ITACS Inc. Remote Access Policy Audit Plan

Darin Bartholomew
Matthew Dampf
Ed Gudusky
Mel Miro
Julien Rossow-Greenberg

Overview

The ability to gain access to your ITACS Inc. network from any location is a vital component to making your organization one that is able to operate 24/7 365 days a year regardless of outside circumstances. Using the following audit plan will ensure the proper implementation of the Remote Access Policy and proper adherence to every control procedure that is outlined in the policy.

Purpose

The Remote Access Policy Audit Plan is in place to properly test and review the Remote Access Policy. The audit plan goes through every objective of the remote access policy and explains how to properly ensure that the objectives are being met while achieving the desired outcome. The audit plan requests several types of evidence to support each objective and asks the question "are the controls adequate?" By having this audit plan it ensures that your Remote Access Policy continues to protect our network and the valuable data within our company.

Responsibilities

It is the responsibility of the ITACS Inc Information Technology office and Technology Support team to ensure that this policy is properly reviewed once a year, per the policy. The Chief Technology Officer should have the final review and sign off of the audit before closing the cycle of audit. Prior to the report going to the CTO it is the responsibility of the auditor to finalize the documentation and get sign off from a member of the IT service staff who support the policy.

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 your 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. This audit plan covers every part of this policy as well as the relevance of the connections between this policy and associated policies for passwords and encryption.

Audit Objective	Control Activities	Evidence of Control Effectiveness	Control Adequacy Assessment
Ensure PC is secure before connecting remotely	Only company issued laptop is allowed to connect	• Software not made available for download by users	• Adequate. Users can't install software on unauthorized machines
	PCs kept up to date by IT department	• WSUS server logs of deployed OS updates • SCCM logs of application patches deployed • VPN logs of all machines that have connected remotely; compare with WSUS and SCCM logs to ensure that each PC on VPN list also appears on the other two lists. • Managed antivirus server logs	• Potentially inadequate. Remote access policy does not officially allude to policies regarding maintenance of OS, application and antivirus patches. We need to see the policies in this area to determine adequacy.
	Strong passwords required	• Password policy documentation • Server logs of password changes • Attempts by auditors to change password to something non-compliant	• Adequate. Ensures that laptop can't easily be accessed and used to connect remotely in the event of a lost or stolen laptop.
Ensure secure connection between remote PC and internal network	VPN is required to connect remotely	• Attempts by auditors to connect without VPN • Citrix VPN software not made available for download by users	• Adequate. VPN should always be required to prevent man in the middle attacks.
	VPN access only made available to certain users	• Group policy (GPO) documentation showing which users are allowed to connect • Firewall logs that show which rules apply to those in the VPN organizational unit (OU)	• Adequate. This ensures that no user has unnecessary access that could threaten the network.

	Two factor authentication required	• RSA software installed by IT department on eligible laptops • Software not made available for download by users • RSA tokens should only be issued by Information Security	• Potentially inadequate. RSA software resides on the same laptop as the Citrix VPN client, making it necessary to compromise only one device to access both forms of authentication. Consider using additional device for second factor of authentication, such as smart card or text message.
	HIPAA access further restricted	• HIPAA data on its own network • Different OU of users that are allowed to access HIPAA network • Separate VPN tunnel for HIPAA users	• Adequate. Regulatory statutes require this data to be kept separate.
Ensure secure usage behavior by employees	VPN Usage Policy	• Employees must agree to policy before access is granted. This is completed via an online digital signature • Policy is documented and available on the company website	• Adequate. Policy is available and agreement is mandatory.
	Prevent usage by persons other than authorized employee	• Logout due to inactivity enabled, configured to a low period of time on the VPN server • VPN account tied to single sign-on, which is only known to employee • Only allow single sessions • Multiple sessions should send email notification to Information Security • Employee termination policy ensures access is revoked upon dismissal	• Adequate. These layered controls mitigate the same threat in several different ways.