BUSINESS CONTINUITY

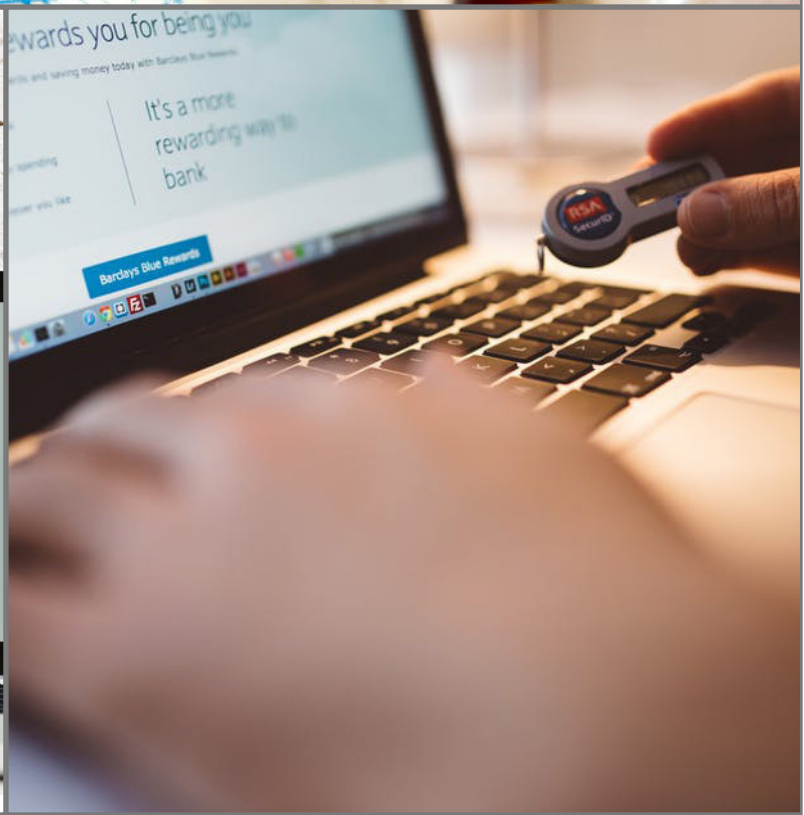

Table of Contents

Version Control

Document Reference: IL7 Security Security – Business Continuity Policy

Version	Description of change	Date	Author	Approver
0.1				

1. Introduction

An ever-increasing threat environment requires any organisation to implement appropriate measures to protect it from information security related threats and to introduce security procedures to ensure Business Continuity. IL7 Security has updated its policy status to align itself with ISO/IEC 27001:2013 in line with the approved Information Security Management System (ISMS), October 2018.

2. Purpose

The purpose of the Business Continuity Security Policy is to ensure there are standards for:

- Planning Business Continuity.
- Implementing Business Continuity Plans BCP.
- Review, verify and improving BCP.
- Built in redundancy of facilities where appropriate.

3. Audience and Scope

This policy presents the outcomes that must be delivered through standards and procedures implemented by all IL7 Security Operating Companies including Head Office for Business Continuity.

It is applicable and binding to all IL7 Security and Operating Companies employees, including Executive Management, permanent staff, contract and temporary employees.

The audience for this policy is IL7 Security and the Operating Companies.

4. Review

This Business Continuity Security policy shall be established, documented and reviewed based on business and information security requirements. It is to be reviewed annually and updated accordingly.

5. Business Continuity

Reference ISO 27001 A17.1

Planning information security continuity

Reference ISO 27001 A17.1.1

The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

An Organisation should determine whether the continuity of information security is captured within the business continuity management process or within the disaster recovery management process.

Information security requirements should be determined when planning for business continuity and disaster recovery.

In the absence of formal business continuity and disaster recovery planning, information security management should assume that information security requirements remain the same in adverse situations, compared to normal operational conditions. Alternatively, an Organisation could perform a business impact analysis for information security aspects to determine the information security requirements applicable to adverse situations.

In order to reduce the time and effort of an 'additional' business impact analysis for information security, it is recommended to capture information security aspects within the normal business continuity management or disaster recovery management business impact analysis. This implies that the information security continuity requirements are explicitly formulated in the business continuity management or disaster recovery management processes.

Implementing information security continuity

Reference ISO 27001 A17.1.2

The organisation shall establish, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

An Organisation should ensure that:

- an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence;
- incident response personnel with the necessary responsibility, authority and competence to manage an incident and maintain information security are nominated;
- documented plans, response and recovery procedures are developed and approved, detailing how the Organisation will manage a disruptive event and will maintain its information security to a predetermined level, based on management-approved information security continuity objectives.

According to the information security continuity requirements, the Organisation should establish, document, implement and maintain:

- information security controls within business continuity or disaster recovery processes, procedures and supporting systems and tools;
- processes, procedures and implementation changes to maintain existing information security controls during an adverse situation;
- compensating controls for information security controls that cannot be maintained during an adverse situation.

Within the context of business continuity or disaster recovery, specific processes and procedures may have been defined. Information that is handled within these processes and procedures or within dedicated information systems to support them should be protected. Therefore, an Organisation should involve information security specialists when establishing, implementing and maintaining business continuity or disaster recovery processes and procedures.

Information security controls that have been implemented should continue to operate during an adverse situation. If security controls are not able to continue to secure information, other controls should be established, implemented and maintained to maintain an acceptable level of information security.

Verify, review and evaluate information security continuity

Reference ISO 27001 A17.1.3

The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

Organisational, technical, procedural and process changes, whether in an operational or continuity context, can lead to changes in information security continuity requirements. In such cases, the continuity of processes, procedures and controls for information security should be reviewed against these changed requirements.

Organisations should verify their information security management continuity by:

- exercising and testing the functionality of information security continuity processes, procedures and controls to ensure that they are consistent with the information security continuity objectives;
- exercising and testing the knowledge and routine to operate information security continuity processes, procedures and controls to ensure that their performance is consistent with the information security continuity objectives;
- reviewing the validity and effectiveness of information security continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.

The verification of information security continuity controls is different from general information security testing and verification and should be performed outside the testing of changes. If possible, it is preferable to integrate verification of information security continuity controls with the Organisation's business continuity or disaster recovery tests.

Availability of information processing facilities

Reference ISO 27001 A17.2.1

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Organisations should identify business requirements for the availability of information systems. Where the availability cannot be guaranteed using the existing systems architecture, redundant components or architectures should be considered.

Where applicable, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

The implementation of redundancies can introduce risks to the integrity or confidentiality of information and information systems, which need to be considered when designing information systems.