ISO/IEC 27001:2013 Information security management systems
-Business requirements for access control-

Security category – 9.1. Business requirements for access control

Control – 9.1.1. Access control policy
The organization should document an access control policy.

***Access control refers to both logical and physical access*.**

Access control rules, access rights and restrictions for specific user roles should be established.

Asset owners decide access rights to assets based on business needs

ISO/IEC 27001:2013 Information security management systems
-Business requirements for access control-

An access control policy should exist and should address some elements:

- security requirements for different business applications;
- consistency between access rights and information classification;
- legislation and contractual obligations regarding limitation of access to data or services;
- segregation of roles that refer to access control;
- periodic review of access rights;
- removal of access rights;
- roles that have privileged access*.*

Principles: ***Need–to–Know and Need-to-Use***

Use: "**Everything is generally forbidden unless expressly permitted**“
instead of
"**Everything is generally permitted unless expressly forbidden**"

ISO/IEC 27001:2013 Information security management systems

-Business requirements for access control-

Control – 9.1.2. Access to networks and network services

Users should only have access to the network and network services that they have been specifically authorized to use.

ISO/IEC 27002 recommends a policy on the access to networks that should cover:

- the networks and networks services which are allowed to be accessed;
- authorization procedures for determining who is allowed to access which networks and services;
- what controls are in place to protect access to networks and services;
- how are the networks and network services accessed (ex. use of VPN or wireless)
- what are the requirements for user authentication to allow access to networks and services;
- how the use of network services is monitored.

Users logging to a network, computer or application should have access only to the information and services required for their business function that they have been authorized to use.