Information access restriction

ISO 27002 Control 8.3

Control

Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control

Purpose

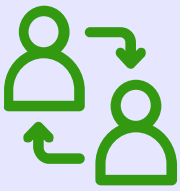
To ensure only authorized access and to prevent unauthorized access to information and other associated assets

Why is it important?

- It supports the need-to-know principle for all information and assets
- Dynamic access management allows granular, real-time control, even when data is shared outside the organization
- Prevents unauthorized exposure of sensitive data to anonymous users

Which topics should be addressed ?

- Restriction of access to information and other associated assets in accordance with the established topic-specific access control policy
- Controlling which data/functions can be accessed by a particular user or group (read, write, delete, execute)
- Preventing public or anonymous access to sensitive information
- Implementing dynamic access management techniques for sensitive, high-value information



What small details are important?

- Access control can be implemented with different granularity, ranging from whole networks to specific data
- Dynamic access can leverage the information classification scheme to determine protection needs
- Dynamic access management does not replace classical access management (ACLs) but enhances it

Link with other frameworks

- NIST 800-53 rev5 : AC-3, AC-24
- NIST CSF 2.0 : PR.AA-02, PR.AA-05, PR.DS-02, PR.DS-10

Renaud Dardenne
Asphalia Consulting