BACK UP & RESTORE* POLICY

Contents

1 Overview

Backing up digital communications, data, and other electronic files is an essential IT practice to insure against the loss of valuable information and reduce recovery times in the event of an incident and to support the availability of services. It is IL7 policy that all data, operating systems and utility files must be adequately and systematically backed up.

1.1 Purpose

This Policy defines what is expected of IL7 to protect systems and data under its control so as to ensure that data is not lost and can be recovered in the event of an equipment failure, intentional destruction of data or a disaster.

1.2 Scope

This Policy applies to all systems and networks that receive, process, store or forward data for and on behalf of IL7, as well as all systems, networks and cloud services used in the provision of IL7 services.

1.3 Applicability

This Policy applies to all IL7 staff, service providers and contractors who develop and maintain IL7 systems.

2 Backup and Restore Policy

2.1 Policy and Controls

This policy is written to ensure that the outcomes of the following Cyber Security Principles are met:

- SP11 Core System Protection and Separation (Ref [1])

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

This policy implements the following NIST controls, which are detailed in NIST Special Publication 800-53 [2]:

CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
SC-28 (2)	Offline Storage

This policy is intrinsically linked to Business Continuity Policy and Disaster Recovery Policy and should be considered alongside them. See references [3] and [4] respectively.

2.2 Data Backup

Project Managers shall ensure that:

Policy ID	Policy Requirement
2.2.1	The data set to be backed up is specified, based on a risk assessment and impact analysis. [NIST CP-9]
2.2.2	The appropriate frequency of backups is determined, based on a risk assessment and impact analysis, for all data types stored within a system. [NIST CP-9]
2.2.3	The Recovery Point Objective and Recovery Time Objective are well understood and hence used to determine backup design requirements. [NIST CP-9]
2.2.4	All backup and restore processes are tested with appropriate frequency, and that backup facilities undergo regular on-site inspections. [NIST CP-9 (1)]
2.2.5	Consideration is given to the snapshot of operational systems alongside information backup, particularly for long term storage or to support rapid disaster recovery. [NIST CP-9 (6), CP-10, SC-28 (2)]
2.2.6	A Backup Plan is produced that accounts for: a) The information, software and systems that should be backed up; b) Recording and Documentation of all backup copies and procedures. c) The extent (e.g. full or differential backup) and frequency of backups. d) The storage location of backups. e) The physical and environmental protection of backups. f) The logical protection of backups (i.e. encryption) when the data is sensitive. g) Regular testing of backup data to ensure integrity. h) Retention period of the backups.

Policy ID	Policy Requirement
2.2.7	Backups of IL7 systems and services are provided with the same level of security as the original information, including physical aspects. [CP-9d]

2.3 Securing Back Ups

System designers shall ensure that:

Policy ID	Policy Requirement
2.3.1	All IL7 systems have backups implemented, covering configuration data as well as live data.
2.3.2	Data backups are encrypted whether at rest in the backup or in transit to it, in accordance with the Encryption Policy (Ref [5]). Exceptions to this can be granted in the event that the risk of key loss/compromise exceeds the risk of compromise of the confidentiality of data and appropriate physical security mitigation measures are put in place. [NIST CP-9]
2.3.3	Backup media are stored in a secure location that has limited physical and electronic access, and access is based on business need. [NIST CP-9]
2.3.4	All access to backup media is tracked and recorded, producing an audit trail of all such access.
2.3.5	Backups are stored in a location that is sufficiently remote from the original data, with the site being chosen following a risk assessment accounting for disasters which may simultaneously affect both locations.
2.3.6	A “3-2-1” backup strategy is used wherever possible i.e. where there will be three copies of data, two will be on site but on different mediums, and one copy will be maintained offsite.
2.3.7	Data classified as SECRET is only backed up to locations that have been assured to handle SECRET data by IL7 Security Directorate. [NIST CP-9]
2.3.8	It is determined whether systems should be considered “critical” (i.e. data must be recoverable in less than one business day from an emergency recovery request) or “non-critical” (everything else).
2.3.9	Critical systems are assessed in conjunction with IL7 Governance, Risk and Assurance team to identify if additional backup requirements are required other than those outlined in this Policy, such as Offline Storage and Redundant systems. [NIST CP-9 (6), SC-28 (2)]

2.4 Physical Security

System Administrators shall ensure that:

3	Policy Requirement
2.4.1	The physical security of the backups is managed to maintain the integrity and availability of IL7 information resources. [NIST CP-9]
2.4.2	All access to the backup location or facility is tracked and logged.
2.4.3	An inventory of backup media and services is maintained.
2.4.4	All IL7 backups are considered to have the same level of sensitivity as the original data, and are treated as such, to ensure that required handling, dissemination and disposal conditions are observed and adhered to. [NIST CP-9]
2.4.5	Data in backups is retained in accordance with IL7 Data Retention Policy (Ref [6]).
2.4.6	Destruction of backups is undertaken in accordance with the Secure Data Erasure Policy (Ref [7]) and IL7 Hardware Destruction Policy (Ref TBC) where applicable. Destruction of backups must require dual-authorisation, either procedurally or technically. [NIST CP-9 (7)]

2.5 Staff Management

Management shall ensure that:

33	Policy Requirement
2.5.1	A sufficient number of adequately trained and experienced staff members are assigned to implement and maintain IL7 backups, based on business requirements, a risk assessment, and an impact analysis.
2.5.2	Staff allocated to maintaining the backups have the relevant security clearance and authorisation to work with all information contained in the backups.
2.5.3	Staff allocated to maintaining the backups have the relevant training to undertake their duties with respect to data backups.

2.6 Backup Testing

System Administrators shall ensure that:

Policy ID	Policy Requirement
2.6.1	Backups are tested quarterly to ensure that the data is being saved correctly, can be fully restored/recovered and mirrors the original data. [NIST CP-9 (1)]
2.6.2	Any failures or issues identified during the backup test are investigated.
2.6.3	Testing the ability to restore backed-up data should be performed onto dedicated test media, not by overwriting the original media in case the backup or restoration process fails and causes irreparable data damage or loss. [NIST CP-9 (2)]

2.7 Data Restoration

System Administrators shall ensure that:

Policy ID	Policy Requirement
2.7.1	For critical systems, recovery of data takes place within the Recovery Time Objective from an emergency recovery request. [NIST CP-10 (4)]
2.7.2	For non-critical systems, and in general, recovery of data takes place within one business day of an emergency recovery request, with the understanding that this may be impossible following a catastrophic event. [NIST CP-10 (4)]
2.7.3	Any non-emergency recovery occurs within five business days, on a time-available basis. [NIST CP-10 (4)]

2.8 Help Desk

Users requiring file restoration shall:

Policy ID	Policy Requirement
2.8.1	Submit a help desk ticket request to the IT Service Desk with the following information: • Information about the file creation date. • The name of the file. • The last time the file was changed. • The date and time it was deleted or destroyed. Justification as to why they require the data restored.

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 [8])

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 the Police.