ISO/IEC 27001:2013 Information security management systems
-Management direction for information security-

Security category – 5.1. Management direction for information security

Control – 5.1.1. Policies for information security
The organization should define, publish and communicate to its employees and to any external parties as needed a set of information security policies.

First level – Information security policy
(definition of information security, the objectives and principles; reasoning for the ISMS; information security is actively supported by management; responsibilities for information security in the organization; references to lower level policies, regulations, manuals; how any deviations from the policy are to be handled by the management; etc)

Information security policy – communicated to staff, persons working for organization and external parties

ISO/IEC 27001:2013 Information security management systems
-Management direction for information security-

Lower level – Specific policies

- Access control,
- Information classification
- Physical and environmental security
- Acceptable use of resources
- Clear desk and clear screen
- Information transfer
- Mobile devices and teleworking
- Restrictions on software installation and use
- Backup
- Protection from malware
- Management of technical vulnerabilities
- Cryptographic controls
- Communications security
- Privacy and protection of personally identifiable information
- Supplier relationships

Its best if the policies are simple and easy to understand

ISO/IEC 27001:2013 Information security management systems
-Management direction for information security-

Control – 5.1.2. Review of policies for information security
The organization should review periodically the policies for information security to make sure they continue to be suitable, adequate and effective.

This review process – should take into consideration changes to the business environment, to legal requirements, to technology, to internal organization.

Whenever circumstances change the information security policies should be updated to reflect the new conditions