gravyty

your force for good

Workstation Security Policy
Version No. 1.4

Version 1.4 | 2023

Table of Contents

1. Overview

1.1. This policy sets the guidelines for workstation information protection maintained by the implementation of appropriate security controls and user security awareness.

2. Purpose

2.1. The purpose of this policy is to enhance the protection of Gravyty's workstations, used by company employees, to avoid information leakage and damage to the integrity and availability of sensitive information.

3. Scope

3.1. This policy applies to Gravyty's workstations.

4. Workstation Security

4.1. General

4.1.1. Only authorized users are to receive equipment or access to systems.

4.1.2. The IT Management Group is to keep an up-to-date real-time inventory of all equipment and access to systems that were granted or rescinded.

4.1.3. Appropriate information protection measures, including training, is to be taken when using workstations, to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorized users.

4.1.4. The IT Management Group is to implement physical and technical safeguards for all systems, to restrict access to them by unauthorized users.

5. Protection measures

5.1. Appropriate protection measures are to include but not be limited to:

5.2. Restricting physical access to systems to authorized personnel only.

5.3. Securing systems and equipment (such as workstations with screen lock or logout) prior to leaving the area, to prevent unauthorized access.

5.4. Enabling a password-protected screensaver with a short timeout period to ensure that workstations that were left unsecured are kept protected.

5.5. Complying with all applicable password security policies and other policies, as set out herein.
5.6. Ensuring systems are used for authorized business purposes only.
5.7. Preventing the installation of unauthorized software on the systems.
5.8. Keeping food and drink away from equipment to avoid accidental spills and damage.
5.9. Securing equipment that contains sensitive information by using cable locks or locking laptops in drawers or cabinets.
5.10. Where possible, enabling portable equipment encryption.
5.11. Complying with the Anti-Virus policy set out herein.
5.12. Ensuring that monitors are positioned away from public view, if necessary, by installing privacy screen filters or other physical barriers to prevent public viewing.
5.13. Ensuring workstations can receive updates (for example, remaining powered up but logged off to facilitate after-hours updates, running exited applications, opening closed documents etc.).
5.14. Ensuring that all systems use a surge protector or have a robust UPS.
5.15. If a wireless network access is used, ensuring access is secure as set out herein in this policy.

6. Software installation

6.1. This section covers all equipment, including computers, servers, and other computing devices operating within Gravyty's network or that otherwise have access to its systems.
6.2. Employees are never to install software on equipment which operates within the network or has access to the systems. Any non-standard software requests must first be approved by the requester's manager and then be made to the IT Management Group in writing. The IT Management Group will obtain and track licenses, test new software for conflicts and compatibility, and perform installations.

7. Malware protection

7.1. All equipment and systems must have standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected equipment must be immediately removed from the systems until they are verified as virus-free by the IT Management Group.