Communication Equipment Security Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0Purpose

This document describes requirements for communication equipment security configurations of <Company Name>.

2.0Scope

This policy applies to all communication equipment that is part of the data network of <Company Name>.

3.0Policy

The security features necessary to minimize risks to communication equipment must be configured in the equipment before it is placed into service. There are two possible roles for the staff that manages the communication equipment: monitoring and administrator. The monitoring role has read only privileges. The administrator role is able to change configuration parameters. All issued commands by users will be recorded, as well as any other security events that may pose a threat to the equipment.

3.01Authentication and Authorization

Local users are not allowed on communication equipment. Everyone must authenticate through the central repository of users using a protocol that reduces the risk of identity theft.

3.02Encrypted transmission

All information transmitted from the device must be encrypted by a strong crypto algorithm to minimize the risks of eavesdropping communications and man-in-the-middle attacks.

3.03Accounting

The events recorded by the communication equipment must be kept in storage media that is subject to a regular backup process. The process of maintaining these backups must ensure that the information is not amended.

3.04Access to the Password of the Communication Equipment's Administrator User

The password of the communication equipment's administrator user must not be known by anyone on the staff that manages the equipment. If, for any reason, it is necessary to make use of the highest administrative privileges within the device, then the staff must file a request to the internal security division for the password,

attaching the justification for its use and completing the required forms. The password must then be reset by the highest administrator to maintain security.

4.0Enforcement

A regular audit of the configuration of communication devices is required. If any abnormality is found in the equipment, investigations of staff who manage the equipment will be performed, and violation shall be punishable in accordance with <Company Name>'s current policies.

5.0Definitions

Strong crypto algorithm: Crypto algorithm which is not possible to break in a reasonable amount of time using a reasonable amount of computing resources.

Eavesdropping communications: Technique used to listen to communications without being able to modify any of the exchanged messages.

Man-in-the-middle attack: Attack where the hacker can control and modify the messages exchanged between the parties involved.

Encrypted transmissions: Transmissions that are made using a crypto algorithm so there can be no effective eavesdropping to communications or man- in-the-middle attack.

6.0 Revision History

6/29/2009 – Version 1.0 Manuel Humberto Santander Peláez