Recite me®

Access Control Policy

www.reciteme.com

Version Information:

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

ISO72001:2013 Information:

This document has been completed using the following ISO72001:2013 standard controls as a reference:

ISO Control	Description
A.7.1.1	Screening
A.7.2.2	Information security awareness, education and training.
A.9.2.6	Removal or adjustment of access rights.
A.9.2.1 > 2	User registration and de-registration/User access provisioning
A.9.2.3	Management of privileged access rights
A.9.2.4	Management of secret authentication information of users
A.9.4.1	Information access restriction
A.18.2.2	Compliance with security policies and standards

Introduction:

In order to maintain control over Personal Data and/or business critical data, suitable access controls, whether logical or physical, must be in place. It is vital that authorised users who have access to Recite Me systems and information are aware of, and understand how, their actions may interact with security.

Purpose:

This policy is to provide a framework for how user accounts and privileges are created, managed and deleted. It includes how new users are authorised and granted appropriate privileges, as well as how these are reviewed and revoked when necessary and includes appropriate controls to prevent users obtaining unauthorised privileges or access.

Scope:

The scope of this policy includes all access to Recite Me information, ICT systems and physical access to real-world areas where information and data is stored. This policy applies throughout the information lifecycle from acquisition/creation, to utilisation, storage and, ultimately, disposal.

Definitions:

- **Personal Data** - Means any information relating to a natural, real person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **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:

System and Information Access:

- 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.
- Staff will be provided with and expected to read and understand the company handbook upon contract commencement, this covers many of the core principles of access control and information security.
- All access control will be created on contract commencement by a member of the information security team or other suitably responsible manager. Access control will then be reviewed on a starter, mover and leaver basis. The appropriate level of access to systems and information will be determined based upon the user's requirements, business needs, job function and role.
- Any change to access control must be formally requested from the information security team and/or another suitably responsible managerial member of staff.
- For systems containing restricted/personal information and data, an access control matrix must be developed to record role-based authorised access on a per individual basis. Authorisation procedures must be in place for managers to authorise all access (including short term and temporary access) recorded on the matrix. The access matrix must be continually updated and maintained to reflect accurate records of access.
- Generic logins shall not be permitted for access to any application or medium containing sensitive information.
- Multi Factor authentication should be enforced within any environment which supports it
- Any passwords must be suitably secure and adhere to the minimum requirements outlined in the company handbook and/or information security policy.

System and Information Access Revocation:

- If a member of staff changes role or their contract is terminated, their manager should ensure that a user's access to the system/information has been reviewed and where appropriate, suitably revoked.
- If a member of staff is deemed to have contravened any of the Information Security Policies or procedures, potentially jeopardising the availability, confidentiality or integrity of any systems or information, their access rights to the system/information should be reviewed by the system owner(s) and/or their line manager.

- Within systems that support it, suitable login attempt thresholds should be put in place; the baseline for which is 5 unsuccessful login attempts in rapid succession resulting in the used credentials being blocked for a period of no less than 15 minutes.
- If it is deemed that it is no longer appropriate nor necessary for a user to have access to systems and/or information then the user's manager will need to inform the owner(s) of the system/information that access rights should be altered/removed immediately.

Physical Access Controls:

Access to any environment in which sensitive information is physically stored (e.g. HDDs / Server rooms) should also be suitably managed. Methods of physically securing access to such environs should be in place (e.g. padlocks) and access logging should also be utilised to track visitation.

- Access to any location containing any medium on which sensitive information may reside should be suitably restricted through use of lock and key, access fob and/or biometrics.
- An access register should be maintained for specific access to said environments.
- Appropriate recording mechanisms need to be in place to record the names, dates, times and signatures for the signing in and out of visitors.
- Any keys, fobs, etc used to access any sensitive information locations should be stored in a secure location when not in use. A suitable record of any such items should be kept and any use of such keys should be recorded.
- Electronic access fobs must be issued to authorised staff on an individual basis. Staff issued with access fobs must have their names and employee numbers recorded against the registered access fob number, including date and time of issue.
- Access fobs should only be used by the registered user. They should never, under any circumstances be loaned to anyone else.
- Any access fobs, etc issued to an employee must be immediately deactivated upon termination of employment.
- Suitable perimeter controls including CCTV should be used for any environment which may contain sensitive information.
- Equipment housing sensitive information should not be stored in a public environment. All doors and windows to any location should also be suitably locked to prevent unauthorised access.
- Access to any physical locations shall only be permitted following a formal request and suitable check performed by the information security team and/or another suitably responsible, managerial staff member.
- All interfaces used for managing system administration and enabling access to information processing must be appropriately secured.
- Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms.

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.

Designated system owners have the responsibility of managing and recording access to such systems.

Designated system owners and/or information owners need to ensure they uphold the security policies and procedures

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 annually.