ITACS Inc. Remote Access Policy

Darin Bartholomew

Matthew Dampf

Ed Gudusky

Mel Miro

Julien Rossow-Greenberg

1. Overview

The ability to gain access to our ITACS Inc. network from any location is a vital component to making our organization one that is able to operate 24/7 365 days a year regardless of outside circumstances. This policy will express all hardware, software, network and procedural requirements to obtain and use an off site connection to the ITACS Inc. network and services.

2. Purpose

This policy defines standards for connecting to any of ITACS Inc. networked resources using remote access technology from a company issued laptop. By adhering to this policy as an organization it is our goal to reduce the organization's risk that is incurred when giving access to our systems to hosts on foreign networks. Given the sensitive information housed by ITACS Inc. and the regulations in our industry this policy is a vital piece to keeping us in compliance and preventing confidentiality of data.

3. Responsibilities

It is the responsibility of the ITACS Inc Information Technology office and Technology Support team to ensure that the organization is able to operate efficiently at all times regardless of where employees are. It is also the employee's responsibility to protect the security and integrity of the ITACS Inc systems and information. This policy, if adhered to, will allow everyone to fulfill these responsibilities.

4. Scope

The ITACS Inc. Remote Access Policy applies to authorized users who use a device connected on a network other than ITACS Inc's network and need access to systems and applications located on ITACS Inc's internal network. The moment a device gains access to

our network, that device and user are expected to be in compliance with this policy. Any type of activity while connected to the network is covered by this policy and every instance of remote access on the network is covered by this policy.

5. Policy

5.1 Dedicated remote access servers will be used for all external access and for HIPAA resource access; both must authenticate external connections using a reliable and accepted access control.

5.2 Connecting to ITACS Inc. systems from any off site location will require a Virtual Private Network (VPN) account and their system configured with approved VPN software. This VPN software will authenticate to the organization's dedicated remote access server. Once connected, the user should treat the connection with the same level of importance as any on-site connection that is made using organization owned equipment. This means maintaining the same level of security that would be standard while on site.

5.2.1 While accessing resources using VPN, downloading and storing files locally is prohibited. Cache and temporary files should be cleared after terminating the Citrix VPN session. Confidential information must not be stored on the local device under any circumstance. Data of such nature can only reside on encrypted drives or encrypted cloud storage.

5.3 The approved VPN software for this organization is from Citrix. Any attempt to use other software or services (e.g. VNC, LogMeIn, Nortel, etc…) will be denied by the network firewall.

5.4 If a user requires special accommodations for data privacy on site (for example, a screen privacy cover) the same accommodation should be made at the off site location.

5.5 Under no circumstance should a device connected to ITACS Inc be left unattended while connected to the network. Only users with a valid access ID are allowed to remotely access the network or use a machine connected to the network. The VPN session will be automatically terminated by the Citrix VPN software if it detects inactivity for more than 60 seconds.

5.6 While connected to the network off site all authorized users are required to still maintain compliance with the acceptable use policy (Technology Support policy 3.56).

5.7 All requests for remote access must be approved by Information Security. As there are multiple systems, access will be granted by Security Group membership and based on specific need.

5.7.1 General Access - Accessing non-restricted company applications should be completed using standard employee credentials. If accessing secure subnets and network resources, an additional RSA dual factor authentication will be required.

5.7.2 IT Administrator Access - If system or network administrators require a full VPN tunnel, a full VPN tunnel with RSA dual factor authentication can be provided.

5.7.3 Vendor Access - External vendors may be provided access as long as the vendor is sponsored by an authorized employee. A vendor account will have limited access and requires authentication through a separate vendor VPN address.

5.7.4 HIPAA Access - Any employee requiring access to systems residing on a HIPAA network will authenticate to a protected remote access server that conforms to HIPAA policies.

5.8 Both Citrix VPN and RSA software will only be available for installation to laptops issued by ITACS Inc. This guarantees that all computers accessing the network are secured, and up to date with the latest software patches and antivirus definitions.

5.9 Any connection to the ITACS Inc. network must be encrypted and in line with the data encryption policy (3.4). This is completed by using the approved Citrix VPN software.

5.10 Passwords are required to comply with the password standards and renewal policy (3.2).

5.11 The public network used to connect into the ITACS network must have a password and secured with at least WPA2 encryption.

5.12 If an authorized user is made aware of a security breach on a device used for a remote connection the user is required to report this breach via the portal within 24 hours of

learning of the breach. Reporting is required even if the device was not currently connected to ITACS Inc.'s network.

6. Policy Compliance

6.1 All remote access network traffic will be monitored like on-site access to look for irregularities on the network.

6.2 The Chief Information Security Officer is responsible for enforcing this policy.

6.3 Remote access permissions will be audited every two years to limit access to only those who need it in current roles.

6.3.1 If an employee is terminated or willfully leaves the organization, their remote access capability will automatically be removed as their account will be disabled.

6.4 Any exception to this policy must be granted in writing by the CISO and receive two endorsements from within the network administration team.

6.4.1 All exceptions to this policy must have a termination period no longer than a year from first acceptance.

6.4.2 Exceptions may be renewed after receiving proper review.

6.5 Anyone found to be in violation of this policy will face the suggested remedies in the acceptable use policy.

6.6 If a violation occurs with an authorized user who is associated with ITACS Inc. but not employed by ITACS Inc. it will be discussed with the user's organization.

7. Related Standards, Policies and Processes

It is suggested that all remote access users read and understand the following policies before requesting remote access. These policies directly relate to scenarios that will be faced by remote users.

data encryption policy

password standards and renewal policy

acceptable use policy

off-site work policy

guest access policy

8. Review Schedule

In an effort to ensure that ITACS Inc. is constantly in compliance with all regulations and best practices in our industry it is recommended that this policy be reviewed at a minimum of yearly as a part of our annual audit of IT processes and policies. Any change or review of this policy should solicit advice from end users to ensure clarity in communication and practicality of the policy.

9. Revision History

Policy implementation – June 2013

Added review schedule – June 2014

Updated to include clearer language in scope as suggested by HR – October 2014

Added reference to new RA hardware and software configuration policy – October 2015