

Demo Company Limited		
Equipment		
ISO/IEC 27001:2013		
Issue 1	A.11.2.1 Equipment siting and protection. A.11.2.2 Supporting utilities A.11.2.3 Cabling security A.11.2.4 Equipment maintenance A.11.2.5 Removal of assets A.11.2.6 Security of equipment and assets off-premises. A.11.2.7 Secure disposal or re-use of equipment A.11.2.8 Unattended user equipment A.11.2.9 Clear desk and clear screen policy	Authorised By:- Directors of Demo Company Limited
Page 1 of 3	Effective Date: 1st Nov 2021	Classification:- Internal
Issue Date: 1st Nov 2021		Last Review Date: 1st Nov 2021

Scope

This controlled process defines information security controls applied for equipment siting and protection, supporting utilities, cabling security, equipment maintenance, removal of assets, security of equipment and assets off-premises, secure disposal or re-use of equipment, unattended user equipment, clear desk, and clear screen policy.

Responsibility and Authority

The appointed information security representatives are responsible for the overall management of this process including its correct implementation and regular review.

Control and Distribution

This process is issued as a controlled document and can only be updated by the authorised information management representative and must include a revision status and traceability of the change process.

A master is retained as part of the information security management system with uncontrolled copies issued at point of use.

The Process

A.11.2.1 Equipment siting and protection.

This is addressed through the documented equipment siting and protection procedure and details controls to protect and store equipment such as computers, printers, telecommunications, servers and building services which protect information assets.

Demo Company Limited		
Equipment		
ISO/IEC 27001:2013		
Issue 1	A.11.2.1 Equipment siting and protection. A.11.2.2 Supporting utilities A.11.2.3 Cabling security A.11.2.4 Equipment maintenance A.11.2.5 Removal of assets A.11.2.6 Security of equipment and assets off-premises. A.11.2.7 Secure disposal or re-use of equipment A.11.2.8 Unattended user equipment A.11.2.9 Clear desk and clear screen policy	Authorised By:- Directors of Demo Company Limited
Page 2 of 3	Effective Date: 1st Nov 2021	Classification:- Internal
Issue Date: 1st Nov 2021		Last Review Date: 1st Nov 2021

A.11.2.2 Supporting utilities

The organisation has installed UPS to protect against power outages and AC to protect against overheating of servers and supporting equipment. These are tested and maintained on an annual basis and records retained. Alarms are installed to monitor, and issues warnings should protection fail. **What other protection in place? IE Dual power supply, generators, emergency cut off?**

A.11.2.3 Cabling security

Cabling security includes underfloor installation, power and communications are separated, locked cabinets, electromagnet shielding and restricted access to patch panels and cable rooms.

A.11.2.4 Equipment maintenance

The organisation uses only approved third party providers and records are retained regarding faults and repairs. Equipment is tested and inspected prior to reuse and a planned preventive maintenance program has been implemented to ensure equipment is available when required.

A.11.2.5 Removal of assets

The **Inventory of Assets** includes the current location of all assets and information, to prevent it being removed from the premises without prior authorisation. Should removal of assets take place then records are retained to ensure approved third parties are used, and security arrangements are implemented.

A.11.2.6 Security of equipment and assets off-premises

Assets taken off site are to be risk assessed by authorised personnel to ensure they are secure and cannot be compromised. Information is retained within the **Inventory of Assets** and includes controls for remote working devices and removable media. This is also addressed in the documented mobile device policy and the teleworking policy.

Demo Company Limited		
Equipment		
ISO/IEC 27001:2013		
Issue 1	A.11.2.1 Equipment siting and protection. A.11.2.2 Supporting utilities A.11.2.3 Cabling security A.11.2.4 Equipment maintenance A.11.2.5 Removal of assets A.11.2.6 Security of equipment and assets off-premises. A.11.2.7 Secure disposal or re-use of equipment A.11.2.8 Unattended user equipment A.11.2.9 Clear desk and clear screen policy	Authorised By:- Directors of Demo Company Limited
Page 3 of 3	Effective Date: 1st Nov 2021	Classification:- Internal
Issue Date: 1st Nov 2021		Last Review Date: 1st Nov 2021

A.11.2.7 Secure disposal or re-use of equipment

Inventory of Assets refers to the method of disposal and includes a statement the assets are not reused. Third party providers are used for secure disposal and information and licenced software removed prior to disposal. Records are retained to evidence correct controls are applied. The organisation has a documented disposal procedure for items which may contain sensitive information including removable media. Upon termination or change of employment assets are returned to the organisation and prepared to ensure information is not compromised should equipment be re used.

A.11.2.8 Unattended user equipment

Users are required to protect equipment which includes termination of active sessions when finished logging off and securing devices when not in use.

A.11.2.9 Clear desk and clear screen policy

The organisation requires that electronic and hard copy information is protected from unauthorised personnel which requires users of such information to lock computer screens when not attended, locking away of sensitive information when not required, removal of information from printers without delay or the use of PIN controls.