Security Policy –
DWP Security Forensic Readiness Policy

Chief Security Officer

Department for Work & Pensions

ThinkSecure

This DWP Security Forensic Readiness Policy is part of a suite of policies 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.

Security policies considered appropriate for public viewing are published here:

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

Security policies 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.

Table of Contents

Policy Title

DWP Security Forensic Readiness Policy

Overview

A Forensic Readiness process must be established, involving specialist individuals (or teams), information, and tools required for dealing with information security incidents or other events (e.g., e-discovery requests) that require forensic investigation.

This policy adopts an exception-based risk management approach, whereby compliance is mandated unless an exception is granted – see section **Policy Compliance** below.

Purpose

The primary objective is to undertake investigations relating to alleged instances of malicious, inappropriate, and / or criminal behaviour, and secure all available evidence relating to any such investigation.

The Department applies a risk-based approach to security and Forensic Readiness. It is accepted that systems and services must have a proportionate, legal, accountable, and necessary level of security management. This policy aims to ensure that all actions taken by the Department of Work and Pensions (DWP) agents considering security incidents or other events that require forensic investigation, adhere to legislation and regulation and established principles of computer-based electronic evidence as set out in this policy, while also maintaining the security and integrity of data held within DWP systems.

Scope

The scope of this policy covers the Department's Forensic Readiness process, when required for forensic investigation 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, Cloud, Test and Development)

This policy does not replace any legal, statutory, or regulatory requirements.

This policy applies to all contractual agreements for the provision of computing and networking services for the department and these policy statements supplement all currently applicable contractual agreements to Departmental computing and networking services, including those provided through managed services.

This policy also applies to:

a) all DWP employees dealing with information security incidents or other events (e.g., e-discovery requests) that require forensic investigation

b) all contracted third-party suppliers required to provide or assist in the timely identification, investigation, and remediation of security incidents in business applications, systems, equipment, and devices

c) all DWP Contracted suppliers who handle/access/process Authority Data

The scope of this policy includes Corporately Owned / Personally Enabled (COPE) devices but does not apply to Bring Your Own Device (BYOD) devices.

Definitions

Digital Device: electronic equipment used to process or store digital data.

Digital Evidence: information or data, stored or transmitted in binary form that may be relied upon as evidence.

Digital Evidence Copy: a bit-by-bit copy of the digital evidence that has been produced to maintain the reliability of the evidence by including both the digital evidence and verification means where the method of verifying it can be either embedded in or independent from the tools used in doing the verification (e.g., checksums).

E Discovery: is a form of digital investigation that attempts to find evidence in email, business communications and other data that could be used in litigation or criminal proceedings.

Policy Statements

1. DWP Cyber Resilience Centre (CRC) Security Incident Response Team (SIRT) are required to ensure the information security Forensic Readiness Plan, for dealing with information security incidents in ALL environments that may require forensic investigation, covers:

   1.1. collection of electronic and physical evidence

   1.2. immediate preservation of evidence on discovery of an information security incident (e.g., to support the need for a chain of custody to show who handled evidence from the time of discovery to the time of legal proceedings)

   1.3. compliance with the DWP Security Incident Management Standard (SS-014), particularly the requirements regarding the collection of admissible evidence

   1.4. maintenance of a log of evidence recovered and the investigation processes undertaken

   1.5. the need to seek legal advice where evidence is recovered

   1.6. actions that may be monitored during the investigation.

2. DWP SIRT and Digital Forensic Incident Response (DFIR) teams are required to manage information security incidents that require forensic investigation and must have competent resources available with:

   2.1. defined roles and responsibilities

   2.2. sufficient skills / experience in managing forensic investigations

   2.3. authority to make critical business decisions and escalate forensic investigations (e.g., to the crisis management team)

   2.4. methods of involving internal and external stakeholders (e.g., legal department, public relations, human resources, law enforcement agencies, media, and industry regulators)

   2.5. established connections with internal and external organisations that provide specialist guidance and information about Forensic investigations. See Appendix A for further Internal and external Forensic Readiness references.

3. All digital evidence must only be collected / acquired by DFIR professionals, and never by system administrators or other privileged users.

4. DWP cloud teams and DFIR teams must engage and have strategies in place for data acquisition on Departmental cloud platforms.

5. A separate cloud security incident management process must be established and include cloud security incident management plans, which must be developed and tested.

6. Cloud security incident management plans must include procedures for the use of cloud native and third-party DFIR tools, which can be deployed on cloud environments to isolate, acquire, parse, and analyse evidence.

7. All potential digital evidence must be collected:

   7.1. as though it could become admissible to a court of law (i.e., following forensic principles contained in ISO/IEC 27037, which provides guidelines for identification, collection, acquisition and preservation of digital evidence, and ENISA digital forensic guidelines)

   7.2. by a competent person able to ensure the admissibility of evidence

   7.3. under the guidance and management of a person who understands any legal, statutory, and regulatory law (including the European Convention on Human Rights (ECHR) (1953) that pertains to an investigatory process

   7.4. using certified tools to strengthen the integrity of the preserved evidence

   7.5. from IT sources relevant to the information security incident (e.g., active, temporary, and deleted files on storage media; email or internet usage; memory caches; and event logs)

   7.6. from non-IT sources relevant to the information security incident (e.g., CCTV recordings, building access logs and eyewitness accounts).

8. All digital evidence must be collected in accordance with any legal, statutory, and regulatory guidance or law by:

   8.1. consider potential privacy implications (e.g., human rights and data protection)

   8.2. identifying constraints in employment or criminal legislation

   8.3. adhering to any specific compliance requirements (e.g., retaining information for further investigation or submitting breach notifications to affected individuals and relevant authorities)

8.4. respecting any incident reporting timescales (e.g., timeframe in which a data breach must be reported to regulatory bodies).

9. Digital evidence collected must include checksums and appropriate passwords and encryption keys needed to access password protected or encrypted areas of storage containing electronic evidence.

10. Important information about the investigation must be recorded (e.g., in a forensics tool, work log or equivalent), including:

    10.1. attributes (e.g., type, owner, and location of equipment) of electronic evidence

    10.2. a chronological sequence of events

    10.3. investigative actions undertaken.

11. The sources of forensic information must be protected by for example:

    11.1. restricting physical and logical access to target computer equipment to a limited number of DFIR resources

    11.2. creating a copy of the data being forensically examined (e.g., imaging a hard drive) without altering the original (e.g., using write blocker hardware or software)

    11.3. preventing unauthorised individuals tampering with possible evidence

12. The integrity of evidence must be protected by:

    12.1. demonstrating that appropriate evidence has been collected, preserved and that it has not been modified

    12.2. proving that copies of evidence are identical to the original (e.g., bit-for-bit copies)

    12.3. analysing evidence in a controlled environment (e.g., using a copy or a forensic image of the computer media to avoid corruption of the original)

    12.4. having evidence reviewed by an impartial, independent expert to ensure that it meets legal requirements

    12.5. ensuring that processes used to create and preserve evidence can be repeated by an independent external party

    12.6. limiting information about an investigation to nominated individuals and ensuring it is kept confidential

12.7. storing endpoint devices in Faraday bags or boxes (or equivalent) to prevent remote access (e.g., to read or modify data, or perform a remote wipe).

13. Results from a forensic investigation must be reported to relevant internal parties (e.g., Risk Owners, System Owners, heads of Product Delivery Units) and appropriate external parties (e.g., external legal counsel, regulators, or law enforcement).

14. Regular cyber security exercises must be performed to test the security Forensic Readiness processes and decision-making capabilities and to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises.

Accountabilities and Responsibilities

a) The DWP Chief Security Officer is the accountable owner of the DWP Security Forensic Readiness Policy and is responsible for ensuring its maintenance and review, through the DWP Deputy Director for Security Policy and Central Services.

b) This policy requires DWP Security and Data Protection (S&DP), DWP Cyber Resilience Centre (CRC), DWP Security Incident Response Team (SIRT) and any contracted accountable parties (suppliers that run or host systems on behalf of DWP), to clearly agree accountabilities and responsibilities for establishing an information security Forensic Readiness framework, including specialist individuals (or teams), information, and tools required by the DWP's information security processes.

c) This policy also requires DWP Cyber Resilience Centre (CRC) and DWP Security Incident Response Team (SIRT) to be responsible for establishing a Forensic Readiness Plan for managing information security incidents (in ALL environments) and other events (e.g., e-discovery requests) that require forensic investigation. The Forensic Readiness Plan must cover the people, processes and technology required to handle forensic investigations quickly and effectively, as defined in the policy statements below.

Compliance

a) All DWP employees, whether permanent or temporary (including DWP's contractors) have security responsibilities and must be aware of, and comply with,

DWP's security policies and standards. Many of DWP's employees and contractors handle sensitive information daily and most security incidents and breaches relate to information security.

b) Security incidents happen where there has been a deliberate attempt, whether successful or not, to compromise DWP assets such as information, people, IT, premises, or any accident resulting in loss of DWP assets.

c) Information security is important, and breeches can, in the most severe circumstances, result in dismissal. All breeches must be reported. Not reporting a breach, or suspected breach, is a disciplinary matter.

d) DWP's Security and Data Protection Team will regularly assess for compliance with this policy and may need to inspect physical locations, technology systems, design and processes and speak to people to facilitate this. All DWP employees, agents, contractors, consultants, business partners and service providers will be required to facilitate, support, and when necessary, participate in any such inspection. DWP Collaboration and Communication Services will use software filters to block access to some online websites and services. DWP Employee Privacy Notice.

e) Individual System Owners are responsible for ensuring that their systems comply with relevant policies and standards. To verify this, System Owners must commission activities such as, but not limited to:

- assessing the effectiveness of controls through tests performed by first-line teams and by 2nd line activities e.g., security testing teams.
- security assurance activities to ensure the adequacy of design of controls including their alignment with good practice.
- independent external audit (3rd line).
- IT Health Checks.

The outcome of such activity will be fed back to the System Owner

f) If for any reason users are unable to comply with this policy or require use of technology which is outside its scope, they may discuss this with their line manager in the first instance and then the Security Advice Centre who can provide advice on scalation/exception routes.

g) An exception to policy may be requested in instances where a business case can be made to undertake an activity that is non-compliant with DWP's Security Policies. This help reduce the risk of non-compliant activity and security incidents.
