ISO/IEC 27001:2013 Information security management systems

-HR Security – Prior to employment-

Security category – 7.1. Prior to employment

Control – 7.1.1. Screening

There have to be background checks for all candidates for employment done in accordance with the legislation and ethics. The checks are to be proportional to the sensitivity of the information to be accessed by the employee, the risks involved and the business requirements.

Screening is meant to prevent the organization hiring the wrong person.

There have to be procedures for screening:

- *criteria and limitations;*
- *who is eligible to screen people;*
- *how is screening performed and when;*
- *why perform verifications.*

ISO/IEC 27001:2013 Information security management systems

-HR Security – Prior to employment-

Screening should respect legislation (privacy, personally identifiable information and employment legislation).

Screening may include:

- character references;
- verification of the CV;
- confirmation of claimed academic and professional qualifications;
- independent verification of identity of the candidate;
- more detailed review (such as credit review, review of criminal records).

The level of detail for the verifications during screening are correlated with the access held by the individual to confidential information.

Screening applies employees, contractors, third-party users.

ISO/IEC 27001:2013 Information security management systems

-HR Security – Prior to employment-

Control – 7.1.2. Terms and conditions of employment

The responsibilities of employees and contractors for information security as well as the responsibilities of the organization should be documented in the contractual agreements.

ISO/IEC 27002 guidelines for the terms and conditions of employment:

- all individuals who have access to confidential information have to sign a confidentiality or non-disclosure agreement before accessing information;
- what are the employee's legal responsibilities and rights, (ex. with regards to copyright legislation, privacy and protection of personally identifiable information, etc)
- responsibilities for the classification of information and management of organizational assets handled by the employee or contractor;
- actions that can be taken by the organization in case the employee disregards security requirements.