Demo Company Limited		
Physical and environmental security		
ISO/IEC 27001:2013		
Issue 1	**A.11.1.1 Physical security perimeter** **A.11.1.2 Physical entry controls** **A.11.1.3 Securing offices, rooms, and facilities** **A.11.1.4 Protecting against external and environmental threats.** **A .11.1.5 Working in secure areas.** **A.11.1.6 Delivery and loading areas**	**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 physical security perimeter, physical entry control, securing offices, rooms, and facilities, protecting against external and environmental threats working in secure areas delivery and loading areas.

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.11.1.1 Physical security perimeter

The organisation operates within secured premises and have installed visitor controls. This allows the business to record and track visitor events.

Perimeter protection includes …….

Reception area is controlled by …….

Physical barriers against extreme weather events …….

Fire doors are alarmed and tested …….

Intruder protection consists of ……. and tested/ maintained.

Servers and communications are protected by …….

A.11.1.2 Physical entry controls

Entry to processing facilities require ……. allowing authorised personnel entry only and logs are retained detailing access approvals and control of visitors.

Secure areas require 2FA.

Visitors and contractors are required to wear identification authorising entry which must be always visible.

Restricted access maybe required to secure areas for maintenance and repairs during which authorised personal accompany the contractors.

Access rights are regularly reviewed see 9.2.5 and 9.2.6

A.11.1.3 Securing offices, rooms, and facilities

The organisation has identified secure areas consisting of ……. which are protected by …….

The business has developed a key holders and end of day procedure to ensure specific areas are inspected prior to lock up. This allows the reporting of failed lock up procedures to be identified and reported.

A.11.1.4 Protecting against external and environmental threats.

Demo Company Limited		
Physical and environmental security		
ISO/IEC 27001:2013		
Issue 1	**A.11.1.1 Physical security perimeter** **A.11.1.2 Physical entry controls** **A.11.1.3 Securing offices, rooms, and facilities** **A.11.1.4 Protecting against external and environmental threats.** **A .11.1.5 Working in secure areas.** **A.11.1.6 Delivery and loading areas**	**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**

The organisation has carried out a risk assessment of external and environmental threats including fire, flood, extreme weather events and man-made events and has applied controls to protect information assets.

A.11.1.5 Working in secure areas.

The organisation has identified secure areas consisting of …….. which are protected by …….. Work in these areas is restricted to authorised personnel and secured when not in use.

A.11.1.6 Delivery and loading areas

The organisation has identified specific areas to allow deliveries and applied controls to ensure access main processing facilities is not accessed.

Deliveries are inspected and suspicious or damaged or tampered with items are immediately segregated and reported to the management team.