# INFORMATION SECURITY CONTINUITY PLANNING (TIER 2)

## 1 Scope

This procedure applies to all business continuity planning in MBP Pvt Ltd.

## 2 Responsibilities

The Chief Information Security Officer is responsible for ensuring that all information security issues have been included and appropriately treated in these information security continuity plans and is also responsible for information security continuity risk assessments.
Manager/Executive responsible for key processes are also responsible for identifying and implementing the steps necessary for their continuity.
The Finance Head is responsible for insurance, financial, accounting and legal aspects of the information security continuity plans.
The Head of HR is responsible for including Information Security Continuity responsibilities (where appropriate) in job descriptions.

## 3 Procedure

### 3.1 Information security continuity management process (ISO27002 Clause 17.1.1)

3.1.1 Information security continuity is integrated with business continuity.
3.1.2 Information security requirements for continuity are at least equal to those during ordinary operation.
3.1.3 Each of the critical outward and inward facing information security processes is identified and listed, in order of criticality, in MBP Pvt Ltd Business Continuity Plan (ISMS-C DOC 17.1.1a).
3.1.4 The critical information assets that are involved in each process are identified and cross-referenced to the asset registers (see control section 8.1.1).
3.1.5 For each of the services, identify the risks (from disasters, security or equipment failures, loss of service, attacks, and loss of service availability) that MBP Pvt Ltd is facing, in line with ISMS-C DOC 17.1.2.
3.1.6 Identify, for each of the risks, the possible information security continuity impacts that they will have on the business, ranging in seriousness from loss of site entrance keys through to loss of site(s).
3.1.7 As required by ISMS-C DOC 17.1.2, the risks are prioritized in terms of their impacts on MBP Pvt Ltd and the information security continuity planning process makes arrangements to tackle these risks in order.
3.1.8 The Information Security Continuity Plan (ISMS-C DOC 17.1.1a) addresses all the information continuity components of MBP Pvt Ltd activities and ensures that adequate trained resources are available to provide continuity of all the identified information security assets, including taking appropriate steps for the protection of [employees/staff] (including information processing [employees/staff]) and all information processing facilities.

# INFORMATION SECURITY CONTINUITY PLANNING (TIER 2)

**3.2 Developing and implementing continuity plans** (ISO27002 Clause 17.1.1; 17.1.2; 17.1.3)

3.2.1 MBP Pvt Ltd Information Security Continuity Plan (ISMS-C DOC 17.1.1a) is drafted by [describe how you do this] and reflects considered plans that ensure information security continuity in the event of any of the occurrences identified in the risk assessment process (ISMS-C DOC 17.1.2).

3.2.2 All the critical information security processes are identified in the plan, together with the responsibilities for restoration of service in the event of a continuity event.

3.2.3 The plan identifies the extent – for each of the critical services – to which service interruption is allowed before the continuity plan is invoked.

3.2.4 Information security continuity plans are verified, reviewed and evaluated in accordance with ISMS-C DOC 17.1.3.

3.2.5 Information security continuity plans are classified as confidential, are available only to [employees/staff] authorised by the Chief Information Security Officer (CISO) (and including members of the Emergency Response Teams).

***Document Owner and Approval***

The *Chief Information Security Officer* is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to *[all/specified]* members of staff on the *[corporate intranet]*.

This procedure was approved by the *Chief Information Security Officer (CISO)* on *[date]* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

| Issue | Description of Change | Approval | Date of Issue |
|---|---|---|---|
| 1 | Initial issue | Zamir Shaikh | 24th July 2024 |
| | | | |
| | | | |