Security Standard –

Data Loss Prevention

(SS-020)

Chief Security Office

Date: 20/05/2026

Department for Work & Pensions

This Data Loss Prevention 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	denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	denotes a description.

1. Contents

2. Revision History

Version	Author	Description	Date
1.0		First published version	20/05/2026

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	20/05/2026

This document is continually reviewed to ensure it is updated in line with risk, business requirements, and technology changes, and will be updated at least every 2 years - the current published version remains valid until superseded.

4. Compliance

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

- controls tests performed by 1st 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. H].
- Formal audits conducted by the Authority 's second and third lines of defence.
- Penetration testing designed to circumvent DLP controls.

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

5. Exceptions Process

(Important) this paragraph contains ‘must’ activities.

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 to 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 limited to, solution architects, security architects, domain architects, technical engineers, developers, security teams, security operations teams, project teams, and suppliers engaged in the design, development, implementation, and operation of systems, services, and applications that handle Authority data.

7. Accessibility Statement

(Important) this paragraph contains ‘must’ activities.

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

8. Introduction

(Important) this paragraph contains '**must**' activities.

Data Loss Prevention (DLP) is a strategic capability, encompassing a set of practices and technical controls, designed to prevent the unauthorised disclosure, alteration, or extraction of the Authority's data assets.

The requirement for a formal, Authority -wide DLP strategy is driven by three key factors;

- The evolving threat landscape where adversaries are increasingly focused on data exfiltration and extortion.
- The Authority's 2030 Business Strategy, which sets the ambition to become a data-driven organisation, places a critical reliance on the robust protection of our data.
- As an operator of Critical National Infrastructure, the Authority must demonstrate a mature and auditable data protection capability to meet its obligations under the NCSC Cyber Assessment Framework (CAF) as part of the GovAssure process.

Historically, DLP requirements have not been explicitly defined within Authority policy, leading to a fragmented and siloed approach. This standard addresses that gap by defining the minimum baseline requirements for a consistent, end-to-end DLP capability.

The requirements within this standard are founded on core principles, including:

- a data-centric security model,
- defence-in-depth,
- strict adherence to least privilege,
- and business-aligned automation.

These principles, detailed in Section 11.1, **must** guide the planning, implementation, and operation of all Authority controls.

9. Purpose

The purpose of this standard is to ensure systems and services are designed, configured, deployed, and managed consistently to prevent the unauthorised disclosure, alteration, or exfiltration of Authority data. It defines the minimum mandatory technical requirements to protect Authority information assets across all systems, networks, applications, endpoints, and cloud environments. This standard forms a key component of the Authority's strategic DLP capability and also serves to provide a baseline against 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

(Important) this paragraph contains '**must**' activities.

This standard applies to all Authority systems, services, and environments that handle, process, store, or transmit electronic Authority data. It applies to all Authority employees, contractors, and third-party suppliers with access to this data.

Prioritisation of Requirements:

Implementation of the requirements defined in this standard must be prioritised based on the sensitivity of the data assets handled.

- Systems processing Sensitive Data Assets (as defined in Appendix G) must implement all mandatory ('must') requirements defined in Section 11 prior to entering operational service.
- Systems processing only standard OFFICIAL data may implement requirements iteratively, subject to a risk assessment approved by the relevant Data Owner.

This standard must be implemented in conjunction with:

- SS-007: Use of Cryptography (for key management)
- SS-012: Protective Monitoring (for SIEM integration)
- SS-023: Cloud Computing (for CASB requirements)

11. Minimum Technical Security Measures

(Important) this paragraph contains '**must**' activities.

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 Core Principles

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Controls **must** focus on the data itself, based on its content regardless of location, application, or user, and **must** address unauthorised, accidental or deliberate exposure of data, recognising that confidentiality controls (e.g. encryption) do not always mitigate data loss risk.	PR.DS-01 PR.DS-02 PR.DS-10
11.1.2	DLP can form part of a layered security approach combining preventative, detective, and corrective controls (Defence-in-Depth).	DE.CM-09
11.1.3	DLP implementations **must** be aligned with business priorities and business risk, with the ongoing involvement of business stakeholders throughout the planning, implementation, and operation of DLP controls (Business Engagement).	GV.OC-02 GV.PO-02

11.1.4	Access to sensitive data and the ability to transfer it outside of controlled environments **must** be strictly limited to the minimum level required for an individual to perform their legitimate business function (Least Privilege & Need-to-Know). See SS-001 (parts 1 and 2) Access and Authentication and Privileged User Access. [Refs. H & I]	PR.AA-05
11.1.5	DLP policies **must** be enforced by automated technical controls to minimise reliance on human intervention, reduce error, and enable real-time response. Any exceptions to this requirement **must** be governed by Digital Design Authority.	PR.DS-01 PR.DS-02 PR.DS-10

11.2 Data Governance and Classification

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	The Department **must** enforce the Government Security Classifications Policy (GSCP) via automated technical controls. DLP solutions **must** be configured to ingest and act upon metadata labels applied by the Department's classification tooling.	GV.PO-02 PR.DS-01 PR.DS-02 PR.DS-10
11.2.2	Data classified as OFFICIAL-SENSITIVE or above **must** be subject to a "Default Deny" policy for external sharing. DLP controls **must** automatically block the transmission of this data to non-HMG domains, however exceptions can be considered for encrypted transmissions.	PR.DS-02

11.2.3	The effectiveness of these controls in correctly identifying and classifying sensitive data **must** be periodically audited to ensure accuracy and completeness, in line with NCSC guidance to "know your data".	GV.OV-03 ID.IM-01

11.3 Endpoint Requirements (Data-in-Use)

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	All Authority-managed user endpoint devices (e.g. desktops, laptops) that are approved to handle data at OFFICIAL-SENSITIVE **must** have technical controls, managed via a central solution, to block or, where a business need is proven via risk assessment, to log and alert on the writing of data to external devices that have been approved for data transfer. This aligns with ISO 27002:2022 Control 8.12 and refers to measures relating to external devices found in SS-015 Malware Protection Standard [Ref. C] and SS-036 Secure Sanitisation and Destruction Standard [Ref. G].	PR.DS-10 PR.PS-04 DE.CM-03
11.3.2	For roles handling sensitive personal data, technical controls **must** be implemented to detect or prevent unauthorised actions such as cut/copy/paste functions, screen capture tools, and the printing of bulk sensitive data.	PR.DS-10 PR.PS-04 DE.CM-03

11.3.3	All Authority data moving from a higher security system to a system with lower security controls **must** be masked by default unless a specific business justification is approved, in line with the Data Obfuscation Policy [Ref. K].	PR.DS-01 PR.DS-02 PR.DS-10

11.4 Network and Email Requirements

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	All internet gateways and connections to third-party services, **must** be monitored by a content-aware DLP solution, unless the source application has native DLP capabilities built in.	DE.CM-01 DE.CM-06
11.4.2	Any DLP solution **must** be capable of inspecting unencrypted traffic and using multiple detection techniques—such as described content matching (for patterns like National Insurance numbers), data fingerprinting (for structured data forms), to identify and block or alert on unauthorised transmissions, in line with SS-006 Security Boundaries Standard [Ref. N]. This aligns with the principles of NIST SP 800-53 AC-4 and CIS Control 3.	PR.DS-02 DE.CM-01 DE.AE-02
11.4.3	Where traffic is encrypted, DLP controls **must** be enforced prior to encryption (e.g. at endpoint, application, or email gateway) and supported by policy-based allow-listing and governance controls. Since encrypted traffic may only be inspected at the endpoints, the robustness and effectiveness of endpoint based DLP controls **must** be regularly assessed.	GV.PO-02 PR.DS-01

11.4.4	Where the Authority deploys client or cloud-based encryption solutions, e.g. to implement a zero trust network access solution, these solutions **must** be able to enforce DLP policies for traffic that has not been encrypted at an application level.	PR.DS-02
11.4.5	Any corporate email gateway **must** be configured with appropriate DLP policies that could include; • bulk-threshold detection e.g. large volumes of data • sensitive data type matching e.g. NINOs • recipient domain validation e.g. non-HMG destinations • automated blocking • quarantining • alerting capabilities. • capability to enforce encryption based on content	PR.DS-02 DE.CM-01

11.5 Cloud Application Security Requirements (SaaS/PaaS)

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	DLP controls **must** be applied on all approved cloud services in line with SS-006 Security Boundaries Standard [Ref. N]. This enforcement **must** apply to data being uploaded (in-motion) and data already stored within those services (at-rest) before data leaves the Department.	PR.DS-01 PR.DS-02

11.5.2	The formal governance process, managed by the Authority, **must** be followed for the review and approval of all new custom connectors, automated workflows, and applications built on low-code platforms.	GV.RR-02
11.5.3	This review **must** specifically assess the potential for the new custom connector, workflow, or application to create unmonitored or unauthorised data exfiltration pathways.	PR.DS-01

11.6 Insider Risk Technical Requirements

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Auditing systems **must** be configured to establish baseline profiles of normal user activity and identify anomalous behaviour patterns (e.g., mass download events, access at unusual times, or sequence of actions indicating flight risk), taking account of differing business circumstances.	ID.AM-03 DE.CM-03
11.6.2	DLP policies **must** be configured to consider risk for users identified by HR signals (e.g., leavers) to be automatically subjected to stricter DLP enforcement policies until the risk level is reduced. Exceptions **must** be raised where this requirement cannot be met.	PR.DS-01 PR.DS-10 DE.CM-03
11.6.3	Monitoring **must** be applied to all users, with a particular focus on privileged accounts. This aligns with NIST SP 800-53 AU-12 (Account Monitoring for Atypical Usage).	DE.CM-03 DE.CM-06

11.7 Incident Response and Monitoring

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	All alerts generated by DLP tools (endpoint, network, cloud, etc.) **must** be ingested into the Authority's central Security Information and Event Management (SIEM) platform, in accordance with SS-012 Protective Monitoring Security Standard [Ref. B]. For third party services, exceptions to this requirement can be raised with Digital Design Authority providing they have an equivalent capability.	PR.PS-04 DE.CM-03 DE.CM-09 DE.AE-03
11.7.2	A formal incident response plan **must** be developed and documented by the Security Incident Response Team (SIRT) and regularly tested for responding to high-severity DLP alerts.	ID.IM-04
11.7.3	This plan **must** define the specific roles, responsibilities, and communication pathways for the Security Incident Response Team (SIRT), the relevant Data Owner, business line managers, and Human Resources, in line with GovSec-007 requirements and SS-014 Security Incident Management Standard [Ref. O]. The plan should define response actions such as log, notify, quarantine, and block based on the severity of the violation.	ID.IM-04

11.8 Implementation and Rollout

(Important) this table contains '**must**' activities.

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	In alignment with the CTEM framework (see Technical Vulnerability Management Policy [Ref. L] and SS-033 Patching and Exposure Management security standard [Ref. M]), all deployed DLP control points (endpoint, network, cloud, and email) **must** be subject to continuous validation. Internal offensive security testing and independent ITHCs **must** be performed before go-live (e.g. in a staging environment) to ensure filters are configured correctly and generating appropriate SIEM alerts.	ID.IM-02
11.8.2	Implementation of DLP controls to meet the requirements of this standard **must** follow a phased, incremental approach. Initial deployment on any channel **must** begin in a 'log-only' or 'monitoring' mode to establish a baseline, identify business process impacts, and tune policies to minimise false positives.	PR.PS-04 DE.CM-09
11.8.3	Progression from 'log-only' mode to 'notify' (user education) and then to 'block' (active prevention) modes **must** be a planned process, approved by the relevant Data Owner and business stakeholders.	GV.RR-02 PR.PS-04 DE.CM-09

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
GV.OC-02	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	11.1.3
GV.PO-02	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organisational mission	11.1.3, 11.2.1, 11.4.3
GV.OV-03	Organisational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	11.2.3
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	11.5.2, 11.8.3

ID.AM-03	Representations of the organisation's authorised network communication and internal and external network data flows are maintained	11.6.1
ID.IM-01	Improvements are identified from evaluations	11.2.3
ID.IM-02	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties	11.8.1
ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	11.7.2, 11.7.3
PR.AA-05	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	11.1.4
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.1.1, 11.1.5, 11.2.1, 11.3.3, 11.4.3, 11.5.1, 11.5.3, 11.6.2
PR.DS-02	The confidentiality, integrity, and availability of data-in-transit are protected	11.1.1,11.1.5, 11.2.1, 11.2.2, 11.3.3, 11.4.2, 11.4.4, 11.4.5, 11.5.1,

PR.DS-10	The confidentiality, integrity, and availability of data-in-use are protected	11.1.1, 11.1.5, 11.2.1, 11.3.1, 11.3.2, 11.3.3, 11.6.2
PR.PS-04	Log records are generated and made available for continuous monitoring	11.3.1, 11.3.2, 11.7.1, 11.8.2, 11.8.3
DE.CM-01	Networks and network services are monitored to find potentially adverse events	11.4.1, 11.4.2, 11.4.5
DE.CM-03	Personnel activity and technology usage are monitored to find potentially adverse events	11.3.1, 11.3.2, 11.6.1, 11.6.2, 11.6.3, 11.7.1
DE.CM-06	External service provider activities and services are monitored to find potentially adverse events	11.4.1, 11.6.3
DE.CM-09	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	11.1.2, 11.7.1, 11.8.2, 11.8.3
DE.AE-02	Potentially adverse events are analysed to better understand associated activities	11.4.2
DE.AE-03	Information is correlated from multiple sources	11.7.1

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-007: Use of Cryptography	Yes
B	SS-012: Protective Monitoring	Yes
C	SS-015 Malware Protection	Yes
D	SS-017: Mobile Device Security	Yes
E	SS-018: Network Security Design	Yes
F	SS-023: Cloud Computing	Yes
G	SS-036: Secure Sanitisation and Destruction	Yes
H	SS-001-1: Access and Authentication	Yes
I	SS-001-2: Privileged User Access	Yes
J	Security Assurance Strategy	No
K	Data Obfuscation Policy	No
L	Technical Vulnerability Management Policy	Yes
M	SS-033: Patching and Exposure Management	Yes
N	SS-006: Security Boundaries	Yes
O	SS-014: Security Incident management	Yes

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 set
ISO 27002:2022
Protecting Bulk Personal Data (NCSC guidance)
NIST SP 800-53
Cyber Assessment Framework
UK Government Security – GovAssure

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
CASB	Cloud Access Security Broker
CTEM	Continuous Threat Exposure Management
CIS	Center for Internet Security
DLP	Data Loss Prevention
IaaS	Infrastructure as a service
ISO	International Standards Organisation
NCSC	National Cyber Security Centre
NHS	National Health Service
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SIEM	Security information and event management
SIRT	Security Incident Response Team
UEBA	User and Entity Behaviour Analytics
USB	Universal Serial Bus

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Low-code/no-code platforms	Platforms that enable coding via a graphical interface.

Appendix F Accessibility artefacts

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

DWP Accessibility Policy
DWP Accessibility Manual
Guidance and tools for digital accessibility
Understanding accessibility requirements for public sector bodies

Appendix G: Sensitive Data Types and Handling Matrix

This section has been redacted – please contact the Authority for details.