ISO/IEC 27001:2013 Information security management systems
-HR Security – During employment-

Security category – 7.2. During employment

Control – 7.2.1. Management responsibilities
The employees and contractors shall be required by the management to apply information security according to the policies and procedures of the organization.

Management should make sure that employees and contractors:

- are informed of their information security roles and responsibilities before obtaining access to confidential information;
- are informed on the information security expectations for their roles
- are motivated to fulfil the security policies;
- receive awareness on information security;
- conform to the terms and conditions of employment;
- are trained regularly to be able to keep skills and qualification up to date;
- can report anonymously violations of security policies and procedures.

Management should exercise control and check the compliance with policies, procedures and regulations in the day-to-day work.

ISO/IEC 27001:2013 Information security management systems
-HR Security – During employment-

Control – 7.2.2. Information security awareness, education and training
There has to be appropriate awareness and training on information security aspects for all employees and contractors as relevant for their positions.

Untrained individuals are a risk for information security.

The organization should develop a security awareness programme to make individuals aware of their responsibilities for information security and how they should act.

All personnel should be trained on information security procedures and policies and on the use of equipment and software relevant to their jobs (internal or external training).

ISO/IEC 27001:2013 Information security management systems
-HR Security – During employment-

Control – 7.2.3. Disciplinary process
The organization should develop and enforce a disciplinary process to be applied in case of security breaches committed by employees. The disciplinary process has to be formal and communicated.

Non-compliance with security policies or controls needs to be dealt with properly.

The disciplinary process:
- shall ensure the treatment is fair and correct and
- shall not commence without prior verification and confirmation that a security breach has occurred
- should provide for a graduated response.

Employees have to be informed about the disciplinary process