1. **Scope**

This procedure applies to all business continuity planning in *{OrganisationName}*.

1. **Responsibilities**
   1. The *{InfoSecManager}* 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.
   2. *{Manager}* responsible for key processes are also responsible for identifying and implementing the steps necessary for their continuity.
   3. The *{CompanySecretary}* is responsible for insurance, financial, accounting and legal aspects of the information security continuity plans.
   4. The *Head of HR* is responsible for including Information Security Continuity responsibilities (where appropriate) in job descriptions.
2. **Planning information security continuity**
   1. Information security continuity is integrated with business continuity.
   2. Information security requirements for continuity are at least equal to those during ordinary operation.
   3. The critical information assets that are involved in each process are identified and cross-referenced to the asset registers.
   4. For each of the services, identify the risks (from disasters, security or equipment failures, loss of service, attacks, and loss of service availability) that *{OrganisationName}* is facing.
   5. 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).
   6. Risks are prioritised in terms of their impacts on *{OrganisationName}* and the information security continuity planning process makes arrangements to tackle these risks in order.
   7. The Information Security Continuity Plan ([ISMS-C DOC 17A](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_17A.docm)) addresses all the information continuity components of *{OrganisationName}*’s 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.
3. **Implementing information security continuity**
   1. {OrganisationName}’s Information Security Continuity Plan 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.
   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. The plan identifies the extent – for each of the critical services – to which service interruption is allowed before the continuity plan is invoked.
   4. Information security continuity plans are verified, reviewed and evaluated.
   5. Information security continuity plans are classified as confidential, are available only to Employees/Staff authorised by the *{BusinessContinuityManager}* (and including members of the *{EmergencyResponseTeams}*).
4. **Verify, review and evaluate information security continuity**
   1. It is a requirement of the Change Control Procedure ([ISMS-C DOC 12](file:///Users/matous/Desktop/QT/ISO27001-FastTrackToolkit-v1.0%20copy/Controls/ISMS-C_DOC_12.docm)) that changes to affecting information security be reflected in the information security continuity plans.
   2. Changes in business strategy, legislation, and risk (either financial or operational) are notified to the *{BusinessContinuityManager}* by the *{ChiefInfoSecOfficer}* as and when they occur, and the information security continuity plans – and their test program – are updated to take account of these changes..
   3. *{OrganisationName}*’s information security continuity plan and its sub-plans are tested in line with the timetable set out in [*name the document: you need at least a three month timetable that describes clearly your testing plan as well as records from testing that has taken place in line with your previous/current plan*].
   4. All individuals identified in that part of the plan being tested are required to be involved in the planned test; the *{InfoSecManager}* keeps an attendance record and minutes of tests that identify actions arising from the testing.
   5. The results of each test are recorded, possible improvements identified and implemented and the *{InfoSecCommittee}* reviews the minutes of business continuity tests on a [quarterly] basis.
5. **Availability of information processing facilities**
   1. Information processing facilities are implemented with redundancy sufficient to meet availability requirements, as described in ISMS-C DOC 17A.

***Document Owner and Approval***

The *{InfoSecManager}* 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]* and is published *[ ]*.

This procedure was approved by the *{ChiefInfoSecOfficer}* 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 | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |