

Access Control Policy

Patronus Technologies Limited

1. Introduction

This policy specifies the access controls applied to information assets, systems and services used by Patronus Technologies Limited. Its purpose is to ensure that access to company and client information is appropriately authorised, restricted and managed throughout the lifecycle of that access.

This policy applies to all directors, employees, contractors and other authorised users who access Patronus Technologies Limited systems or information.

2. Access Control Rules – General

Access to information, systems and services must be granted according to business need and the principle of least privilege.

Access must only be provided to individuals who require it to perform their authorised responsibilities.

All user access must be attributable to an identifiable individual. Access rights must be appropriately authorised before being granted and must reflect the user's role and responsibilities.

Access credentials and individual user accounts must not be shared with another person.

Users must not attempt to access systems, information or functionality for which they have not been authorised.

3. User Access Lifecycle

Access to organisational systems and information must be approved before being provided to a new user. Access must be limited to the systems and privileges required for the individual's role.

Users must receive appropriate information security training and be made aware of relevant policies before being provided with access to sensitive information or systems.

Access rights must be reviewed and amended when an individual's role or responsibilities change.

When an employee, contractor or other authorised user leaves the organisation or no longer requires access, their access must be revoked promptly. Company equipment, credentials and other access mechanisms must be recovered or disabled as appropriate.

Expired, unused or redundant accounts must be removed or disabled at the earliest appropriate opportunity. Redundant user IDs must not be reassigned to other individuals.

4. Access Reviews

User access rights must be reviewed periodically and following significant changes to roles, responsibilities or systems.

Reviews must consider whether access remains necessary and appropriate, including administrative and privileged access.

Unnecessary or inappropriate access must be removed or amended promptly.

5. Privileged Access

Administrative and privileged access must be restricted to authorised individuals who require it for their role.

Privileged access must be granted according to the principle of least privilege and used only where necessary to perform authorised administrative or technical activities.

Where technically feasible, privileged administrative access should be separated from normal day-to-day user access.

Privileged accounts must be protected using multi-factor authentication and are subject to periodic access review.

6. Shared and Service Accounts

Individual user accounts must be used wherever technically possible.

Shared accounts should be avoided unless required for a legitimate technical or operational reason.

Where shared, system or service accounts are necessary, their use must be authorised, access appropriately restricted and credentials securely managed. Responsibility for such accounts must be identifiable.

7. Password and Authentication Rules

Passwords must be sufficiently strong and appropriate to the security requirements of the relevant system. Where system functionality permits, appropriate minimum password requirements must be enforced.

Passwords must be unique and must not be reused across organisational and personal accounts.

Passwords and authentication credentials must not be shared or transmitted insecurely.

Organisational passwords and credentials must be stored using an approved password management solution.

Default or temporary credentials must be changed before or upon first use where applicable.

Passwords must be changed promptly where compromise is known or suspected.

Authentication credentials must be appropriately protected during storage and transmission.

Passwords must be obscured where displayed during entry.

8. Multi-Factor Authentication (MFA)

Patronus Technologies Limited mandates the use of multi-factor authentication for services, systems and platforms used to access organisational data or information-processing facilities.

MFA is required for user accounts, including administrative and privileged accounts, wherever technically supported.

MFA must use authentication mechanisms supported and approved by the relevant system and provide an additional authentication factor beyond the user's primary password or credential.

Access to systems without MFA is not permitted unless MFA is not technically supported and a documented risk-based exception has been approved by the Information Security Manager.

MFA arrangements and approved exceptions are reviewed periodically to ensure their continued appropriateness.

9. Remote Access

Access to organisational systems from remote locations must be undertaken using approved devices, accounts and

services and in accordance with applicable information security policies.

Devices used to access organisational information must meet Patronus Technologies Limited security requirements.

Users must take reasonable precautions to prevent unauthorised access to or viewing of information when working remotely or in public locations.

10. Physical Access

Patronus Technologies Limited operates as a remote organisation and does not maintain information-processing facilities or corporate premises requiring organisational physical access controls.

Physical security of devices used by personnel is addressed through applicable device, remote-working and acceptable-use controls.

Physical security of cloud infrastructure and hosted information-processing facilities is managed by the relevant service providers and considered through Patronus Technologies Limited's supplier management and information security arrangements.

11. Data Masking and Non-Production Data

Patronus Technologies Limited recognises that personal, confidential and safeguarding information may require additional protection where information is used outside its primary operational purpose.

Live personal or safeguarding data must not be used for development, testing, demonstration or training purposes unless its use is specifically authorised and appropriate safeguards have been applied.

Where representative data is required, synthetic, anonymised, pseudonymised or appropriately masked data should be used wherever practicable.

Data masking or equivalent techniques may also be used where specific information must be hidden or partially obscured to prevent unnecessary disclosure.

Access to unmasked sensitive information must be restricted according to business need and the principle of least privilege.

12. Access Control Monitoring and Exceptions

Access-control arrangements are reviewed as part of Patronus Technologies Limited's information security management processes.

Suspected unauthorised access, credential compromise or inappropriate use of access privileges must be reported immediately in accordance with the Information Security Incident Management process.

Any exception to this policy must have a legitimate business or technical justification, be appropriately risk assessed and be authorised by the Information Security Manager.

13. Compliance

Failure to comply with this policy may result in removal or restriction of system access and may constitute a breach of contractual, employment or legal obligations.

Non-compliance will be addressed in accordance with the Information Security Disciplinary Policy and other applicable organisational procedures.