gravyty

your force for good

Network/Server Security Policy

Version No: 1.5

Version 1.5. | 2023

Table of Contents

1. Overview 3
2. Purpose 3
3. Scope 3
4. Network/Server security 3
5. General 3
6. Server Configuration Guidelines 3
7. Wireless Network Security 4

1. Overview

1.1. Network information security in Gravyty is intended to enhance the protection of data transmitted through routers. Server information security in Gravyty is intended to maintain server security hardening and physical protection.

2. Purpose

2.1. The purposes of this policy are:

- To ensure the safeguarding and protection of information in Gravyty's network and supporting infrastructure.
- To enhance the protection of data in transit and the protection of data at rest when on Gravyty's local servers.

3. Scope

3.1. This policy applies to Gravyty's local network and servers.

4. Network/Server security

4.1. General

4.1.1. Appropriate controls are to be implemented to ensure the security of Gravyty's sensitive information while transmitted over any network. These controls are to include network segregation, network connection control and appropriate encryption controls.

4.1.2. All connections between Gravyty's networks and networks outside of Gravyty must pass through appropriate firewall controls.

5. Server configuration guidelines

5.1. The most recent security patches are to be installed on the systems immediately, but never less frequently than on a weekly basis, unless immediate application would interfere with ongoing business requirements.

5.2. Servers should be physically located in an access-controlled environment.

6. Router security

6.1. The router is to have the enable password set to the current production router password from the router's support organization.

6.2. The enabled password on the router is to be kept in a secure encrypted form.

6.3. The following must be disallowed:

- IP directed broadcasts
- Incoming packets at the router sourced with invalid addresses such as an RFC1918 address
- TCP small services
- UDP small services
- All source routing
- Web services running on router
- Access rules are to be added and adapted in line with business needs and agreed upon by the IT Management Group.

6.2 Each router is to have the following statement posted on it in clear view: "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device."

7. Wireless network security

7.1. All wireless Access Points must be compliant with 802.11b/g wireless standards.

7.2. Only one Gravyty SSID (Service Set Identifier) is to reside on the WLAN. The Access Points are not to broadcast the SSID and are to support 802.1X authentication.

7.3. Vendors, customers and other third parties are not to have access through the WLAN.