ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Security category – 9.4. System and application access control

Control – 9.4.1. Information access restriction
Access to information and applications should be restricted in line with the access control policy.

Restrictions of access to information should be based on individual business requirements.

Some guidelines on the restriction requirements include:
- control the access of users in terms of what they can do - read, write, delete, execute;
- control which data can be accessed by each particular user;
- control the access rights of applications;
- provide menus to control access to application system functions.

ISO/IEC 27001:2013 Information security management systems

-System and application access control-

Control – 9.4.2. Secure log-on procedures

Access to systems and applications should be controlled with a secure log-on procedure.

The log-on procedure needs to be:

- ***easy to understand;***
- ***user-friendly;***
- ***must not give information about the system or application that the user is trying to access (before accessing it);***
- ***should minimize the opportunity for unauthorized access.***

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

ISO/IEC 27002 guidelines for a good log-on procedures:

a) not displaying system or application identifiers until the log-on is completed;
b) display a general notice warning that the computer should only be accessed by authorized users;
c) not providing help messages during the log-on;
d) validate the log-on information only on completion;
e) protect against brute force log-on attempts;
f) record unsuccessful and successful attempts;
g) raise a security event if a potential attempted or successful breach of log-on;
h) display the following information on completion of a successful log-on: date and time of the previous successful log-on; details of any unsuccessful log-on attempts;
i) do not display the password being entered;
j) do not transmit passwords in clear text over a network;
k) terminate inactive sessions after a defined period of inactivity;
l) restrict connection times to provide additional security for high-risk applications.

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Control – 9.4.3. Password management system
The organization should use interactive password management systems that ensure quality passwords.

A password management system should:

- enforce the use of individual user IDs and passwords to maintain accountability;
- allow users to select and change their own passwords and include a confirmation procedure;
- enforce a choice of quality passwords;
- force users to change their passwords at the first log-on;
- enforce regular password changes and as needed;
- maintain a record of previously used passwords and prevent the re-use of past passwords;
- not display passwords on the screen when being entered;
- store password files separately from application system data;
- store and transmit passwords in protected form.

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Control – 9.4.4. Use of privileged utility programs
The organization should restrict and strictly control the use of utility programs that are capable of overriding system and application controls.

Because utility programs may provide access to the parts of the system by overriding controls they can be a risk for security.

The use of such programs should be controlled:

- users have to be identified and authorized for their use and logs should be maintained;
- the use of utility programs should be limited to the minimum needed;
- utility programs should be segregated from application software and users should not have access to privilege functions from their normal user accounts.

ISO/IEC 27001:2013 Information security management systems
-System and application access control-

Control – 9.4.5. Access to program source code
Access to program source code should be restricted.

Unauthorized access to program source code can be a great opportunity for an intruder to modify the system.

Use of libraries – method to protect source code

There are a few requirements for the source code libraries :

- as much as possible libraries should not be held in operational systems;
- there have to be some rules for the management of program source code and libraries where they are stored;
- the updating of program source libraries should only be done with authorization;
- all accesses to program source libraries should be logged;
- maintenance and copying of program source libraries should be subject to strict change control procedures.