Security Standard – Security Incident Management (SS-014)

Chief Security Office

Date: 18/09/2024

Department for Work & Pensions

This Security Incident Management 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

1. Contents **3**
2. Revision History **4**
3. Approval History **5**
4. Compliance **5**
5. Exceptions Process **6**
6. Audience **6**
7. Accessibility Requirements **6**
8. Introduction **7**
Definition Description Table 8
Assets .... **Error! Bookmark not defined.**
9. Purpose **9**
10. Scope **10**
11. Minimum Technical Security Measures **11**
11.1 Plan and prepare against security incidents 11
11.2 Security incident detection and identification 12
11.3 Collection and Preservation of Evidence 14
11.4 Security Incident Response, Mitigation and Reporting 17
11.5 Security Incident Recovery and Remediation 19
11.6 Post Security Incident Review 20
11.7 Legal and Regulatory Requirements 20
12 Appendices **21**
Appendix A – Security Outcomes 21
Appendix B Internal References 24
Appendix C External References 24
Appendix D Abbreviations 25
Appendix E Definition of Terms 25
Appendix F Accessibility artefacts 25
Appendix G – Security Incident Report Form 26

2. Revision History

Version	Author	Description	Date
1.0		First published version	26/05/2017
2.0		Full update in line with current best practices and standards; • Updated Intro, purpose, audience, scope; added reference to CIS v8 security controls • Added NIST CSF references 11.1.1 & 11.1.2 Required details of the security incident management plan; annual testing 11.2.2 Security Incident referral form embedded 11.2.5 Contact telephone number added 11.3.2 NPCC ref added 11.3.3 DFIR professionals; cloud platform requirements 11.3.5 power down, remove from network 11.3.7 Full Disk Encryption; Encryption standard 11.3.8 Annually; DWP Information Mgmt. Policy 11.3.9 Hash algorithms added; work on copies, original evidence only with authorisation 11.3.11 NPCC guidelines; contacting NCSC/notifying the Authority 11.3.14 Anti-tampering measures; Added ref to Privileged User Standard 11.4.2 Supplier reporting requirements 11.4.3 Collation and analysis of security incidents 11.4.4 Security incident response requirements 11.5.1 Security incident recovery requirements 11.6.2 DFIR professionals; SIRT TRUST & VERIFY 11.7 Legal & Regulatory requirements	26/10/2023

2.1		All NIST references reviewed and updated to reflect NIST 2.0. Approval history - Review period changed to up to 2 years Compliance – Ref added to Security Assurance Strategy Intro – updated definitions Scope – People and property 11.1.1 Reviewed and tested 11.1.3 Suppliers, employees, contractors & temp staff 11.2.1, 11.2.2 & 11.2.5 Reference added to Appendix G 11.3.5 Into 11.6.1 Lessons identified; high or very high incidents 11.6.2 Attempted breaches in supply chain. Internal References – added Incident and Crisis Management Framework overview Appendix G – Security Incident report form	18/09/2024

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	26/05/2017
2.0		Chief Security Officer	26/10/2023
2.1		Chief Security Officer	18/09/2024

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. A].
- 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 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 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.

7. Accessibility Requirements

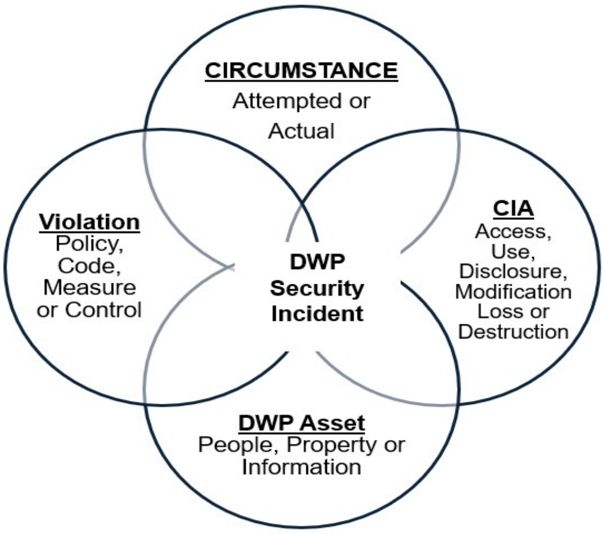
Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

This Security Incident Management Security Standard defines the minimum security measures that **must** be implemented for use within the Authority and its supplier base.

ISO/IEC27035-1 2016 defines an information *security event* as “an occurrence indicating a possible breach of information security or failure of controls” and *security incident* as “one or multiple related and identified information security events that meet established criteria and can harm an organisation’s asset or compromises its operations.”

The Authority recognises a security incident as ***“The attempted or actual unauthorised access, use, disclosure, modification, loss or destruction of an Authority asset (or a supplier asset that provides a service to the Authority) in violation of security policy.”***


CIRCUMSTANCE
Attempted or Actual
Violation
Policy, Code, Measure or Control
DWP Security Incident
CIA
Access, Use, Disclosure, Modification Loss or Destruction
DWP Asset
People, Property or Information

The security incident definition:

- is intentionally high level and intended to provide sufficient information to help everyone understand if a security incident has occurred.
- reflects the information security ‘CIA Triad’ principles of confidentiality, integrity, and availability.
- applies to all categories of security incident – including Cyber, Information, Personnel and Physical.

Definition Description Table

The description table below, offers further clarification to support understanding.

Definition	Description
Access	'Enter, obtain or retrieve.'
Actual	'Existing now; current'
Asset	In the context of this Security Incident Management Standard, the term 'asset' includes (but is not limited to): • **People** – customers, colleagues & citizens • **Property** - anything tangible or intangible which is capable of being owned • **Information** - data that is transferred, collected, created, generated, used, and/or stored
Attempted	'Makes an effort to achieve or complete.'
Destruction	'The action or process of causing so much damage to something that it no longer exists or cannot be repaired.'
Disclosure	'The action of making new or sensitive information known'
Loss	'The fact or process of losing something.'
Modification	'The act of changing something.'
Security Policy	The Authority's security and data protection policies.
Unauthorised	'Not having official permission or approval.'
Use	'Take, hold, or deploy (something)'
Violation	'An action that breaks or acts against something.'

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 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 ensure that:

- A security incident management framework is established, including specialist individuals (or teams), information, and tools required by the Authority's security incident management process.
- Security incidents must be identified, responded to, recovered from, and followed up using an approved security incident management process, in a timely fashion.
- Collaborative working and data sharing are utilised to support response activity throughout the lifecycle of a security incident to protect the Authority and its agencies and public bodies e.g., sharing information about attack vectors, Indicators of Compromise (IOCs), Tactics, Techniques and Procedures (TTPs) at the earliest opportunity and without the need for a Non-Disclosure Agreement (NDA).
- The Authority applies a risk-focused approach to security incident management. It is accepted that systems and services must have a proportionate and appropriate level of security management. This standard aims to assist in the reduction of impact from security incidents on employees, customers, citizens, information assets and other Authority assets and thereby reduce the likelihood of potential reputational damage to the Authority.
- Ensure that security incidents are managed consistently across the Authority and by third party providers where applicable.
- Support the achievement of 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 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 that Authority systems and services 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 is to cover systems handling data within the Government Security Classification Policy (GSCP). All of the Authority’s Security Incident Management implementations falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations. The security control requirements laid out in this standard are product agnostic and applicable for all information systems that are provisioned for departmental use.

The scope of this standard covers the Authority’s requirement for the identification, management and resolution of security incidents across:

a) IT infrastructure, including hardware, firmware, middleware and network devices;
b) operating systems;
c) applications;
d) network appliances (anything connected to the corporate network not included above);
e) all environments (i.e. Production, Pre-Production, Test and Development);
f) people
g) property

This standard does not replace any legal or regulatory requirements.
This standard applies to all contractual agreements for the provision of computing and networking services for the Authority and these statements supplement all currently applicable contractual agreements to Authority computing and networking services, including those provided through managed services.

This standard also applies to:

- Authority employees using, designing, implementing and running new and current IT solutions or systems (i.e. infrastructure, applications, end user devices);
- all contracted third-party suppliers, who may be required to provide or assist in the timely identification, investigation, and remediation of security incidents in business applications, systems, equipment, and devices to ensure the appropriate levels of assurance for the confidentiality, integrity, and availability of the Authority’s assets, including data;
- all Authority data, and any data that the Authority is processing for other data controllers;
- all Authority employees - who should understand their responsibilities in using the Authority’s information assets including its systems;
- Authority Contracted suppliers that handle/access/process Authority Data.

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

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 Plan and prepare against security incidents

The primary objective of this section is to pre-empt, control and manage the occurrence of security incidents. The measures below will help to reduce the likelihood and impact of security incidents.

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	A detailed security incident management plan **must** exist, which includes; • communication methods (as well as any out-of-band methods) and information disclosure; • contact details for relevant parties, such as business managers, operational specialists, technical experts and external suppliers; • service owners and/or suppliers **must** produce supporting information (e.g. event logs) within an agreed timeframe and acceptable format; • service owners, internal Authority teams, and/or suppliers **must** provide security-related event logs (e.g. those produced by applications, systems, network devices and security products); • details about affected business environments (e.g. processes, operations and applications); • technical details (e.g. network diagrams, system configurations and external network connections); • threat intelligence and the results of threat analysis The security management plan, its process and procedures **must** be reviewed and tested at least annually.	ID.IM-04 GV.SC-08

11.1.2	The security incident management plan **must** also define: • severity ratings, detailing the level and scale of disruption to critical business processes (e.g. disruption to single user, multiple users, minor systems or major systems); • impact ratings, detailing how a compromise of the confidentiality, integrity or availability of information could have an impact on the Authority, or citizens where relevant; • priority ratings, identifying how quickly the incident must be resolved based on relevant criteria (e.g. whether the affected system is customer or internet facing, severity rating, dependencies of critical systems, whether it's an easy or quick fix, and strategic importance of the affected systems).	ID.IM-04 DE.AE-08
11.1.3	Security awareness training **must** be provided to all suppliers and employees (including contractors and temporary staff) as part of induction and also as part of annual refresh security training program. Additional training **must** be provided to personnel who are involved in security incident management to ensure that their roles and responsibilities are clear and understood.	PR.AT-01

11.2 Security incident detection and identification

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	All employees **must** be familiar with the Department's "Reporting Security Incidents" process referenced from the Department's Information Management Policy [Ref. B] and Acceptable Use Policy [Ref. C] to understand what constitutes a potential security incident, how to report a security incident, and what actions they **must** and **must not** take themselves. This information is also detailed in Appendix G.	PR.AT-01

11.2.2	All security incidents identified by a Supplier having access to the Authority's data, information and system **must** be notified to the Authority as quickly as possible via a "Security Incident referral form", see Appendix G. This **must** include security incidents that are likely to have an impact on Authority (employees/citizens; Authority assets; Authority's reputation). The form should contain as much information as possible. The Authority will validate the reported incident. Suppliers **must** then email (without delay) to SECURITYINCIDENT.RESPONSETEAM-SIRT-@DWP.GOV.UK . The Authority also articulates (with direction), that if very serious, then contact the Authority directly.	RS.CO-02
11.2.3	The detection and reporting of system security events or existence of information security vulnerability **must** be automated where possible. Automated detection capabilities include network-based and host based Intrusion Detection and Prevention systems (IDPS), anti-virus software and log analysers.	DE.AE-08 ID.RA-08
11.2.4	All security incidents identified by the Authority as medium or higher **must** be actioned and attract a full Authority response. The risk rating is used by the Authority to determine the proportionate follow up action to be taken. All low rated security incidents **must** be actioned at the most appropriate management level.	RS.MA-03 RS.MA-04
11.2.5	All security incidents identified out of normal office hours **must** follow the Authority's Security Incident Management Process – Out of Hours. If known or suspected to be serious, then contact the Authority directly. For suppliers, please use the "Security Incident referral form", see Appendix G	RS.CO-02 RS.MA-02
11.2.6	All activities, results and related decisions **must** be logged and available for review. An independent third party should be able to review those processes, if required.	RS.AN-06

11.3 Collection and Preservation of Evidence

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	All digital evidence **must** have a security data classification. If for any reason the security classification of the digital evidence is not determined at the time of acquisition, then the default level **must** be comparable to the classification level of OFFICIAL-SENSITIVE until correctly classified. The digital evidence could be re-classified following initial response and triage.	ID.AM-05
11.3.2	The DWP Information Management Policy [Ref. B] and DWP Forensic Readiness Policy [Ref. C], and general forensic procedures (such as National Police Chiefs' Council [NPCC] Good Practice Guide for Digital Evidence – see External References) **must** be followed while collecting, storing and preserving the evidence.	RS.AN-07
11.3.3	All digital evidence **must** only be collected by digital forensic & incident response (DFIR) professionals, and never by system administrators or other privileged users. • Authority cloud teams and DFIR teams **must** engage and have strategies in place for data acquisition on Departmental cloud platforms. • A separate cloud security incident management process **must** be established, to include cloud security incident management plans, which **must** be developed and tested. • Cloud security incident management plans **must** include procedures for the use of cloud-native and third-party Digital Forensic Incident Response (DFIR) tools, which can be deployed on cloud environments to isolate, acquire, parse, and analyse evidence.	RS.AN-03 RS.AN-06 PR.AT-02 ID.IM-04
11.3.4	All actions taken in the collection and preservation of the evidence **must** be logged, preserved and available for review. An audit trail or other record of processes applied to digital evidence **must** be created and preserved. An independent third party **must** be able to review those processes, if required.	RS.AN-06
11.3.5	All digital evidence **must** be labelled to preserve the chain of custody. The chain of custody **must** be completed when an investigator assumes physical control of digital electronic artefacts (and any incorporated storage devices). Storage devices **must** be powered down / power source removed, and the device removed from the network if connected.	RS.AN-06 RS.AN-07

	The following information regarding the collection **must** be logged: • Description of the evidence • Time and Date the evidence was gathered • Exact location of the evidence from where it was gathered • Name of the person collecting the evidence • Relevant circumstances surrounding the collection • Any controls taken into consideration • Any analysis performed on the digital evidence • Disposition methods of evidence, where applicable • Transfer details, as per 11.3.7	
11.3.6	Each person who handles the evidence **must** sign the chain of custody log indicating the time they took the responsibility for the evidence and the time they handed off to the next person in the chain of custody. This information **must** be continuously shared with the Authority.	RS.AN-06 RS.AN-07
11.3.7	All digital evidence and the log of imaging and copying process **must** be stored in a physical secure location and with Full Disk Encryption in line with SS-007 Use of Cryptography security standard [Ref. F].	PR.DS-01 RS.AN-06 RS.AN-07
11.3.8	All digital evidence preserved securely **must** be monitored at least annually. All digital evidence **must** be reviewed, stored and destroyed in accordance with the Authority's Information Management policy.	ID.AM-08
11.3.9	All investigation and analysis of digital evidence **must** be performed on the copy, and not on the original evidence. Forensic tool **must** be used to make forensic images or copies. The hash value (SHA1 and SHA256) of the forensic image **must** be verified with the original evidence to gain assurance that the evidence has not be changed by an analysis. Additional images or copies should be made if required (for example, if evidence on the copy or image is destroyed due to forensic work, a fresh copy of the original media should be made to continue with the forensics analysis). Only working on copies preserves the integrity of the evidence. The decision to access original evidence should be made carefully, considering the potential risks and legal requirements, ensure it remains admissible in legal proceedings. Authority validation/authorisation **must** be obtained prior to working on original evidence.	RS.AN-06 RS.AN-07

11.3.10	All imaging and copying processes **must** keep the proof of the processes carried out for audit purposes.	RS.AN-06
11.3.11	All high and very high rated security incidents involving actionable crime **must** be reported to law enforcement agencies via appropriate channels. Law enforcement should be involved in the acquisition stage, but where this is not possible evidence collected by Authority digital forensics employees (or their Suppliers) should be collected in accordance with the NPCC guidelines and Chain of Custody maintained. In some case, the security data classification or evidence of an actionable crime is only known after the initial response and analysis. In those circumstances to ensure continuity is maintained, Chain of Custody and records of acquisition and analysis should be passed to the relevant law enforcement agency. Depending upon the nature of the incident, for all high and very high rated security incidents where malicious activity is identified, and assistance from NCSC is required this can be requested of the Authority via the measures described above. Alternatively, suppliers may contact NCSC directly, but they **must** still inform the Authority immediately. To ensure continuity is maintained, Chain of custody and records of acquisition and analysis should be passed to the NCSC via the Authority where necessary. In all circumstances, legal advice **must** be sought from the Authority's legal team before informing regulatory and/or law enforcement agencies.	RS.AN-06 RS.AN-08 RS.MA-01 RS.MA-04 RS.CO-03
11.3.12	All relevant and available network activity logs (such as IDPS logs, network flow data captured by a flow monitoring system, packet captures collected during an incident, firewall and other network devices logs) **must** be collected and correlated from disparate sources to support network forensic analysis.	DE.AE-03
11.3.13	All relevant and available logs from application or database servers **must** be investigated to identify signs of any malicious activity.	DE.AE-02

11.3.14	Any forensic report **must** be retained as per the Authority's Information Management Policy. The summary of findings **must** be shared with SIRT as per the security incident process. The digital forensic team may carry out a technical report after the closure of security incident solely for lessons learnt purposes. The technical report **must** be retained by the Authority and stored in a secured location with appropriate anti-tampering measures, and clear role-based access controls in line with SS001 pt.2 Privileged User Access Security Standard [Ref. E].	ID.AM-08 RS.CO-03

11.4 Security Incident Response, Mitigation and Reporting

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	All efforts **must** be undertaken to limit the effect or scope of an incident. Depending upon the nature of incident, the Authority would recommend taking containment steps on the affected system(s) to prevent any further damage to the system or the data on it. These steps would depend on the nature of the compromise/malware, and whether there is the need for preserving evidence.	RS.MI-01
11.4.2	A summary of the findings (including incident type and category, information affected and events leading up to incidents) **must** be documented and maintained on a continuous basis, using a consistent approach in a report circulated to the key stakeholders at the earliest opportunity, based on the severity rating of the security incident. All reports documenting high rated and very high rated security incidents from a Supplier **must** be informed to the Authority. There is an expectation for the Supplier to provide its own report into what happened; why; and what it is doing to ensure doesn't happen again etc. (and to provide any findings from its own internal investigation to the Authority).	RS.CO-02 RS.CO-03

11.4.3	Information about security incidents must be collated and reviewed regularly, to help: • determine patterns and trends of security incidents • understand the costs and impacts associated with incidents • assess the operational implications (e.g. the effect on the safety, reliability and availability of benefit payment systems) • identify common factors that have influenced incidents (typically by performing a root cause analysis) • determine the effectiveness of controls (e.g. which controls are better at preventing, detecting and delaying incidents or minimising the business impact of incidents) • reduce the likelihood, frequency or impact of future similar incidents • provide a comparison of internal and external incident information • improve future information risk assessments and security audits.	ID.IM-01
11.4.4	The response to information security incidents **must** include: • analysing available information, such as system, network and technical logs; • handling necessary evidence (e.g. collecting it in accordance with legal constraints and protecting it against unauthorised tampering); • investigating the cause of information security incidents, supported by specialists, such as experts in forensics and cyber incident response; • containing the information security incident (e.g. by making changes to access control systems, increasing network capacity, terminating or diverting network connections, or shutting down systems) • eradicating the cause of the information security incident • logging all actions taken • invoking crisis management or business continuity plans when a serious incident takes place.	RS.AN-03 RS.AN-06 RS.MI-01 RS.MI-02 RS.MA-04

11.5 Security Incident Recovery and Remediation

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Recovery from security incidents **must** involve (if appropriate): • postponing any planned changes to network or IT infrastructure (e.g. upgrading to a new operating system), sometimes referred to as a change freeze; • rebuilding systems or networks (and supporting IT facilities) to a previously known secure state; • restoring from information that has not been compromised by the information security incident; • enabling any transactions in progress at the point of failure to either be completed (e.g. rolled forward) or removed (e.g. using auto roll-back techniques); • verifying data being restored is accurate and complete; • closure of the information security incident.	RC.RP-01 RC.RP-02 RC.RP-03 RC.RP-05 RC.RP-06
11.5.2	Compromised systems **must** be restored to normal operation. This may include for example restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords or tightening network perimeter security. Compromised systems when rebuilt from scratch **must** be configured effectively and **must** be secured to a known good condition.	RC.RP-01 RC.RP-05
11.5.3	Once the cause of the incident is established, corrective action **must** be taken and additional controls introduced to prevent the same course of events happening again in the future. This action includes closing any vulnerability that existed and was exploited during the incident.	ID.IM-03

11.6 Post Security Incident Review

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	Post security incident/lessons identified review meetings of security incidents classified as high or very high, **must** be completed within two weeks of the security incident resolution.	ID.IM-03
11.6.2	Root-cause analysis **must** be performed by DFIR professionals and validated to identify the root cause of the security incident and confirm how the security incident happened including who and what is at risk. This requirement does not apply to attempted but unsuccessful breaches in the DWP supply chain. SIRT operates under the TRUST and VERIFY model.	RS.AN-03
11.6.3	Security incidents **must** be re-classified based on the actual impact.	RS.MA-03 DE.AE-04
11.6.4	The report of security incidents **must** be regularly reviewed as part of the information security management lifecycle to identify changes in the threat environment that might request for amendments to the security incident management plan, security risk assessment, security policy or security standards and procedures.	ID.IM-03 ID.IM-04

11.7 Legal and Regulatory Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Relevant legal and regulatory requirements **must** be identified and met during security incident response, which include: • security-related laws and regulations relevant to the incident • any specific compliance requirements (e.g. retaining information for further investigation or submitting breach notifications to affected individuals and relevant authorities) • incident reporting timescales (e.g. timeframe in which a data breach must be reported to regulatory bodies).	GV.OC-03

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

Ref	Security Outcome (Sub-category)	Related Security Measure
GV.OC-03	Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	11.7.1
GV.SC-08	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	11.1.1
ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	11.3.1
ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.3.8, 11.3.14
ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	11.2.3
ID.IM-01	Improvements are identified from evaluations	11.4.3
ID.IM-03	Improvements are identified from execution of operational processes, procedures, and activities	11.5.3, 11.6.1, 11.6.4

ID.IM-04	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved	11.1.1, 11.1.2, 11.3.3, 11.6.4
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind	11.1.3, 11.2.1
PR.AT-02	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind	11.3.3
PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected	11.3.7
DE.AE-02	Potentially adverse events are analyzed to better understand associated activities	11.3.13
DE.AE-03	Information is correlated from multiple sources	11.3.12
DE.AE-04	The estimated impact and scope of adverse events are understood	11.6.3
DE.AE-08	Incidents are declared when adverse events meet the defined incident criteria	11.1.2, 11.2.3

RS.MA-01	The incident response plan is executed in coordination with relevant third parties once an incident is declared	11.3.11
RS.MA-02	Incident reports are triaged and validated	11.2.5
RS.MA-03	Incidents are categorized and prioritized	11.2.4, 11.6.3
RS.MA-04	Incidents are escalated or elevated as needed	11.2.4, 11.3.11, 11.4.4
RS.AN-03	Analysis is performed to establish what has taken place during an incident and the root cause of the incident	11.3.3, 11.4.4, 11.6.2
RS.AN-06	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved	11.2.6, 11.3.3, 11.3.4, 11.3.5, 11.3.6, 11.3.7, 11.3.9, 11.3.10, 11.3.11, 11.4.4
RS.AN-07	Incident data and metadata are collected, and their integrity and provenance are preserved	11.3.2, 11.3.5, 11.3.6, 11.3.7, 11.3.9
RS.AN-08	An incident's magnitude is estimated and validated	11.3.11
RS.CO-02	Internal and external stakeholders are notified of incidents	11.2.2, 11.2.5, 11.4.2
RS.CO-03	Internal and external stakeholders are notified of incidents	11.3.11, 11.3.14, 11.4.2
RS.MI-01	Incidents are contained	11.4.1, 11.4.4
RS.MI-02	Incidents are eradicated	11.4.4

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	Security Assurance Strategy	No
B	Information Management Policy	Yes
C	Acceptable Use Policy	Yes
D	DWP Forensic Readiness Policy	Yes
E	SS-001 pt.2 Privileged User Access Security Standard	Yes
F	SS-007 Use of Cryptography security standard	Yes
G	Incident and Crisis Management Framework overview	Yes

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 set
National Police Chiefs' Council (NPCC) Good Practice Guide for Digital Evidence, March 2012
NIST Computer Security Incident Handling Guide Special Publication 800-61 Revision 2 August 2012
CESG Security Incident Management (GPG24) Issue No: 1.2, October 2015

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
CRC	Cyber Resilience Centre (CRC)
DA	Design Authority (DA)
Authority	The Authority refers to the Department for Work and Pensions
DFIR	Digital Forensic & Incident Response
GSCP	Government Security Classification Policy (GSCP)
ISO	Information Commissioner's Office (ISO)
NCSC	National Cyber Security Centre (NCSC)
NIST	National Institute of Standards and Technology (NIST)
OGD	Other Government Bodies (OGD)
SIRT	Security Incident Response Team (SIRT)
Supplier	Is inclusive of contractor, their employees or any sub-contractors used

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition

Appendix F Accessibility artefacts

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

DWP Digital Accessibility Policy | DWP Intranet

https://accessibility-manual.dwp.gov.uk/

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

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

Appendix G – Security Incident Report Form

Please copy and paste the following table into an email with the Subject: Security Incident Report Form. Answer all questions and send to: SECURITYINCIDENT.RESPONSETEAM-SIRT-@DWP.GOV.UK

PLEASE NOTE: To comply with General Data Protection Regulations (GDPR) do not include any sensitive personal data on this referral form.

Your Details:

Name:	
Telephone number & email address:	
Alternative name and contact details:	

Supplier Details (for completion by DWP Suppliers only)

Organisation Name:	
Organisation Location:	
Organisation Security Team contact name(s) & contact details:	
Organisation Data Protection Officer name & contact details:	
Organisation's primary DWP contact name(s) & contact details:	
Organisation's secondary DWP contact name(s) & contact details:	
Please state briefly what service you supply to DWP including details any IT systems you supply or have access to.	

Incident Details

Date incident occurred?	
Date incident discovered?	
Do you know if the incident has had any impact on the rights and freedoms of the citizen which may have made them vulnerable, put them at risk or caused them unnecessary distress?	
Is there any media interest in this incident or any risk to the reputation of DWP?	
Has the Information Commissioner Office (ICO) been made aware of this incident? If yes, please provide details?	
Has the National Cyber Security Centre or National Crime Agency been made aware of this incident? If yes, please provide details?	
When did the security incident happen?	

Please include all details known at the time of completion. e.g. When did this happen, during business hours or out of hours? Is the incident over (contained) or is it still happening? Could the incident get worse?	
Where did the security incident happen? **Please include all details known at the time of completion.** e.g. Did the incident occur in the office or away from the office (i.e. working from home).	
Why did the security incident happen? **Please include all details known at the time of completion.** e.g. Was the incident accidental, deliberate or due to negligence? Is there evidence of motivation such as a disgruntled employee/contactor, hacktivists, criminal?	
How did the security incident happen? **Please include all details known at the time of completion.** e.g. How did the security incident happen? Is there evidence that existing controls failed or were bypassed or that there was a gap.	
Please use the space below to provide information about any activity already taken to manage or contain this incident. If possible, please attach a copy of any relevant information including investigation or root cause reports.	