[Company]

ACCESS CONTROL POLICY

Access to systems and resources

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Access Control Policy

3.1 Purpose

The purpose of the policy is to ensure the correct access to the correct information and resources by the correct people.

3.2 Scope

All employees and third-party users.

All systems and applications deemed in scope by the ISO 27001 scope statement.

Physical access is defined in the Physical and Environmental Policy.

3.3 Principle

Access control is granted on the principle of least privilege. Users are only provided access to the information they require to perform their tasks and role.

3.4 Confidentiality Agreements

All employees and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities

3.5 Role Based Access

Access to systems is based on role. Access is granted by the business owner, system owner or data owner and formally approved.

3.6 Unique Identifier

Users are assigned a unique username or identifier on the principle of one user one ID to ensure individual accountability. Usernames and identifiers are not shared between users.

3.7 Access Authentication

Users are positively identified and authenticated before gaining access to systems, services, or information.

3.8 Access Rights Review

User access to systems is reviewed at least annually to ensure it is still appropriate and relevant.

Inactive and dormant accounts are investigated, and appropriate action taken including the updating of required documentation.

The main user access system is reviewed every 90 days to ensure it is still appropriate and relevant.

3.9 Privilege Accounts / Administrator Accounts

Administrator accounts are not provided to users, including but not limited to laptops and mobile technology.

Where feasible privilege and administrator users are assigned specific privilege and administrator accounts in addition to their normal account for the specific use on the completion of privilege and administrator tasks.

Privilege and administrator accounts are not shared accounts, not generic accounts and do not share passwords.

Privilege and administrator accounts are clearly identifiable.

A register of privilege and administrator accounts is maintained.

Privilege and administrator accounts are logged and monitored.

Privilege and administrator accounts are provided for a set period of time.

3.10 Passwords

Access to systems and information is authenticated by passwords.

Initial passwords provided to users must be changed on first use.

Vendor supplied and default passwords are changed immediately upon installation.

Passwords are not generic, shared or set at a group level.

Passwords are to be kept confidential and not written down.

Passwords are not displayed when entered.

Passwords are not coded or included in any scripts or code or macros.

Passwords are encrypted when transmitted over networks.

Systems lock out users after 6 failed access attempts.

Passwords have a minimum length and format of 8 characters and a mix of alphanumeric characters.

System sessions that are idle for 15 minutes require passwords to be entered to regain access.

A password history file is maintained to prevent the reuse of passwords for at least four cycles.

Passwords are changed every 90 days.

3.11 User Account Provisioning

Account creation, modification and deletion is performed by authorised personnel and is fully documented.

Individual line managers approve account creation, modification, and deletion.

Business, system, or information owners approve access to systems and information. A form is used to clearly indicate the required access and an authorisation email or signature is provided.

All users requesting password resets or changes to authentication credentials have their identity verified.

3.12 Leavers

Line managers and HR inform the account provisioning team a user's leave date.

When a user leaves the company, all access is revoked, as a minimum to the main authentication technology, and to all systems and data recorded in the role-based access list.

User IDs, passwords and authentication credentials of leavers are not reused.

3.13 Authentication

The main access authentication system

- Does not display system or application identifiers until the log-on process has been successfully completed
- Display a general notice warning that the computer should only be accessed by authorized users
- Not provide help messages during the log-on procedure that would aid an unauthorized user

- Validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect
- Protect against brute force log-on attempts
- Log unsuccessful and successful attempts
- Raise a security event if a potential attempted or successful breach of log-on controls is detected
- Not display a password being entered
- Not transmit passwords in clear text over a network
- Terminate inactive sessions after a defined period of inactivity, especially in high-risk locations such as public or external areas outside the organization's security management or on mobile devices
- Restrict connection times to provide additional security for high-risk applications

3.14 Remote Access

Remote access to company networks and cloud-based services follows the same rules previously covered by this policy with the addition of the requirement for two factor authentications where available.

Remote connections are set to disconnect after a set period of time.

A list of users with remote access to internal network systems is maintained.

3.15 Third Party Remote Access

Access is only granted to third parties under current contract with an applicable non-disclosure agreement in place.

Access is granted for a specific time, to a specific system, to a specific individual and provided on receipt of a formal, valid, authorised access request.

Access is removed immediately on completion of the requirement.

A list of third parties and individuals with access is maintained.

3.16 Monitoring and Reporting

Access to systems is monitored and reported and actions that directly or indirectly affect or could affect the confidentiality, integrity or availability of data are managed via the Incident Management process.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.