ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Security category – 6.2. Mobile devices and teleworking

Control – 6.2.1. Mobile devices policy
The organization should have a policy and security measures in place to manage risks associated to mobile devices use.

Mobile devices policy should consider:
- registration of mobile devices
- physical protection of mobile devices
- restrictions on software installation
- mobile device software versions and for applying patches
- restriction of connection to information services
- access controls
- cryptographic techniques
- malware protection
- remote disabling, erasure or lockout
- backups
- use of web services and apps

ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Care should be exercised when using mobile devices in public places.

Mobile devices should be protected physically against theft.

Users should be trained on the security measures for mobile devices.

In case of remote connections to the organization’s site or databases the authentication should cover not only the device but also for the user.

When using private devices for business purposes:
- separate business and private use of the devices (ex. with a software)
- give access to business information only after the user has signed an agreement acknowledging duties, waiving the ownership of business data and allowing remote wiping of data by the organization in case of theft or loss of the device

ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Control – 6.2.2. Teleworking
The organization should have a policy and security measures implemented to protect information that is accessed, is processed or stored at teleworking sites.

Teleworking = “remote work” or “flexible workplace”, or “virtual work”

Decide whether to allow private owned equipment for teleworking or provide equipment.

Define a policy – conditions and restrictions for teleworking

ISO/IEC 27001:2013 Information security management systems
-Mobile devices and teleworking-

Conditions and restrictions on teleworking (ISO/IEC 27002 guidelines):

- physical security of the location;
- permissions (hours of work, the information and services);
- communication security;
- use of virtual desktop access;
- potential for unauthorized access (ex. family, friends, visitors)
- use of home networks and restrictions;
- possible need to obtain access to privately owned equipment;
- software licensing;
- malware protection and firewall;
- hardware and software maintenance
- backup and business continuity;
- revocation of authority and access rights