assets are not available to unauthorized persons.

- a. Workstations

Safeguards must be implemented to protect information stored on individual workstations or PCs.

- (1) Individual workstations or PCs that store Tenet information must be backed up to prevent the loss of data. While many methods exist to perform backups, the preferred method is to back up a PC or workstation to a network server daily.
- (2) Individual workstations or PCs that store Tenet information must be encrypted with the standard/approved Hard Disk and Media software solutions.
- (3) Tenet network servers are routinely copied to tape, disk, and other storage media. Even if the User has deleted it, this information may be recovered and reviewed by systems

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

administrators.

b. Portable Computers

Additional safeguards must be implemented to protect information stored on portable computers, including laptops, tablets, and, mobile devices.

- (1) While many methods exist to perform backups, the preferred method is to back up a PC or workstation to a network server daily. Users should keep information that they want backed up on their network home directory.
- (2) Individual portable computers that store Tenet information must be protected, as specified in [EC.PS.04.05 – Technical Controls Security Standard](#).
- (3) Information asset Users must take steps to minimize the opportunity for misappropriation of portable computers and the information contained on these computers. These steps include:
  - (a) Store portable computers in a secured enclosure (*e.g.*, locked drawers, locked cabinets, locked offices) when not attended by members of the entity's workforce. Laptops must not be left in docking stations or on desktops when unattended.
  - (b) Locking cables may be considered as an alternative to storing computers in a secured enclosure.


c. Modems

Unauthorized modems must not be connected to PCs, workstations or laptops. When modem use is authorized, the connection must be established in accordance with [EC.PS.04.08 Network-PBX-Transmission Security Standard](#).

6. Telecommute

Users must have Tenet Facility Management approval prior to telecommuting or accessing Tenet information assets remotely. This permission may be revoked at any time. Telecommuters must abide by:

- a. All Tenet Information Security Policies, Standards and Procedures;
- b. Tenet [Telecommuting Guidelines](#); and

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

- c. Tenet’s Remote Access Procedures (IS.PRO.13 Remote Access Procedures).

#### 7. Prohibition Against Harassment

Tenet strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Tenet prohibits the use of any information asset, including, but not limited to: voice-mail, computers, e-mail and the Internet in ways that are disruptive, offensive to others, or harmful to morale. Examples of inappropriate use of the information systems include, but are not limited to, the following:

- a. Threatening or harassing other employees.
- b. Using obscene or abusive language.
- c. Creating, displaying, or transmitting offensive or derogatory images, messages or cartoons regarding sex, race, religion, color, national origin, marital status, age over 40, physical or mental disability, medical condition or sexual orientation, or which in any way violate Tenet’s policy prohibiting employment discrimination and harassment in employment.
- d. Creating, displaying, or transmitting “junk mail”, such as cartoons, gossip, or “joke of the day” messages.
- e. Creating, displaying, or transmitting “chain letters”.
- f. Soliciting others for commercial ventures or for religious, charitable, or political causes. This includes “for sale” and “for rent” messages or other personal notices.


Employees are expressly prohibited from abusing Tenet’s information systems.

## 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 the Information Privacy and Security Program (the “Program”) Standards at the facility level.

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page:</b> 4 of 14
		<b>Effective Date:</b> 10-27-16
		<b>Retires Policy Dated:</b> 02-13-15
		<b>Previous Versions Dated:</b> 09-16-13; 12-22-04; 11-06-00

- (1) Tenet Facility Leadership will
  - (a) Adopt this standard and where necessary develop specific written procedures in order for the Tenet Facility to operationalize this standard;
  - (b) Develop appropriate methods to monitor adherence to the written procedures; and
  - (c) 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)/Region/Market
  - 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 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:


- [EC.PS.01.00 Information Privacy and Security Administration Policy](#)

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

- [EC.PS.01.01 Information Privacy Security Incident Handling Standard](#)
- [EC.PS.01.05 Contingency Planning Program Standard](#)
- [EC.PS.02.01 Uses, Disclosures and Minimum Necessary Standard](#)
- [EC.PS.04.00 Information Security Policy](#)
- [EC.PS.04.08 Network-PBX-Transmission Security Standard](#)
- IS.PRO.04.13 Remote Access Procedures
- [Information Privacy & Security Glossary of Definitions](#)
- [Tenet Telecommuting Guidelines](#)
- [Regulatory Compliance Policy COMP-RCC 4.21 Internal Reporting Of Potential Compliance Issues](#)
- [Human Resources HR.ERW.22 Security Inspection](#)

## **VI. ATTACHMENTS:**

- Attachment A: Choosing a Password

	<b>Information Privacy and Security Program</b>	<b>No. EC.PS.04.02</b>
	<b>Title:</b>  <b>USER SECURITY AND USER CONDUCT STANDARD</b>	<b>Page: 4 of 14</b>
		<b>Effective Date: 10-27-16</b>
		<b>Retires Policy Dated: 02-13-15</b>
		<b>Previous Versions Dated: 09-16-13; 12-22-04; 11-06-00</b>

Attachment A  
EC.PS.04.02 User Security and Conduct Standard  
Page 1 of 1

## CHOOSING A PASSWORD

Unique passwords can be created by following these guidelines:

- String several words together (these passwords are also known as "pass phrases"). An Example: IAmFast1.
- Transform a regular word according to a specific method, such as changing a letter to a number reflecting its position in the word. An example: Applesauce becomes 1Pplesauce.
- Combine punctuation or numbers with a regular word. An example: texas = Tex1\_2as.
- Create acronyms from words in a song, a poem, or another known sequence of words. For example, the phrase "I Like To Eat Ice Cream in February," becomes: ILTEiCi2 with the use of the number "2" for February.
- Combine a number of personal facts like birth dates and favorite colors "09Red14Blue56."

Do not use passwords that would be easy to guess or crack, including:

- Passwords that are identical or substantially similar to the User ID to which it is assigned;
- Passwords that are identical or substantially similar to passwords used within a twelve (12) month period;
- Any part of your name, a spouse's name, or children's names;
- Any part of your street address (street, town, house number, zip code) or your home, work, pager or cell phone numbers;
- Any of your family's social security numbers or birth dates;
- Single words found in a dictionary, including proper names, geographical locations, common acronyms, and slang (computer programs can be used to search single word or common passwords); and
- Common character sequences such as "123456" or same digit or letter such as "AAAA" or "11111."