gravyty

your force for good

Encryption Policy

Version No: 1.4

This document contains proprietary or confidential company information.

Table of Contents

1. Overview 3
2. Purpose 3
3. Scope 3
4. General 3
5. Encryption Guidelines 3

1. Overview

1.1. One mean of protecting sensitive data is encryption. This policy details Gravyty's preferred encryption algorithm, related devices, and control requirements.

2. Purpose

2.1. The purpose of this policy is to provide guidelines for encrypting Gravyty's sensitive data to prevent information leakage.

3. Scope

3.1. This policy applies to all mobile devices containing stored data owned by Gravyty.

4. General

4.1. While Gravyty's systems are meant to provide a reasonable level of privacy, users should be aware that the data they create on Gravyty equipment or systems remains the property of Gravyty.

4.2. Any information that users consider sensitive or vulnerable must be encrypted.

4.3. For security and network maintenance purposes, the IT Management Group may monitor equipment, systems and traffic (including internet usage) at any time.

5. Encryption Guidelines

5.1. Proven, standard algorithms should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. Key lengths must be at least 128 bits.

5.2. Gravyty's key length requirements will be reviewed annually and upgraded as technology allows.

5.3. All mobile devices containing stored data owned by Gravyty must use an approved method of encryption to protect data at rest.

5.4. Mobile devices are defined to include laptops, tablets, and smartphones.

5.5. No Gravyty data may exist on a laptop in cleartext form.

5.6. Laptops must employ full disk encryption with an approved software encryption package.

5.7. All Gravyty data stored on a smartphone or tablet must be saved to an encrypted file system using Gravyty-approved software.

5.8. Gravyty shall also employ remote wipe technology to remotely disable and delete any confidential data stored on a Gravyty tablet or smartphone that is reported lost or stolen.

5.9. All keys used for encryption and decryption must meet complexity requirements described in the Password Security standards set herein.