DWP Forensic Readiness Policy

Contents

1. Background and Purpose

This policy addresses the requirement to ensure a systematic, standardised and legal process for incident response and business continuity, to ensure that evidence found in an investigation is preserved and the continuity of evidence maintained.

1.1 A process must be established for dealing with information security incidents or other events (e.g. e-discovery requests) that require forensic investigation.

1.2 The objective is to identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

1.3 The policy is not intended to replace or supplant existing policies and standards and must be used in conjunction with the Security Standard – Security Incident Management (SS-014) and associated policies, standards and guidance.

2. Scope

2.1 This policy does not apply where investigations are being conducted by Department for Work and Pensions (DWP) Jobcentre Plus's Counter Fraud, Compliance and Debt (CFCD), where benefit fraud is being investigated. In such cases, separate arrangements apply for the conduct of forensic investigations.

2.2 This policy applies to all other 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.

2.3 This policy applies to:

a) DWP staff designing, implementing and running new and current IT solutions;

b) all DWP suppliers, whose systems or services store, handle or process DWP information;

to ensure the appropriate levels of assurance for the confidentiality, integrity and availability of the Department's assets.

2.4 All security incidents identified by DWP employees and suppliers MUST be notified to the Contact Centre or where appropriate the Authority, as quickly as

possible. The report must contain as much information as possible. The Contact Centre or where appropriate the Authority, will validate the reported incident and refer to Security Incident Response Team (SIRT) if the incident is identified as medium or higher risk.

2.5 All security incidents identified out of hours MUST follow the DWP Security Incident Management Process – Out of Hours. Please refer to Security Standard – Security Incident Management (SS-014).

3. Accountabilities

3.1 The DWP Chief Security Officer is the accountable owner of the DWP Forensic Readiness Policy and is responsible for its maintenance and review as delegated through the Deputy Director for Security Policy and Compliance.

3.2. Digital Product Owners/Digital Product Development and DWP SIRT Leads will be accountable and responsible for ensuring people and processes are in place to perform the activities required for forensic readiness as outlined in this policy.

4. Policy Statements

4.1 A process must be established for dealing with information security incidents that may require forensic investigation. The process must be undertaken following consultation as appropriate between Digital Product Owners / Digital Product Development Leads, DWP Technology Services and Operational Service Owners, third party suppliers, DWP SIRT, and where applicable the Authority.

4.2 Whether a full formal forensic investigation is required must be assessed on:

a) Evidence of a reportable crime,

b) Evidence of internal fraud, theft, other loss,

c) Potential for embarrassment, reputation loss,

d) Immediate impact on customers, partners.

4.3 At all times those involved must act according to 'need to know' principles. They must be particularly aware whether any employees or suppliers, such as 'whistle blowers' and investigators, need to be protected from possible adverse impact by keeping their names and their involvement confidential.

4.4 DWP Security Standard – Security Incident Management (SS-014) must be followed when dealing with information security incidents that may require forensic investigation. This covers:

a) collection of electronic and physical evidence

b) 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)

c) compliance with a published standard or code of practice for the collection of admissible evidence

d) maintenance of a log of evidence recovered and the investigation processes undertaken

e) the need to seek legal advice where evidence is recovered

f) actions that may be monitored during the investigation.

4.5 Evidence must be collected:

a) with the intention of possible legal action

b) with respect for individuals' privacy and human rights

c) 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)

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

4.6 Evidence collected must include passwords and encryption keys needed to access password protected or encrypted areas of storage containing electronic evidence.

4.7 Electronic evidence must be collected in accordance with legal constraints by:

a) by assessing possible privacy implications (e.g. human rights and data protection - UK Data Protection Act 2018)

b) identifying constraints in employment legislation

c) complying with legal conditions in which investigations are conducted (e.g. UK Regulation of Investigatory Powers Act 2000).

4.8 The forensic investigation must be supported by recording important information about the investigation (e.g. in a forensics tool, work log or equivalent), including:

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

b) a chronological sequence of events

c) investigative actions undertaken.

4.9 The sources of forensic information must be protected by:

a) restricting physical and logical access to target computer equipment to a limited number of authorised individuals

b) preventing individuals tampering with possible evidence

c) establishing a litigation hold (e.g. by stopping document housekeeping routines such as deleting emails) to prevent deletion of documents and record archives which might contain electronic evidence.

4.10 The integrity of evidence must be protected by:

a) demonstrating that appropriate evidence has been collected, preserved and that it has not been modified

b) 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)

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

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

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

4.11 Results from a forensic investigation must be reported to relevant parties (e.g. Digital Product Owners / Digital Product Development Leads, DWP Technology Services and Operational Service Owners, third party suppliers, DWP SIRT, and where applicable the Authority, in-house legal counsel external legal counsel, regulators or counterparties).

5. Policy Compliance

5.1 Where forensic readiness is not implemented in line with this policy, an exception to the policy must be sought from the DWP risk management function – Enterprise Security Risk Management (ESRM), where appropriate via the Authority.

5.2 If the potential consequence of the degree of forensic readiness exceeds the DWP's risk tolerance a report must be made to the DWP risk management function – ESRM, where appropriate via the Authority, which will agree and oversee with the DWP Accountable Owner(s), a plan to manage the system / service risks.

5.3 Compliance to this policy will be declared through annual attestation to the policy by DWP Accountable Owner(s). Accountable parties must be prepared and able to evidence compliance to this policy, if appropriate with technical vulnerability output from their compliant network.