Access Control Policy

1. User-Access Management

The objective is to prevent unauthorised access to information systems. Unique user identifications (IDs) will ensure users can be linked to, and made responsible for, their actions.

1.1 User Registration

Formal user registration will be required for granting access to multi-user information systems and services including:

- unique user IDs with strict limits to group IDs and preferably not permitted
- checks on authority from the system's owner for system entry
- giving users a written statement of their access rights
- requiring statements from users to confirm understanding
- withholding access until authorisation is completed
- recording all persons registered for user of the service
- cancelling rights for leavers or those changing jobs
- periodic checks to remove redundant user account IDs.

Staff contracts should include clauses specifying sanctions for failure to observe rules covering unauthorised access.

1.2 Privilege Management

A "privilege" is any facility in a multi-user system that enables one user to override system or application controls.

The allocation of privileges should be restricted and controlled through a formal authorisation process that should consider the following:

- privileges associated with each system product need to be identified
- privileges should be allocated on a need-to-use and event-by-event basis
- an authorisation process and record of privileges should be maintained
- development and use of system routines should be promoted
- privilege identifiers should be different from that for normal business use.

1.3 User Password Management

Where passwords are used to validate a user's personal identity for access to information systems or services, the allocation will be controlled through a formal management process that will consider:

- requiring a signed statement of confidentiality
- control of the issue of temporary passwords
- issuing temporary passwords with a full level of security.

Passwords will not be stored on a computer system in an unprotected form.

The issues use and maintenance of passwords will follow the company policy defined in the latest issue of the Password Security Policy.

1.4 Review of User Access Rights

A formal process is required to maintain effective control over access rights to data and information services so that:

- user access rights are reviewed at regular intervals and after changes
- special privileges access rights should be reviewed more frequently
- privilege allocations should be regularly checked.

2. User Responsibilities

The objective is to prevent access by unauthorised users, and the compromise or theft of information and information processing facilities.

2.1 Password Use

Users will follow good security practice in password selection and the following should be considered:

- keep passwords confidential
- avoid keeping paper records unless securely stored
- change passwords whenever security is threatened
- select passwords with a minimum of eight characters, that are easy to remember, not based on anything easy to guess, free from consecutive characters or numbers
- regular changing of passwords and avoidance of using old passwords
- change temporary passwords at first log-on
- do not use passwords in an automated log-on process
- do not share individual passwords.

Special consideration should go to users of multiple services or platforms with a view to using a single quality password.

The issues use and maintenance of passwords will follow the company policy defined in the latest issue of the Password Security Policy.

2.2 Unattended User Equipment

Users and contractors will ensure equipment left unattended, even temporarily, has appropriate protection by:

- terminating active sessions when the session is finished
- logging off workstations, laptops, servers etc. when the session is finished
- ensuring the log-off procedure has been completed when switching off or leaving the equipment unattended
- securing computers and terminals from unauthorised use.

2.3 Clear Desk and Clear Screen Policy

The following controls will be considered:

- storage of paper and computer media in locked cabinets
- sensitive or critical business information will be locked away when not required
- personal computers and terminals will not be left logged on when not attended and should be protected by key locks, passwords and other appropriate controls
- in and outgoing mail and faxes should be protected
- photocopiers should be locked outside normal working hours
- sensitive or classified information will be overseen by authorised personnel during processing and cleared from printers immediately.

3. Network Access Control

The objective is to protect network services and to control unauthorised access to both internal and external network services.

3.1 Policy on Use of Network Services

The policy concerning the use of networks and network services should be consistent with the business access control policy and covers:

- which networks and network services are allowed to be accessed
- the authorisation procedures to determine who is allowed access
- the management controls and procedures to protect access to network connections and services.

3.2 User Authentication for External Connections

External connections provide potential for unauthorised access through dial-up methods and therefore need control based on a risk assessment. Authentication of remote users can be achieved by:

- cryptographic based techniques
- hardware tokens
- challenge/response protocol
- dial back procedures and controls

Where selected, controlled policies and instructions for the safe working of the above, will be developed.

A facility for automatic connection to a remote computer could provide a way of gaining unauthorised access to a business application and thus should be authenticated. Node authentication can serve as an alternative for authenticating groups of remote users where they are connected to a secure, shared computer facility.

3.3 Equipment Identification in Networks

Should be considered if it is important if a session can only be initiated from a particular location or computer terminal. An identifier attached to the terminal can be used and if so it may also be necessary to apply physical protection to the terminal to maintain security of the terminal identifier.

3.4 Remote Diagnostic and Configuration Port Protection

Access to remote ports should be securely controlled, especially to control the activity of maintenance engineers using remote diagnostic facilities.

Dial up facilities should be protected by a key lock or similar with a support procedure where access can only be achieved through arrangements between the Company and the hardware/software support personnel.

4. Operating System Access Control

The objective is to prevent unauthorised access to operating systems. The facilities should be capable of the following:

- identifying and verifying the identity, terminal and location of each authorised user
- recording of successful and failed system accesses
- providing appropriate means for authentication
- where appropriate, restricting the connection times of users
- consideration of other methods, such as challenge/response.

4.1 Secure Log-on Procedures

Access to information services should be via a secure log-on process that will provide the minimum information about the system. A good log-ion procedure should:

- not display system/application identifiers until after successful log-on
- display a general warning about access only for authorised users
- not provide help messages during log-on that would aid access
- validate the log-on information only on the completion of all input data
- limit the number of unsuccessful log-on attempts and record them and then force a time delay before further attempts. Possibly disconnect data link connections
- limit the maximum/minimum time for a log-on;
- on completion, display date and time of previous successful log-on;
- provide details of any unsuccessful log-on attempts since last log-on.

4..2 User Identification and Authentication

Passwords are the most common method of authentication but cryptographic means can be used, as can smart cards, memory tokens, biometrics and others.

4.3 A good management system for passwords should:

- enforce the use of individual passwords, and where appropriate, allow users to select their own password
- enforce a choice of quality passwords
- enforce changes to passwords to an agreed plan
- on user selected passwords, change temporary passwords at first log-on
- maintain a record of previous user passwords
- not display passwords on the screen at entry
- store password files separately from applications system data
- store encrypted passwords using a one-way encryption algorithm
- alter default passwords following installation software.

4.4 Use of System Utilities

Where system utilities exist that can over-ride system and application controls the following controls should be considered:

- use of authentication procedures for system utilities
- segregation of system utilities from application software
- limitations on the use of system utilities
- authorisation for ad hoc use of systems utilities
- limitations of the availability of system utilities
- logging off all use of system utilities
- defining and documenting of authorisation levels for system utilities
- removal of all unnecessary software-based utilities and system software.

4.5 Session Time Out

Inactive terminals in high-risk locations should shut down after a defined period and the time out delay should reflect the security risk of the area and the users of the terminal.

5. Limitation of Connection Time

Restricting connection time in high risk applications should be controlled, including;

- using predetermined time slots
- restricting connection times to normal office hours.

6. Application and Information Access Control

The objective is to prevent unauthorised access to information held in application systems. Logical access to software and information should be restricted to authorised users and application systems should:

- control user access to information and application system functions
- provide protection from unauthorised access for any utility and operating system software that is capable of overriding system application controls
- not compromise the security of other systems with which information resources are shared
- be able to provide access to information to the owner only, other nominated authorised individuals, or defined groups of users.

6.1 Information Access Restriction

Application of the following controls should be considered in order to support access restrictions requirements:

- provision of menus to control access to applications system functions
- restrict users' knowledge of information or application systems functions which they are not authorised to access, with appropriate editing of user documentation
- controlling the access right of users
- ensuring that outputs from applications handling sensitive information contain only the relevant information and go only to authorised terminals and locations and include periodic reviews.

6.2 It may be that the system is so sensitive that the application should run on a dedicated computer and should only share resources with trusted application system. The following considerations apply:

- the sensitivity of the application system should be explicitly identified and documented by the application owners;
- when a sensitive application is run in a shared environment, the application system with which it will share resources should be identified and agreed with the owner of the sensitive application.

7. Mobile Computing and Teleworking

The objective is to ensure information security when using mobile computing and teleworking facilities. The risk of using mobile computing and the risks of working in an unprotected environment should be considered and appropriate protection applied.

7.1 Mobile Computing and Communications

Mobile computing using notebooks, palmtops, laptops and mobile phones requires special care to ensure that the business information is not compromised. A formal policy is required which takes account of physical protection, access controls, cryptographic techniques, backups and virus protection. This should include rules and advice on connecting mobile facilities to networks and guidance on their use in public places.

Procedures against malicious software should be put in place and kept up-to-date and quick and easy backups should be possible. These backups should be protected against theft or loss.

When connected to networks, remote access to business information across public networks using mobile computing facilities should take place only after authentication and identification, with suitable access control in place.

Mobile computing facilities should be protected against theft. Training will be arranged for staff using mobile computing to raise awareness. See the Mobile Computing Policy for further information on the use of equipment away from the office.

7.2 Teleworking

Teleworking uses communications technology to enable staff to work remotely from a fixed location outside their organisation. Protection is required against equipment theft, unauthorised disclosure of information, unauthorised remote access to the Organisation's internal system or misuse of the facilities.

Control procedures should be in place and the following will be considered:

- existing physical security of the site, taking into account the physical security of the building and the local environment

- proposed teleworking environment
- communications security requirements including the remote access required to the Organisation's internal systems, the sensitivity of the information and the sensitivity of the internal system
- the threat of unauthorised access to information by people within the remote accommodation.

The controls and arrangements to be considered should include:

- provision of suitable equipment and storage furniture
- definition of the work permitted, hours of work, classification of information and authorisation permits for internal systems
- suitable communications equipment including secure remote access
- physical security
- rules and guidance on family and visitors' access to the equipment
- provision of hardware and software support and maintenance
- procedures for backup and business continuity
- audit and security monitoring
- revocation of authority, access rights and the return of the equipment when activity ceases.

8. RELATED DOCUMENTATION

Information Security Policy

Communications Policy

Password Security Policy

Mobile Computing Policy

9. REFERENCES

ISO 27001:2013, ISO 27002:2013