Rogue Device Detection Procedure

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX..

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Procedure Statements 4

2.1 Network Access Control Statements 4

2.2 Network Access Control Setup (IT Administrator) 4

2.3 Network Access Control Monitoring (ISO) 4

3. Procedure Compliance & Enforcement 5

3.1 Compliance Measures 5

3.2 Enforcement 5

4. Glossary / Acronyms 6

4.1 Glossary / Acronyms 6

5. Document Management 7

5.1 Document Revision Log 7

5.2 Document Ownership 7

5.3 Document Coordinator 7

5.4 Document Approvers 7

5.5 Distribution 7

# Introduction

## Document Definition

This document is a Procedure.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Objective

The objective of this procedure is using a Network Access Control solution to

* discover all devices on the network, and then fingerprints and profiles them so the IT administrator has a global view of what is on the network.
* Enforcement: There will be times when an unauthorized device or user attempts to connect to the network. When this happens, the NAC solution can automatically disconnect the device. There is also an option to quarantine the device until an investigation is done to determine if the device was supposed to be authorized and why it was exhibiting unauthorized behaviours.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This procedure applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This procedure applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Procedure Statements

## Network Access Control Statements

* The NAC server: this is the link between the user database and enforcement points and ties it all together with security policies.
* The enforcement points: the network devices, such as routers, switches, firewalls, SSL VPN gateways, and wireless access points. These devices ultimately allow or don’t allow a user to access XXXX network.
* The user database: this contains a list of all the authorized users and the various groups they belong to. This can be the Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) server.

## Network Access Control Setup (IT Administrator)

1. Install the NAC server and configure all wireless access points and switches to use the NAC server for authentication.
2. Define basic profiling and authentication rules on the NAC server. This determines which resources certain users and devices have access to.
3. Define inspection and compliance policies (i.e only XXXX approved systems can connect to the network). These dictate the security posture checks.
4. Always test and fine-tune the rules and policies.
5. Define alerts and reports, such that failed authentications are logged and sent to information security officer (ISO) for analysis. Weekly reports should be generated and are useful to see trending data.

## Network Access Control Monitoring (ISO)

1. Receive daily alerts from NAC device and investigate any unauthourised access
2. If discovered that a rogue device connected to the network, identify the port and the device responsible.
3. Determine the rogue device was not able to access network resources or introduce malware into the system
4. Prepare a report for security committee on the incident
5. Log on to the NAC device
6. Obtain a list of all ports and IPs from IT and ensure they are been monitored by the NAC.
7. Check the report of all network access on the NAC to confirm they are from approved devices

# Procedure Compliance & Enforcement

## Compliance Measures

Not applicable.

## Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Glossary / Acronyms

## Glossary / Acronyms

|  |  |
| --- | --- |
| ISO | Information Security Officer |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Procedure is owned by the YYYY

## Document Coordinator

This Procedure is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Distribution

* *IT*
* *ISO*