Demo Company Limited		
Operations Security		
ISO/IEC 27001:2013		
Issue 1	**A.12.1.1 Documented operating procedures** **A.12.1.2 Change management** **A.12.1.3 Capacity management** **A.12.1.4 Separation of development, testing and operational environments.**	**Authorised By:- Directors of Demo Company Limited**
Page 1 of 2	**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 documented operating procedures, change management, capacity management, separation of development, testing and operational environments.

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.12.1.1 Documented operating procedures

Operating procedures have been developed and documented as part of the information security management systems which are available to authorised persons within the shared drive.
Documented processes include controls to address requirements of ISO 27001 Annex A controls.

This are issued as controlled documents with status and control detailed within each header control.

Controls	Annex A	Controls	Annex A

A.12.1.2 Change management

The organisation has a documented change management process which details formal controls including authorisation and recording of changes and is also detailed in organisation of information security section 6.1.5. The process also assesses changes including installation of software that may introduce technical vulnerabilities detailed in section 12.6.1 of the technical vulnerability management document.

This requires identification and recording of changes, planning, and testing, assessment of security impacts, verification, communication to interested parties, roll back and emergency change controls also addressed with the information security incident management policy.

The documented procedure separation of environments procedure defines controls applied when introducing changes to the live environment through development and testing.

A.12.1.3 Capacity management

The organisation carries out regular monitoring of resources including human, technological and procurement to ensure projections for future requirements are assessed and action agreed.

This is particularly focused on critical systems and includes disk space, decommissioning, bandwidth, facilities, and optimisation of scheduling.

A.12.1.4 Separation of development, testing and operational environments.

This section is addressed through the documented separation of environments procedure.