Analog/ISDN Line Security Policy

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Retired*

1. Overview

See Purpose.

2. Purpose

This document explains <Company Name> analog and ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

3. Scope

This policy covers only those lines that are to be connected to a point inside <Company Name> building and testing sites. It does not pertain to ISDN/phone lines that are connected into employee homes, PBX desktop phones, and those lines used by Telecom for emergency and non-corporate information purposes.

4. Policy

4.1 Scenarios & Business Impact

There are two important scenarios that involve analog line misuse, which we attempt to guard against through this policy. The first is an outside attacker who calls a set of analog line numbers in the hope of connecting to a computer that has a modem attached to it. If the modem answers (and most computers today are configured out-of-the-box to auto-answer) from inside <Company Name> premises, then there is the possibility of breaching <Company Name>'s internal network through that computer, unmonitored. At the very least, information that is held on that computer alone can be compromised. This potentially results in the loss of millions of dollars worth of corporate information.

The second scenario is the threat of anyone with physical access into a <Company Name> facility being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted networking of <Company Name> through the computer's Ethernet connection, and then call out to an unmonitored site using the modem, with

the ability to siphon <Company Name> information to an unknown location. This could also potentially result in the substantial loss of vital information.

Specific procedures for addressing the security risks inherent in each of these scenarios follow.

4.2 Facsimile Machines
As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.
- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a centralized administrative area designated for departmental use, and away from other computer equipment.
- A computer which is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

Waivers for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request.

Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- When in use, the computer is to be physically disconnected from <Company Name>'s internal network.
- The line will be used solely for <Company Name> business, and not for personal reasons.
- All downloaded material, prior to being introduced into <Company Name> systems and networks, must have been scanned by an approved anti-virus utility (e.g., McAfee VirusScan) which has been kept current through regular updates.

4.3 Computer-to-Analog Line Connections
The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within <Company Name> will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to <Company Name>, and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case by case basis.
Replacement lines, such as those requested because of a move, fall under the category of "new" lines. They will also be considered on a case by case basis.

4.4 Requesting an Analog/ISDN Line

Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to Telecom:

- a clearly detailed business case of why other secure connections available at <Company Name> cannot be used,
- the business purpose for which the analog line is to be used,
- the software and hardware to be connected to the line and used across the line,
- what external connections the requester is seeking access.

The business case must answer, at a minimum, the following questions:

- What business needs to be conducted over the line?
- Why is a <Company Name>-equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?
- Why is <Company Name>'s current dial-out access pool unable to accomplish the same tasks as an analog line?

In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:

- Will the machines that are using the analog lines be physically disconnected from <Company Name>'s internal network?
- Where will the analog line be placed? A cubicle or lab?
- Is dial-in from outside of <Company Name> needed?
- How many lines are being requested, and how many people will use the line?
- How often will the line be used? Once a week, 2 hours per day...?
- What is the earliest date the line can be terminated from service?
- The line must be terminated as soon as it is no longer in use.
- What other means will be used to secure the line from unauthorized use?
- Is this a replacement line from an old location? What was the purpose of the original line?
- What types of protocols will be run over the line?
- Will a <Company Name>-authorized anti-virus scanner be installed on the machine(s) using the analog lines?
- The requester should use the Analog/ISDN Line Request Form to address these issues and submit a request.

5 Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, 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

None.

8 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Converted format and retired.