BUSINESS CONTINUITY POLICY

Contents

1 Overview

Business Continuity Management (BCM) is the capability of IL7 Operations in being able to maintain pre-agreed "business as usual" levels, in the event of a major service disruption, due to causes including terrorist attacks and natural disasters.

IL7 supports networks that are complex, and data held on a variety of servers, storage devices and media owned and manged by a variety of teams, that may have their confidentiality, integrity and availability compromised and critical services disrupted. BCM is a risk mitigation approach to organisational resilience and involves managing risks to critical business functions to ensure continuity of service in the event of a breach or compromise being realised.

There are two significant security aspects within BCM. These are, Information Security Requirements for BCM and Information Protection during the management of an incident.

The general drivers of this policy are as follows

- The primary consideration of Security, maintenance of service availability and accuracy of information, along with Health and Safety in the event of an incident.
- The NIS Directive requires operators of essential services (OESs) and digital service providers (DSPs) that support the nation's Critical National Infrastructure (CNI) to enhance their cyber security by employing risk management and appropriate security measures, as well as measures that minimise the impact of incidents and ensure business continuity
- EU's General Data Protection Regulation (GDPR) in granting data subjects a number of new rights, requesting organisations to adopt "appropriate technical and organisational measures" to protect personal data, as well as "the ability to restore the availability and access to personal information" in the event of an incident.
- Resilience against increasing Cyber Attacks against CNI, that disrupt business operations.
- Versatile, dispersed and interconnected business delivery structures increase the number of points of failure, necessitating business continuity planning.

1.1 Purpose

This Policy supplements IL7 Business Continuity Management Policy and Guidance(Ref [1]), expanding on the requirement that IL7 systems and services *"Work closely with security, procurement and contract management teams to ensure that adequate security, information assurance and business continuity."* This Policy does not form a complete policy for the development of IL7 BCM; it focuses only on the security aspects of BCM. As such, it should be read in conjunction with the above document.

1.2 Scope

This Policy applies to all programmes, projects, systems and services depended upon by IL7 to deliver its objectives.

This document elaborates the close working with security and such, it does not pertain to the establishment of the Team's Business Continuity but to ensure that security requirements are embedded in pursuant plans.

Therefore, the scope of document is confined to the Security Aspects of Business Continuity.

1.3 Applicability

This Policy applies to Team/Programme/Project Leads.

2 Business ContinuityPolicy

It is IL7 Policy to base BCM on Business Impact Analysis of all key Business Processes identified in the Business Operating Model against a number of potential Business Continuity (BC) scenarios.

The following requirements do not establish a BC Plan or Policy but stipulates the security elements that need to be embedded in such a policies and plans.

2.1 Policy and Controls

This policy is one of several that are required to support the principles below.

- SP01 Governance and Risk Management [2]
- SP06 Operational Security [3]

This Policy, together with(Ref [1]), implements the following NIST controls that are detailed in NIST Special Publication 800-53 (Ref [4]).

CP-1	Contingency Planning Policy and Procedures
CP-2	Simulated Events
CP-2(8)	Identify Critical Assets
CP-3	Contingency Training
CP-4	Contingency Plan Testing
CP-6	Recovery Time / Point Objectives
SI-13	Predictable Failure Prevention
IR-3(2)	Coordination with Related Plans
IR-4(3)	Continuity of Operations

2.2 Procedural Policies

Policy ID	Policy Requirement
2.2.1	The requirements in this document are fully integrated with IL7 Policy suite and particularly IL7 Business Continuity Management Policy (Ref [1]).
2.2.2	The BC process will raise alerts in a security event sufficient to determine if the BC Plan is to be invoked and to recover from any disruption [NIST CP-1, IR-03(2), IR-04(3)].
2.2.3	Business critical information and assets are identified. Appropriate stakeholders and Information Asset Owners are to carry out risk assessment and plan treatment. [NIST CP-2(8)]
2.2.4	Critical operational business information assets which aim to prevent business disruptions or recovery are identified. Appropriate stakeholders and Information Asset Owners are to carry out risk assessment and plan treatment. [NIST CP-2(8), CP-6]
2.2.5	Business information and assets whose breach might affect business operations are identified. Appropriate stakeholders and Information Asset Owners are to carry out risk assessment and plan treatment. [NIST CP-2(8), CP-6]
2.2.6	Information whose compromise may cause business disruption is identified. Appropriate stakeholders and Information Asset Owners are to carry out risk assessment and plan treatment. [NIST CP-2(8), SI-13]
2.2.7	The impact of the failure of assets associated with information, such as information repositories or access mediums to critical information, are also to be considered. [NIST SI-13]
2.2.8	An emergency risk assessment during a business disruption is commissioned. The appropriate stakeholders and Information Asset Owners are to apply interim controls pertinent to the circumstances. [NIST IR-3(2)]
2.2.9	If personal data is affected, the event is managed according to operational, legal and regulatory requirements, including but not limited to GDPR (DPA18), Codes of Connections, Contracts and SLAs [NIST IR-3(2)].
2.2.10	Contingency measures are to be assessed to ensure the ongoing protection of business sensitive information and ongoing compliance with guidance as per 5.2.9. Contingency measures must not place information assets at further risk. [NIST CP-1].

Policy ID	Policy Requirement
2.2.11	Information assets identified above are included in the BC simulations. Appropriate security/cyber resources are identified and engaged in testing and training within the BCP. [NIST CP-2, CP-3, CP-4]
2.2.12	Appropriate levels of support for security audit and any security certifications and security assurance is planned for and provided.
2.2.13	The Team Security is furnished with the annual Business Continuity Review or a suitable summary of the cyber security aspects of the report.
2.2.14	The Team Security is furnished with the Lessons Learnt Review or a suitable summary of the cyber security aspects of the report.

3 Exemptions, Exceptions and Breaches

3.1 Exemptions and Exceptions Policy

All IL7 systems and personnel must make every effort to comply with the entirety of the policy set, however, in the case that either some aspect of the policy set is not applicable, or that a system or member of staff is unable to comply with it, please refer to the exemptions and exceptions policy (Ref [5])

3.2 Breach of Policy

IL7 reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this Policy. IL7 members of staff or contractors who breach this Policy may be subject to disciplinary action, including suspension and dismissal as provided for in IL7 Disciplinary Procedure.

Breaches of this Policy by a third party-managed service provider may lead to the withdrawal of IL7 information technology resources to that third-party service provider and/or the cancellation of any contract(s) between IL7 and the third party service provider.

IL7 will refer any use of its IT resources for illegal activities to t