Information Systems Procedure	**No.**	**IS.PRO.04.11**
Title:	**Page:**	**1 of 7**
	Effective Date:	**11-16-16**
REMOTE VENDOR SUPPORT	**Retires Procedure Dated:**	
	Previous Versions Dated:	

I. PURPOSE:

The purpose of this procedure is to outline the security requirements for Tenet administrators who control access to Tenet systems by vendors or other authorized third parties for support purposes. The controls and requirements contained within may not represent the current configuration of the Tenet network. These controls are provided to codify the security requirements and facilitate adoption of a secure future state. These requirements are designed to minimize the potential exposure to Tenet from damages which may result from unauthorized use of Tenet resources. Damages include the exposure of confidential information, damage to public image and damage to Tenet internal systems.

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. A "**Gateway Broker**" refers to an application that enables an individual to operate a computer from another computer over the internet. It may also be referred to as third-party remote access support tools or interactive remote support tools.

D. An "**Information Asset**," "**Resource**," or "**Asset**" is, without limitation, any computer, network, electronic file, record, service, hardware, software, regardless of type or media that is purchased by, owned by, leased to, contracted by operated by, used by or controlled by Tenet. This is to include ALL data residing in, or generated by those resources regardless of its format or storage device.

E. "**Multifactor Authentication**" or "**MFA**" is a method of access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism.

F. "**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.

G. 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, consultants, clients, business partners and electronic (web site) visitors.

H. A "**Vendor**" refers to an individual, third-party or company that provides or performs certain functions, activities, or services to Tenet and requires access to internal infrastructure to provide support. These individuals are collectively referred to as Vendors, and may include, but are not limited to contractors, subcontractors, agents, third party vendors, and business associates.

I. Additional capitalized terms used herein are defined in the Information Privacy & Security Glossary of Definitions.

III. PROCEDURE:

This set of requirements must be applied in addition to existing controls, and does not replace existing policies and/or standards. These requirements must be clearly communicated to vendors prior to granting them remote access to Tenet resources. Users are obligated to report instances of non-compliance to the Corporate Information Security team.

The key security controls required to secure Tenet resources when using third-party remote support tools are outlined below.

A. Common Security Controls

1. Remote authentication to the Tenet network must be made with multifactor authentication (MFA). When deploying new technologies, Tenet administrators must mandate that multifactor authentication be used for any remote gateway access provided as a service.

   In the event that implementing MFA is not possible, some mitigating technical controls must be applied. Appropriate controls could include:

   a. Network Segmentation based on user, group or device profiles.

   b. Regular reviews of user groups, roles and access via single factor authentication.

   c. Enhanced logging and alerting of activity on systems which support single factor authentication.

2. Granting Access

   a. Where there is a business requirement, third-party service provider access requests must be submitted and approved in accordance with EC.PS.04.02 User Security and User Conduct Standard and EC.PS.04.05 Technical Controls Security Standard.

   b. Remote vendor's access rights must be limited to the minimum services required, following the principle of least privilege. If a

Vendor does not specifically require remote access to sensitive data, systems or networks, then they should not be granted such access.

c. Periodic reviews of remote access permissions must be carried out to ensure that this procedure is enforced. The review must include a review and removal of access to resources that vendors or groups may no longer require. Refer to EC.PS.02.01 Uses, Disclosures and Minimum Necessary Standard for more information.

3. Privileged Accounts

a. Privileged or administrator accounts must only be given to remote access vendors with appropriate justification and on an exception basis only.

b. Access must be given only on systems required and must be periodically reviewed. The Corporate Information Security team can provide guidance to this on a case by case basis.

4. Traffic Inspection

Where possible, remote access technologies used must support authentication, authorization and accounting and must allow decryption and inspection of traffic, in support of legal and regulatory requirements.

5. Audit Logging and Monitoring

a. Where possible, all relevant logs from remote access connections must be logged and processed by the Tenet security event manager.

a. These security events must be reviewed on a regular basis for possible security violations.

6. Password Policy

All remote access users must adhere to password standards in accordance with EC.PS.04.02 User Security and User Conduct Standard and EC.PS.04.05 Technical Controls Security Standard.

B. Gateway Brokered Security Controls

Vendors may ask Tenet users to establish a gateway-brokered remote access session in order to provide remote support. A typical characteristic of interactive/gateway brokered connections is that the remote party has access to or visibility of the Tenet users logged in session. This potentially includes all data and systems that a Tenet user has permission to access. Particular care is needed when Tenet users with administrator or privileged accounts allow remote support to connect to their logged in session.

1. Session Control Requirements

   a. Persistent remote access must only be allowed from Tenet managed devices. Exceptions need to be approved by the Corporate Information Security team. Please refer to IS.PRO.04.13 Remote Access Procedure for additional details regarding persistent remote access controls and requirements.

   b. Unattended Access is prohibited.

      (1) A user is required to be present at the physical computer, and must explicitly accept the remote connection request only from trusted third parties offering remote support.

      (2) When sharing a screen, the Tenet user should maintain control of the desktop. Actions that need to be carried out shall be communicated to the Tenet employee by the vendor who has "view only" access to the session.

      (3) Users and/or vendors must not install, use or configure a remote access tool which allows unattended access.

   c. Unique User Identifier

      (1) Each login session must uniquely identify the remote support user.

      (2) Vendors must not share their user account credentials.

   d. Identity Validation

      (1) Users must not grant access to a vendor without confirming their identity. Ensure that only remote support vendors authorized to connect to Tenet resources are permitted to do so.

      (2) Do not accept unsolicited phone calls or emails purporting to be from a trusted vendor or partner.

      (3) Refer to the EC.PS.04.02 User Security and User Conduct Standard for more information.

e. Disclosure of Passwords or Access Keys

(1) Some remote support tools allow the remote user to connect by using the local user's Active Directory credentials. Users must never share their password with vendors for use remotely.

(2) If an application or service requires entry of the Tenet user's credentials, the Tenet user must enter the credentials themselves.

f. Activity Monitoring

(1) If the vendor needs to remotely manage control of an end-user computer using a remote access tool, the end-user must actively monitor the support person's activity.

(2) If the support person is observed performing any unnecessary task, the end-user must immediately disable access and the incident must be reported in accordance with EC.PS.01.01 Information Privacy Security Incident Handling Standard.

2. Technology Control Requirements

a. Remote Access Tools

(1) Only the use of Tenet approved remote access technologies and tools are permitted.

(2) Remote access software and services must be licensed and supported commercially.

(3) Remote access software and services must be at current software versions and updated when patches are made available by the manufacturer.

(4) Gateway-Brokered or interactive technologies tools must not be configured with any settings that prevent the Users' workstation from locking its screen.

(5) No off-shore gateway brokered connections for remote support tools are permitted.

(6) No freeware/shareware software or services for remote tools are permitted.

(7) The Corporate Information Security team may remove or block access to a particular tool or website at their discretion.

b. Data Loss Prevention. Be aware that most Gateway-Brokered remote access tools contain some form of file transfer capability.

(1) Users must ensure that the remote vendor does not copy data to the clipboard or transfer data to their own computer.

(2) Where possible, access to remotely “copy” or “cut” data must be disabled by default.

c. Network Connectivity

It is not permitted to connect to the guest wireless network or other unsecured networks for the purposes of permitting remote vendor support access to Tenet systems.

3. Requirements for Vendor Networks and Devices

As a condition of gaining access to Tenet’s networks, vendors must secure their own connected systems in a manner consistent with Tenet requirements. Refer to EC.PS.04.08 Network-PBX-Transmission Security Standard and IS.PRO.04.00 Tenet Asset Security Requirements for more information.

C. Exceptions

Exceptions to this procedure must be documented and submitted for approval through the Corporate Information Security and Compliance Exception process. All exceptions are reviewed annually by the Corporate Information Security team.

D. Compliance

The Corporate Information Security team will verify compliance to these controls and requirements through various methods, including business tool reports, internal and external audits, and device interrogation by a Network Access Control (NAC) system, SSL interception and other technologies.

IV. REFERENCES:

- EC.PS.01.00 Information Privacy and Security Administration Policy
- EC.PS.01.01 Information Privacy Security Incident Handling Standard
- EC.PS.02.01 Uses, Disclosures and Minimum Necessary Standard
- EC.PS.04.02 User Security and User Conduct Standard

- EC.PS.04.05 Technical Controls Security Standard
- EC.PS.04.08 Network-PBX-Transmission Security Standard
- IS.PRO.04.00 Tenet Asset Security Requirements
- IS.PRO.04.13 Remote Access Procedure
- Information Privacy & Security Glossary of Definitions