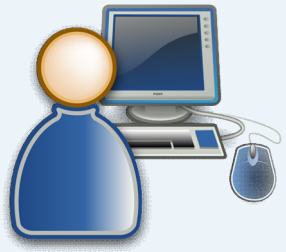
ISO/IEC 27001:2013 Information security management systems
-User access management-

Security category – 9.2. User access management



Control – 9.2.1. User registration and de-registration
There has to be a formal user registration and de-registration process to enable assignment of access rights.

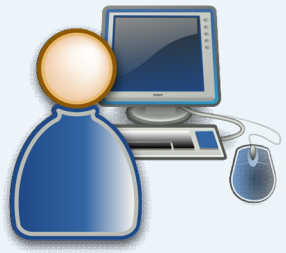
Every user should be formally authorized and registered to each information system, network or service that it accesses for the business needs.

Management of user IDs:

- use unique user IDs to enable users to be linked to their actions;
- immediately disable or remove user IDs of users who have left the organization;
- periodically identify and remove or disable redundant user IDs and
- ensure that redundant user IDs are not issued to other users.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.2. User access provisioning
The organization should implement a formal user access provisioning process to assign or to revoke access rights for all user types to all systems and services.



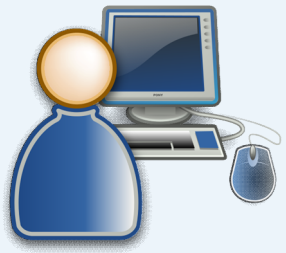
- the owner of the information system is responsible to approve or revoking of access rights to user IDs;
- access rights should not be activated before authorization;
- a central record of access rights granted to each user ID should be kept;
- access rights should be adapted for users who change roles or jobs and removed for users who left the organization.

An easier way to manage access rights is by using role based access - defining user profiles for different roles and positions in the organization.

Define sanctions for unauthorized access

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.3. Management of privileged access rights
The allocation of privileged access rights should be controlled and there should be a formal process for this.

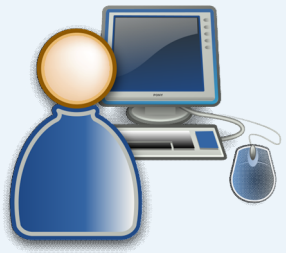


Privileges = means to shortcut controls.
Unnecessary allocation and use of privileges may lead to to security breaches.

ISO/IEC 27002 recommendations on the allocation of privileged access rights:
- clear identification of privilege access rights and the users for every application, operating system, database; etc
- allocation of privileged access rights on a need-to-use basis and preferably on an event-by-event basis;
- use an authorization process for granting privileged access rights and not grant them until authorization is obtained;
- assign the privilege access rights to a user ID that is different from the ones used for regular business activities.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.4. Management of secret authentication information of users
There should be a formal process for the allocation of secret authentication information.

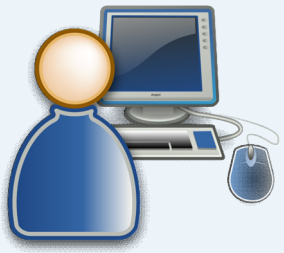


Secret authentication is done usually through passwords.

Requirements for allocation of secret authentication information:
- users should be asked to sign a statement to keep personal secret authentication information (passwords) confidential;
- if the users select their own passwords - they should be provided initially with a temporary password that they should be forced to change;
- passwords should be given to users in a secure manner and users should acknowledge their receipt.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.5. Review of users access rights
Asset owners should periodically review user's access rights.

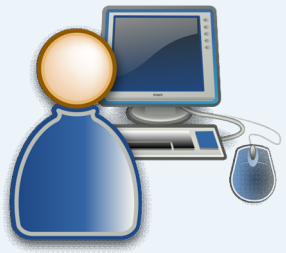


Access rights have to be based on business needs and when the business need changes or passes the access should be cancelled.

Periodically access rights should be reviewed and if found that some access rights are not needed they have to be withdrawn.

ISO/IEC 27001:2013 Information security management systems
-User access management-

Control – 9.2.6. Removal of users of access rights
At the end of employment or contract the access rights of employees or external parties should be removed. In case of changing positions the access rights should be adjusted.



If an employment is terminated the access rights associated should be removed.

If the user is part of a group – and access rights are allocated at group level – the individuals leaving should be removed from the group and the other members should be informed to no longer share information with the person departing.