Communications Equipment Policy

Free Use Disclaimer: This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.

Things to Consider: Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the policy for your organization

Last Update Status: Retired

1. Overview
2. Purpose
This document describes requirements for communication equipment security configurations of <Company Name>.

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

4. Policy
4.1 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.

4.2 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.

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

4.4 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.

4.5 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.

5. Policy Compliance

5.1 Compliance Measurement
The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions
Any exception to the policy must be approved by the Infosec Team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes
None.

7 Definitions and Terms
The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Eavesdropping
- Man-in-the-middle Attack
- Strong Encryption

8 Revision History

<table>
<thead>
<tr>
<th>Date of Change</th>
<th>Responsible</th>
<th>Summary of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec 2013</td>
<td>SANS Policy Team</td>
<td>Converted to new format and retired</td>
</tr>
</tbody>
</table>