Security Standard - Backup and Recovery (SS-035)

Chief Security Office

Date: 30/08/2023

Department for Work & Pensions

This Backup and Recovery Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Department are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards.

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

2. Revision History

Version	Author	Description	Date
1.0		First issue	15/05/2023
1.1		11.1.7 Backup testing every 12 months in line with IT Service Continuity Mgmt. 11.5.2 'Secure network' replaced with 'secure protocols' 11.9 Added requirements for Backups in Cloud Environments	30/08/2023

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	15/05/2023
1.1		Chief Security Officer	30/08/2023

This document will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted "final" status, and at yearly intervals thereafter.

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by first-line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. L].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions Process

In this document the term **"must"** is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

Such exception requests will invoke the Risk Management process to clarify the potential impact of any deviation to the configuration detailed in this standard.

Exceptions to the standard **must** be maintained on a risk register for accountability, traceability, and security governance reporting to senior management.

6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications that require backup and recovery.

7. Accessibility Statement

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

This Backup and Recovery Security Standard defines the minimum technical security measures that **must** be implemented in backup solutions (both virtual and physical) to effectively secure operational systems, in order to protect against potential compromises occurring on those systems.

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e., guidance published by NIST, CIS and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third-party providers, such as the CIS Critical Security Controls v8 controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- protect citizen and operational data stored and processed within Authority systems.
- ensure security controls that are applicable to backup and recovery activities are implemented consistently across the Authority and by third party providers.
- minimise risks from known threats (physical and logical, including ransomware), to an acceptable level.
- support the achievement of the security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF), and are enabled by the implementation of controls from the CIS Critical Security Controls v8 controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure systems and services requiring backup and recovery capabilities are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard also serves to provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

This standard applies to all systems and services within the Authority and supplier base (contracted third party providers) that are required to make use of backup and recovery capabilities (both virtual and physical), for the purposes of delivering applications and services that handle Authority data.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

10.1 Out of Scope

For guidance on high availability cloud services, the following standards **must** also be consulted in conjunction with this Backup & Recovery standard:

- SS-023 Cloud Computing Security standard [Ref. A]
- SS-025 Virtualisation Security standard [Ref. B]

The following elements are not addressed in this standard;

- Hard copy records management is covered by the DWP Information Management Policy [Ref. C].
- Optical media as it is not recommended for backup and recovery purposes.
- Specific architectural design requirements are not included in this standard.

11. Minimum Technical Security Measures

The following section defines the minimum-security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

11.1 Backup Principles

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Data that requires backup, **must** be identified, classified, inventoried, and protected in line with SS-015 Malware Protection Security Standard [Ref. K]. Backup tooling may utilise native anti-malware capabilities.	ID.AM-2 ID.AM-5 PR.DS-1
11.1.2	A backup plan (or schedule) **must** be created in accordance with availability requirements of the data in scope. A Low Level Design (LLD) should support the backup implementation.	PR.IP-4
11.1.3	Backup requirements **must** be disseminated and available before a system enters production/live environment.	PR.IP-4
11.1.4	Backup operations **must** be monitored in accordance with SS-012 Protective Monitoring Security Standard [Ref. D].	PR.IP-4
11.1.5	All systems and data in scope **must** have recovery time objectives (RTO) and recovery point objectives (RPO) defined and documented, along with a retention period that supports these.	PR.IP-4
11.1.6	Backup plans **must** be reviewed every 15 months at a minimum to ensure that all identified requirements are met including but not limited to: • business objectives • capacity and performance • contractual obligations	PR.IP-4
11.1.7	The backup plan (or schedule) **must** detail; • a process to request recovery or copy of backups • whom **must** carry out backups • what data requires backup • how frequently data **must** be backed up • how data **must** be backed up • how verification of backups **must** be achieved • security measures that **must** be applied to the backup data • where encryption is utilised to protect the data, it **must** be implemented in accordance with SS-007 Use of Cryptography Security Standard [Ref. E]	PR.IP-4 PR.IP-10

	• backup procedures • restoration procedures • tests of the backup process and procedures (which **must** be conducted at least every 12 months in line with IT Service Continuity Mgmt.) • an IT disaster recovery plan • recovery time objectives (RTO) and recovery point objectives (RPO) • Retention periods, that **must** align with and enable the RPO of the target system • the frequency of the off-site backup process, where applicable, and • justification in the backup plan (or schedule) • must be reviewed every 18 months to ensure they are still appropriate and can deliver the recovery time objectives (RTO) and recovery point objectives (RPO)	

11.2 Monitoring of Backup Processes

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Backup activities **must** have the ability to produce reports and alerts related to the status of the backup activity as required.	PR.IP-4
11.2.2	Backup failure reports **must** be acted upon.	PR.IP-4
11.2.3	Backup processes **must** include the validation and confirmation of the integrity of data.	PR.IP-4 PR.DS-6
11.2.4	Backups (and their recovery processes) **must** be tested at least every 15 months to ensure business data can be recovered successfully.	PR.IP-4

11.3 Protection of Backups and Media

The data stored in the backup environment attracts the same classification as data in a live/production environment.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	This standard addresses the requirements of data classified at the OFFICIAL tier of the HMG Government Security Classifications. Any requirements to handle data above that classification should be referred to the Authority. The backup media **must** be protected in line with the DWP Information Management Policy [Ref. C].	PR.IP-4
11.3.2	Backup data **must** be stored data in a UK location.	PR.IP-4
11.3.3	Storage of backup media **must** be in line with Authority data handling procedures.	PR.IP-4
11.3.4	There **must** be robust environmental controls separating back up from the live environment in line with the DWP Physical Security Policy [Ref. G].	PR.IP-4
11.3.5	Sufficient storage capacity **must** be available to take a backup.	PR.IP-4
11.3.6	Where sufficient storage capacity is not available to take a backup, a risk **must** be recorded, understood, and analysed, and assigned to a Risk Owner so that appropriate mitigations can be identified.	ID.RA-1
11.3.7	Access controls for backup administrators **must** be detailed and maintained, in line with SS-001 (part 2) Privileged User Access Security Standard [Ref. F].	PR.IP-4
11.3.8	Sensitive data **must** be encrypted in transit and at rest. When at rest, file level encryption **must** be implemented where the Official data value requires it, this will align with the consuming production service, in line with SS-007 Use of Cryptography Security Standard [Ref. H].	PR.IP-4
11.3.9	Environment related events **must** be monitored for corruptions and failures, with appropriate action taken to resolve in line within agreed operating parameters.	PR.IP-4
11.3.10	Backup datasets and media **must** be retained in accordance with the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of the target system.	PR.IP-4

11.4 Management of Media

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	The media **must** not exceed the manufacturers usage recommendations.	PR.IP-4
11.4.2	The media **must** be stored in a physical environment in line with the DWP Physical Security Policy [Ref. G] and manufacturer's recommendations.	PR.IP-4
11.4.3	A process for recovery **must** be documented, audited, and tested, including with suppliers where appropriate	ID.SC-5 PR.IP-4 PR.IP-10
11.4.4	The destruction of any media that is damaged **must** follow SS-036 Sanitisation and Destruction Security Standard [Ref. I], where appropriate. Magnetic tape may degrade over time. This can corrupt or destroy data backed up to this type of media	PR.IP-4

11.5 Requirements for Backups

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Encryption procedures **must** be followed prior to transport of files over the network, in accordance with SS-007 Use of Cryptography Security Standard [Ref. H].	RC.RP-1 RC.IM-1 RC.IM-2
11.5.2	Encrypted backup files **must** be transported using secure protocols in line with SS-007 Use of Cryptography Security Standard [Ref. H].	RC.RP-1 RC.IM-1 RC.IM-2
11.5.3	Backup files **must** be processed and stored in an Authority approved secure network environment.	RC.RP-1 RC.IM-1 RC.IM-2
11.5.4	Backup files **must** be protected from unauthorised access, modification, or destruction.	RC.RP-1 RC.IM-1 RC.IM-2

11.6 Recovery of Backups and Backup Media

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	The highest classification of data within the recovery environment must be identified. This standard addresses the requirements of data at the OFFICIAL tier. Any requirements to handle data above that classification **must** be referred to the Authority. The media must be protected in line with the DWP Information Management Policy [Ref. C].	PR.IP-4
11.6.2	Data **must** be decrypted and recovered within an Authority approved, secure network environment, commensurate with its security classification.	RC.RP-1 RC.IM-1 RC.IM-2
11.6.3	Encryption/decryption procedures **must** be referred to whilst the recovery process is invoked. The procedures must be in line with SS-007 Use of Cryptography Security Standard [Ref. H].	RC.RP-1 RC.IM-1 RC.IM-2
11.6.4	Access to the recovered data **must** be restricted to authorised personnel in line with SS-001 (part 2) Privileged User Access Security Standard [Ref. F].	RC.RP-1 RC.IM-1 RC.IM-2
11.6.5	Encrypted backup files **must** be transported over a secure network, in line with SS-007 Use of Cryptography Security Standard [Ref. H].	RC.RP-1 RC.IM-1 RC.IM-2
11.6.6	All systems must have documented response and recovery plans in place and managed.	PR.IP-9

11.7 Monitoring of Recovery Processes

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Recovery activities **must** have the ability to produce reports and alerts related to the status of the recovery activity as required.	RC.RP-1 RC.IM-1 RC.IM-2 RC.CO-3
11.7.2	Recovery processes **must** include the validation and confirmation of the integrity of data.	PR.DS-6 RC.RP-1 RC.IM-1 RC.IM-2 RC.CO-3
11.7.3	Recovery jobs that fail **must** be acted upon.	RC.RP-1 RC.IM-1 RC.IM-2

		RC.CO-3
11.7.4	Recovery / Backup plans **must** be updated on at least an annual basis.	RC.RP-1 RC.IM-1 RC.IM-2 RC.CO-3

11.8 Requirements for Backup Deletion and Destruction

Where backup data must be stored, protection from unauthorised access, corruption, and availability issues **must** be in place. Backups can include copies of data and snapshots, amongst others.

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	The backup and recovery teams **must** establish a deletion procedure in line with SS-036 Sanitisation and Destruction Security Standard [Ref. I].	RC.RP-1 RC.IM-1 RC.IM-2

11.9 Requirements for Backups in Cloud Environments

Application does not require backup – only the data. Backup responsibility lies with System or Service Owners.

Ref	Minimum Technical Security Measures		NIST ID
	Cloud Service Provider (CSP) Responsibility	**Authority/System Owner (SO) Responsibility**	
11.9.1	Where the CSP provides a backup service, SOs **must** be provided with assurances that backups are appropriately protected and have a data recovery ability or reversion that supports the Recovery Point Objective of the target system.	(No additional security measures)	PR.IP-4
11.9.2	The CSP **must** include the following specifications for backup capabilities: ○ scope and schedule of backups ○ backup methods and data formats, including encryption, if relevant ○ retention periods for backup data ○ procedures for verifying integrity of backup data ○ procedures and timescales involved in restoring data from backup ○ procedures to test the backup capabilities ○ storage location of backups	Where supported by the CSP, the Authority Backup & Recovery Service **must** be used to perform backups. • The Authority Backup & Recovery Service Owner must ensure that the service can deliver capability at a level to meet the general requirements of the Authority • The Authority System Owners' responsibility is to ensure that the scope of backup and the policy applied meets the specific Service Recovery Objective	PR.IP-4
11.9.3	The CSP **must** provide secure and segregated access to backups, such as virtual snapshots, if such services are provided.	If the CSP does not provide backup capabilities, the SOs **must** be responsible for implementation and management of their own backups, in line with the requirements outlined in this standard.	PR.IP-4

12 Appendices

Appendix A – Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 1 – List of Security Outcomes Mapping

NIST Ref	Security Outcome (sub-category)	Related Security measure
ID.AM-2	Software platforms and applications within the organization are inventoried	11.1.1
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	11.1.1
ID.RA-1	Asset vulnerabilities are identified and documented	11.3.6
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	11.4.3
PR.DS-1	Data-at-rest is protected	11.1.1
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.2.3, 11.7.2
PR.IP-4	Backups of information are conducted, maintained and tested	11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.3.1, 11.3.2, 11.3.3, 11.3.4, 11.3.5, 11.3.7, 11.3.8, 11.3.9, 11.3.10, 11.4.1, 11.4.2, 11.4.3,

		11.4.4, 11.6.1, 11.9.1, 11.9.2, 11.9.3
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	11.6.6
PR.IP-10	Response and recovery plans are tested	11.1.7, 11.4.3
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident	11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.7.1, 11.7.2, 11.7.3, 11.7.4, 11.8.1
RC.IM-1	Recovery plans incorporate lessons learned	11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.7.1, 11.7.2, 11.7.3, 11.7.4, 11.8.1
RC.IM-2	Recovery strategies are updated	11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.7.1, 11.7.2, 11.7.3, 11.7.4, 11.8.1
RC.CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	11.7.1, 11.7.2, 11.7.3, 11.7.4

Appendix B Internal References

Below, is a list of internal documents that **should** be read in conjunction with this standard.

Table 2 – Internal References

Ref	Document	Publicly Available*
A	SS-023 Cloud Computing Security standard	Yes
B	SS-025 Virtualisation Security standard	Yes
C	DWP Information Management Policy	Yes
D	SS-012 Protective Monitoring Security Standard	Yes
E	DWP Security Classification Policy	Yes
F	SS-001 (part 2): Privileged User Access Security Standard	Yes
G	DWP Physical Security Policy	Yes
H	SS-007 Use of Cryptography Security Standard	Yes
I	SS-036 Sanitisation and Destruction Security Standard	Yes
J	SS-002 Public Key Infrastructure & Key Management Security Standard	Yes
K	SS-015 Malware Protection Security Standard	Yes
L	Security Assurance Strategy	No

Requests to access non-publicly available documents **should be made to the Authority.*

Appendix C External References

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 3 – External References

External Documents List
CIS Critical Security Controls v8 controls set
NIST – Cyber Security Framework – 2018-04-16
NIST – 800-53 – Rev 5 – Security and Privacy Controls for Information Systems and Organisations
NIST Special Publication 800-209 – Security Guidelines for Storage Infrastructure
ISO/IEC 27001:2013
Government functional standard GOVS 007 security

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition	Owner
CMDB	Configuration Management Database	Industry term
DWP	Department of Work and Pensions.	UK Government
GSCP	Government Security Classification Policy	UK Government
ISO	International Organization for Standardization	Industry term
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government

Appendix E Glossary

Table 5 – Glossary

Term	Definition
Backup plan	Identify what information is for backup, from where and to what location and frequency
IT Disaster recovery plan	Identify recovery steps and who is responsible for co-ordination of them, if the technology in use, becomes unavailable.
Media	Portable electronic media, such as disks, tapes, flash drives
RPO	Recovery point objective – 'the point in time to which data **must** be recovered after an outage.' (as per NIST definition)
RTO	Recovery time objective – 'the overall length of time an information system's components can be in the recovery phase before negatively impacting the organisations mission or mission business processes' (as per NIST definition)

Appendix F Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility

https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps