©(ORGANISATION NAME)

ACCESS CONTROL POLICY

Subject: Access Control Policy		Author: MuVio Solutions Ltd
Document Type: Policy (Internal)	Page: 1 of 14	Authorised by:
Effective Date: June, 2024	Version 1.0	Next Review:

Author	Signature	Date
Muvio Solutions Ltd (Consultant Designation)		

Revision History:

Version	Date	Change Number	Summary of Changes
1.0	April, 2024		

Distribution:

Name	Title

Approved By:

Name	Signature	Date
Name (Designation)		
Name (Designation)		
Name (Designation)		
Name (Designation)		

Document Ownership

Information Security

Document Control

The validity of this document is limited to the use of the policy as a guideline for Information Security Organisation-wide. In the event that the adopted policy framework changes, the document will have to be reviewed and the document owner must assess this

document for relevancy at that point. This document will be reviewed at least annually and updated accordingly to reflect changes to business objectives or the risk environment.

Document Control

The Document Owner controls the distribution of this document. The distribution is as follows:

- Chief Information Security Officer
- Chief Information Officer
- Chief Risk Officer
- Chief Audit Executive
- Chief Compliance Officer
- Head, Human Resources

Notice and Warning

CONTENTS

1.0 INTRODUCTION

Access to information and information systems is a fundamental aspect of Information Security. Access control is concerned with determining the allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. The access control policy provides guidance on access control to information systems and applications, either allowing or restricting access to information systems. This allows for the preservation of confidentiality within the Organisation and protects the Organisation's information and information systems from unauthorised access.

1.1 PURPOSE

The purpose of this policy is to establish directives, which will forestall uncontrolled or unauthorised access, misuse of user privileges, or unauthorised disclosure to third parties, that may result in security breaches, malicious damage, misuse, or theft of corporate resources.

1.2 OBJECTIVES

The objective of this document is to ensure that:

▪ Business, legal and security requirements drive the authorisation process and access to information and information assets.

▪ Access to information and information processing facilities is limited.

▪ A well monitored authorised user access is in place to prevent unauthorised access to systems, applications, and services.

1.3 SCOPE

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to Organisation systems.

1.4 RELATED DOCUMENTS

The following policies and procedures are relevant to this document:

- Mobile Computing Policy
- Travel (Remote Access and VPN) Policy
- Network Security Policy

2. POLICY DETAILS

- Access to information and information assets must be commensurate with the security requirements of that resource and the classification of data it provides access to.
- Access to all Organisation-wide information and information systems shall be granted to all users based on the principle of least privilege.

2.1 BUSINESS REQUIREMENTS OF ACCESS CONTROL

The control of access to our information assets is a fundamental part of a defence in depth strategy to information security. If we are to effectively protect the confidentiality, integrity, and availability of classified data then we must ensure that a comprehensive mix of physical and logical controls are in place.

But our policy regarding access control must ensure that the measures we implement are appropriate to business requirement for protection and are not unnecessarily strict. The policy therefore must be based on a clear understanding of business requirements as specified by the owners of the assets involved.

These requirements may depend on factors such as:

- The data/information classification of the information stored and processed by a particular system or service. (e.g. Confidential, Secret, Internal or Public)
- Relevant legislation that may apply e.g., the Data Protection Act, Sarbanes Oxley.
- The regulatory framework in which the organisation and/or the system operates.
- Contractual obligations to third parties.
- The threats, vulnerabilities and risks involved.
- The organisation's risk appetite.

Business requirements should be established as part of the requirements gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

In addition to the specific requirements, several general principles will be used when designing access controls for Organisation systems and services. These are:

- ***Defence in Depth*** – security should not depend upon a single control but several complementary controls.
- ***Least Privilege*** – the default approach taken should be to assume that access is not required, rather than to assume that it is.
- ***Need to Know*** – access is only granted to the information required to perform a role, and no more.

- ***Need to Use*** – Users will only be able to access physical and logical facilities required for their role.

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that may occur.

2.2 USER ACCESS MANAGEMENT

- Formal user access control procedures must be documented, implemented, and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. The procedure must cover all stages of the lifecycle of user access, from the initial registration (onboarding) of new users to the final deregistration (offboarding) of users who no longer require access to the organisation information assets.
- User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks, this should be monitored and reviewed at regular intervals as well by an independent body such as IT Audit team or Information security team.

2.3 USER REGISTRATION AND DEREGISTRATION

- A request for access to the organisation's network and computer systems must first be submitted to IT Service Desk for approval. All requests will be processed according to a formal procedure that ensures that appropriate security checks are conducted, and correct authorisation is obtained prior to user account creation. The principle of segregation of duties will apply such that a maker checker process is adopted during and after the creation of the user account and the assignment of permissions.
- Each user account will have a unique username that is not shared with any other user and is associated with a specific individual i.e. not a role or job title. Generic user accounts i.e., single accounts to be used by a group of people should be discouraged as they provide insufficient allocation of responsibility and traceability.
- An initial strong password should be created right from when the account is setup and communicated to the user via secure means. The user must be required to change the password on first use of the account. The new password must also be according the the organisation's password policy.
- When an employee leaves the organisation under normal circumstances, their access to computer systems and data must be revoked at the close of business on the employee's

last working day. It is the responsibility of the line manager to request the suspension of the access rights via the IT Service Desk.

- In exceptional circumstances where there is a perceived risk that the employee may take action that may harm the organisation prior to or upon termination, a request to revoke access may be approved and actioned in advance of termination notice. This precaution should especially apply in the case where the individual concerned has privileged access rights e.g., system or domain admin.

- User accounts for leavers should be initially suspended or disabled and not deleted. However, depending on the role of the user leaving the organisation, and if the employee is not being investigate, the account may be deleted immediately or after two (2) weeks of separation from the organisation. User account names should not be reused as this may cause confusion in the event of a later investigation.

2.4 USER ACCESS PROVISIONING

- Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general, this should be role-based i.e., a user account will be added to a group that has been created with the access permissions required for that specific job role.

- Group roles should be maintained in line with business requirements and any changes to them should be formally authorised, monitored, and controlled via the change management process.

- Ad-hoc additional permissions should not be granted to user accounts outside of the group role; if such permissions are required this should be treated as a change and formally requested and approved before implementation.

2.5 REMOVAL OR ADJUSTMENT OF ACCESS RIGHTS

- Where an adjustment of access rights or permissions is required e.g., due to an individual changing role (usually termed as movers), this should be carried out as part of the role change. It should be ensured that access rights no longer required as part of the new role are removed from the user account. If a user is taking on a new role in addition to their existing one (rather than instead of) then a new composite role should be requested via change management. Due consideration of any issues of segregation of duties should be given.

- Under no circumstances should administrators be permitted to change their own user accounts or permissions.

2.6 MANAGEMENT OF PRIVILEGED ACCESS RIGHTS

- Privileged access rights such as those associated with administrator level accounts must be identified for each system or network and well controlled. In general, technical users (such as IT support staff) should not make day to day use of user accounts with privileged access, rather a separate "admin" user account should be created and used only when the additional privileges are required. These accounts should be specific to an individual e.g., "John Smith Admin"; generic admin accounts should not be used as they provide insufficient identification for a user.

- Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training and have the technical know-how to understand the implications of the access rights associated with their account.

- The use of user accounts with privileged access in automated routines such as batch or interface jobs should be avoided where possible. Where this is unavoidable the password used should be protected and changed on a regular basis, e.g. every 60 or 90 days or yearly.

2.7 USER AUTHENTICATION FOR EXTERNAL CONNECTIONS

- In line with the network security policy, the use of modems on non-organisation owned PCs or devices connected to the organisation's network can compromise the security of the network. Specific approval must be obtained from the IT Service Desk before connecting any equipment to the organisation's network as per Organisation's Bring Your Own Device Policy.

- Where remote access to the network is required via VPN, a request must be made via the IT Service Desk. A policy of using two factor authentication for remote access should be used in line with the principle of "something you have and something you know" to reduce the risk of unauthorised access from the Internet.

- For further information please refer to the Organisation Travel (Remote Access and VPN) Policy and Network Security Policy.

2.8 SUPPLIER REMOTE ACCESS TO THE ORGANISATION NETWORK

- Partner agencies or 3rd party suppliers must not be given details of how to access the organisation's network without permission from the IT Service Desk. Any changes to supplier's connections (e.g., on termination of a contract) must be immediately sent to

the IT Service Desk so that access can be updated or revoked. The IT Service Desk must control and monitor all permissions and access methods.

- Partners or 3rd party suppliers must contact the IT Service Desk through their contact person within the organisation, on each occasion to request permission to connect to the network and a log of activities must be maintained. Remote access software and user accounts must be disabled when not in use.

2.9 REVIEW OF USER ACCESS RIGHTS

On a regular basis (at least quarterly), asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. The purpose is to identify:

- People who should not have access (e.g., leavers)
- User accounts with more access than required for their role.
- User accounts with incorrect role allocations.
- User accounts that do not provide adequate identification e.g., generic, or shared accounts.
- Any other issues that do not comply with this policy.

This review will be performed according to a formal procedure and corrective actions must be identified and implemented.

A review of user accounts with privileged access will be carried out by the Information Security manager on a quarterly basis to ensure that this policy is being complied with.

2.10 USER AUTHENTICATION AND PASSWORD POLICY

- A strong password is an essential barrier against unauthorised access. Unfortunately, this area is often proven to be the weak link in an organisation's security strategy and variety of ways to improve the security of user authentication are available, including various forms of two factor authentication and biometric techniques.

Organisation's policy is to make use of additional authentication methods based on a risk assessment which considers:

- The value of the assets protected.
- The degree of threat believed to exist.
- The cost of the additional authentication method(s).
- The ease of use and practicality of the proposed method(s).
- Any other relevant controls in place.

- Use of multi-factor authentication methods should be justified based on the above factors and securely implemented and maintained where appropriate.

- Single Sign-On (SSO) will be used within the internal network, where supported by relevant systems unless the security requirements are deemed to be such that an additional authentication method is required.

- Whether single or multi-factor authentication is used, the complexity of user passwords should be enforced in all networks and systems using the following parameters:

Parameter	Value
Minimum length	8
Maximum length	16
Re-use cycle	Cannot be the same as any of the previous 8 passwords
Characters Required	At least one capital letter At least one symbol/special character At least one number
Password similarity	New password cannot share more than three characters in the same position as the old password
Change Frequency	At least every 30 or 60 days
Account lockout	On 5 incorrect logon attempts
Account lockout action	Account must be re-enabled by IT Service Desk
Other controls	Password cannot contain the username

Any exceptions to these rules must be authorised by the Head of IT, and this should undergo change management approval and documented in a risk register for tracking purpose.

3 USER RESPONSIBILITIES

To exercise due care and try to ensure the security of its information, the Organisation expends a significant amount of time and money in implementing effective controls to reduce risk and vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems in their day-to-day activities. Many recent high-profile security breaches have been largely caused by unauthorised access to user accounts resulting from passwords being stolen or guessed.

It is vital therefore that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organisation.

To maximise the security of our information every user must:

- Use a strong password i.e., one which is in line with the rules set out in this policy.
- Never tell anyone their password or allow anyone else use their account.
- Not record the password in writing or electronically e.g., in a file or email.
- Avoid using the same password for other user accounts, either personal or business-related.
- Ensure that any PC or device connected to the organisation network which is not in use should not be left unattended. It must be locked or logged out.
- Leave nothing on display that may contain access or sensitive information such as login usernames and passwords.
- Inform the IT Service Desk of any changes to their role and access requirements.

Failure to comply with these requirements may result in the organisation taking disciplinary action against the concerned employee/individual.

4 SYSTEM AND APPLICATION ACCESS CONTROL

As part of the evaluation process for new or significantly changed systems, requirements for effective access control should be addressed and appropriate measures implemented.

These should consist of a comprehensive security model that includes support for the following:

- Creation of individual user accounts.
- Definition of roles or groups to which user accounts can be assigned.
- Allocation of permissions to objects (e.g., files, programs, menus) of different types (e.g., read, write, delete, execute) to subjects (user accounts and groups).
- Provision of varying views of menu options and data according to the user account and its permission levels.
- User account administration, including ability to disable and delete accounts.
- User logon controls such as:
    - Non-display of password as it is entered.
    - Account lockout once the number of incorrect logon attempts exceeds a specified threshold.
    - Provide information about number of unsuccessful login attempts and last successful logon once user has successfully logged on.
    - Date and time-based logon restrictions.
    - Device and location logon restrictions.
    - User inactivity timeout
- Password management, including:
    - Ability for users to change passwords when the need arises.

- Controls over acceptable passwords.
- Password expiry.
- Hashed/encrypted password storage and transmission.
- Security auditing facilities, including logon/logoffs, unsuccessful login attempts, object access and account administration activities.

Access to utility programs that provide a method of bypassing system security (e.g., data manipulation tools) should be strictly controlled and their use restricted to identified individuals and specific circumstances e.g., as part of a named project or change.

5 RECOMMENDATIONS/ADVISORY ON ACCESS CONTROL

Organisations with 1 – 5 Employees	Organisations with 6 – 20 Employees	Organisations with more than 20 Employees
• Consider cloud based IAM solutions that offer centralised user management, authentication, and access control. • Adopt Google Workspace which offers collaborative tools like Gmail, Google Drive for file storage. Microsoft 365 Business Basic which provides email, OneDrive file storage with built-in access control and security features or Dropbox. • Implement a password management tool like LastPass or Zoho Vault allowing authorised employees to securely store and share passwords and other sensitive information. • Implement secure remote access solutions, such as virtual private networks	• Consider Cloud based IAM solutions that offer centralised user management, authentication, and access control. • Adopt Google Workspace which offers collaborative tools like Gmail, Google Drive or Microsoft 365 Business Basic which provides email, OneDrive storage with built-in access control and security features or Dropbox. • Implement Privileged Access Management (PAM) solutions to secure and manage access to privileged accounts and administrative resources. • Assign roles and permissions based on the responsibilities and	• Consider Cloud based IAM solutions that offer centralised user management, authentication, and access control. • Adopt Google Workspace Enterprise or Microsoft 365 Enterprise which Offers advanced security features like data loss prevention, endpoint management, advanced threat protection, identity management. • Use OneLogin which provides SSO, MFA, user provisioning, and access control solutions designed for enterprise-level Organisations to secure access to cloud and on-premises applications.

(VPNs) or remote desktop solutions, to enable secure access to company resources from outside the office. • Conduct regular training and awareness programs for employees to educate them on access rights management best practices, data security, and the proper use of access rights tools.	access requirements of each employee. • Implement secure remote access solutions, such as virtual private networks (VPNs) or remote desktop solutions, to enable secure access to company resources from outside the office. • Conduct regular training and awareness programs for employees to educate them on access rights management best practices, data security, and the proper use of access rights tools.	• Assign roles and permissions based on the responsibilities and access requirements of each employee or user group. • Consider implementing access governance and compliance solutions to ensure access rights are effectively managed, reviewed, and audited. • Conduct regular training and awareness programs for employees to educate them on access rights management best practices, data security, and the proper use of access rights tools.

If you have any questions about the above policy, please contact them to the IT Manager or Head of IT.