| Demo Company Limited | | |
|---|---|---|
| **Information security aspects of business continuity management** | | |
| **ISO/IEC 27001:2013** | | |
| **Issue 1** | **A.17.1.1 Planning information security continuity**<br>**A.17.1.2 Implementing information security continuity.**<br>**A.17.1.3 Verify, review, and evaluate information security continuity.**<br>**A.17.2.1 Availability of information processing facilities** | **Authorised By:- Directors of Demo Company** |
| **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 planning information security continuity, implementing information security continuity, verify, review, and evaluate information security continuity.

**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.17.1.1 Planning information security continuity**

Should adverse conditions occur resulting in significant disruption to normal business activities the organisation has developed a business continuity/disaster recover plan which includes the protection of information. There is a documented information backup policy which applies controls to ensure regular backing up of information to enable the recovery of information in adverse situations. The organisation has risk assessed potential external and environmental threats which is documented in physical and environmental security section 11.1.4.

| Demo Company Limited | | |
|---|---|---|
| **Information security aspects of business continuity management** | | |
| **ISO/IEC 27001:2013** | | |
| **Issue 1** | **A.17.1.1 Planning information security continuity**<br>**A.17.1.2 Implementing information security continuity.**<br>**A.17.1.3 Verify, review, and evaluate information security continuity.**<br>**A.17.2.1 Availability of information processing facilities** | **Authorised By:- Directors of Demo Company** |
| **Page 2 of 2** | **Effective Date: 1st Nov 2021** | **Classification: - Internal** |
| **Issue Date: 1st Nov 2021** | | **Last Review Date: 1st Nov 2021** |

**A.17.1.2 Implementing information security continuity.**

The business continuity/disaster recovery plan is documented and includes management responsibilities, incident management team, information continuity objectives including response and recovery, maintaining of information security controls and other controls applied where adverse situation do not allow usual controls to be applied.

**A.17.1.3 Verify, review, and evaluate information security continuity.**

The business continuity/disaster recovery plan is verified and tested regularly to ensure information security policies and controls are effective under adverse conditions. These tests are carried out against a rolling program, are risk based and results documented including recommended changes where required.

**A.17.2.1 Availability of information processing facilities**

The business continuity/disaster recovery plan includes the testing of information systems availability to ensure levels of redundancy can be identified and where appropriate improved.

This includes failover works as intended IE the invoking of a disaster recovery site and its ability to operate as intended.