Personnel Security

- The public institution shall identify (inventories) its own human resources. For each official position with access, the scope of duties and the analyzed security requirements are defined (the level of access to zones, rooms, documents, systems etc.).
- The public institution shall verify the identity of employees and job candidates based on the submitted original documents (containing names, surnames, date of birth, address and photo).
- The institution shall screen individuals prior to hiring them as well as taking up a role related to access to sensitive information. In particular, it does so before authorizing access to digitalization systems of the institution.
- The institution shall ensure that institutional systems are protected during and
- after personnel actions such as terminations and transfers.
- The institution shall provide basic training on information security upon commencement of employment.
- The institution shall ensure the identification of people having access to the facilities by introducing mandatory identifiers (badges).
- The institution shall ensure that security personnel are immediately provided with information on the denial of access for the departing employee.
- The institution shall ensure periodic verification of physical access and authorizations for employees and external subcontractors related to position and work performed.
- The public institution shall provide all employees with awareness training in social engineering threats. Completion of the training shall contain the training program content, its duration, the instructor and the trainee's signature.
- The public institution shall have procedures for verifying the qualifications of candidates and employees.
- The institution shall ensure that people with no criminal record are employed in key positions. This is done by a successful job candidate submitting a Criminal Record Certificate.

Revision #2
Created 11 July 2025 15:24:36 by RISA
Updated 14 July 2025 07:37:29 by RISA