Recite me®

Encryption Policy

www.reciteme.com

Version	Date	Details	Author
1.0.0	20/02/2022	Initial Version	Rob Crozier

Table of Contents:

Introduction:

It is of paramount importance to Recite Me that all personal data and/or business critical data is protected from unauthorised access, disclosure or loss. We will therefore ensure that suitable encryption methods are in place for all such data.

Purpose:

This document outlines Recite Me's use of encryption across our organisation and spans all electronic devices and methods of communication.

Scope:

The scope of this policy includes all Recite Me information and ICT systems where information and data is stored. It also applies to all company employees, elected members, partner organisations, third-parties and vendors.

Definitions:

- **Personal Data** - Means any information relating to a natural, real person ('data subject'), from which potentially confidential, identifying information can be extracted.
- **Encryption** - A process of scrambling data to prevent unauthorised access.
- **Mobile Devices** - Includes any mobile phone or tablet computers that store data.
- **Removable Media** - Includes any device that can be inserted into a digital device to store data. This includes USB memory sticks, portable hard drives and CD/DVDs.
- **Third-parties** - Any individual, business and or contractor working with, or on behalf of Recite Me.

Policy Statement:

This policy has been constructed based on the guidelines from ISO:27001 and Cyber Essentials Plus.

Areas of Risk:

The following areas of risk have been identified:

- Desktop PC's and workstations
- Laptops
- Email
- USB and memory sticks
- Mobile devices

- Backup storage
- Production data storage

Encryption Strategy:

Encryption strategies have been identified for all areas of risk within this policy

- Desktop PC's and workstations
  All company desktop machines and workstations must be suitably encrypted. For any Windows machines, BitLocker full disk encryption should be used. For any other machines a suitable HDD encryption mechanism should be utilised. All desktop encryption should utilise no less than a 256 encryption key.

  Desktop machines and workstations should be fully encrypted prior to distribution to staff.

- Laptops
  All company laptops must be suitably encrypted. For any Windows machines, BitLocker full disk encryption should be used. For any other machines a suitable HDD encryption mechanism should be utilised. All desktop encryption should utilise no less than a 256 encryption key.

  Desktop machines and workstations should be fully encrypted prior to distribution to staff.

- Email
  All company mail shall be sent through our Google Workspace account which maintains suitable security controls including encryption, malware checking and anti-virus.

- USB and memory sticks
  All laptops and desktops should have removable media restricted and nmo-execute configured for any other USB medium.

- Mobile devices
  Any mobile device distributed to a staff member should not be used to store sensitive information and should also be configured with a remote wipe feature to allow the device to be remotely wiped in the event that it is lost or stolen.

- Backup storage
  Any system backups, whether from local workstations or production servers, should be encrypted using AES encryption with a minimum of a 256x encryption key.

- Production data storage
  Any production data storage that is not used for high-availability caching and may

contain sensitive information should be suitably encrypted with no less than a 256x encryption key.

Training:

Regular training shall take place for all staff members, tailored to their level of responsibility and their management and/or overseeing of sensitive data. This training will focus on key threat vectors affecting the information they have access to and will also cover key risk mitigation strategies.

Data-centres:

Any third-party data-centres contracted by Recite Me must hold a valid ISO:27001 certificate. Any data held within data-centres in the US must be within a facility that has a suitable SOC 2 accreditation.

Responsibilities:

It is the responsibility of business directors to ensure that all managers are aware of this policy and that it is observed. Managers should also be made aware that they have the responsibility to ensure staff within their team also have sufficient access to and/or sufficient knowledge of this policy and that it is observed.

Recite Me's ICT department and Information Security team are responsible for ensuring that the prerequisite encryption mechanisms are used prior to staff hardware distribution. Equally, this team is also responsible for ensuring that suitable encryption is implemented in a satisfactory way on all media types mentioned in this policy.

Staff members are responsible for reading and adhering to the information mentioned in our information security handbook which covers the key details on encryption for the devices they use and the data that they will have access to

Breaches:

Breaches of this policy and/or a security incident can be defined as an event which could have, or has resulted in, loss or damage to business assets, or an event which is in breach of the business security procedures and policies. All company employees, elected members, partner organisations, third-parties and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through Recite Me's Incident Reporting Procedure.

Recite Me will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an employee causing said breach, then the matter may be dealt with under company disciplinary procedures.

Review:

This policy will be reviewed following any substantial changes to infrastructure or related business policies, legislation changes and or any non-compliance complaints. The document will be automatically reviewed after annually.