Authentication information

ISO 27002 Control 5.17

Control

Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information

Purpose

To ensure proper entity authentication and prevent failures of authentication processes

Authentication and Identity management

- Authentication directly follows the management of identities
- During Identification, one pretend to be someone
- During authentication, one proves that they are who they pretend

What are the best practices

- Initial passwords should be random
- Initial passwords should be communicated secretly
- Identity should be confirmed prior to the initial communication
- Acknowledgement of reception of credentials should be logged
- Initial passwords should be forcibly
- Users should be aware of the risks of mishandling their authentication information
- Users should use passwords safe when needed
- Use Multi-Factors Authentication when needed / when possible

Misconceptions

- Passwords length is not an end in itself and does not guarantee security : with too much complexity and length, passwords are written on post-it
- Passwords frequency modification should not be too high : a “good” password for which there is no suspicion of compromission should not be modified (too often)
- I Can Share My Password Safely : A common misconception is that sharing passwords with trusted individuals or colleagues is harmless

Link with other frameworks

- NIST 800-53 rev5 : IA-5
- NIST CSF 2.0 : PR.AA-01, PR.AA-05

Renaud Dardenne
Asphalia Consulting