DWP Technical Vulnerability Management Policy

1. Introduction

The high-level principle and objectives of this policy are that:

1.1. A process must be established for the timely identification, investigation and remediation of technical vulnerabilities in business applications, systems, equipment and devices.

1.2. The primary objective is to address and if possible remediate technical vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in serious security incidents.

1.3. The Department applies a risk-focused approach to technical vulnerabilities. It is accepted that systems and services must have a proportionate and appropriate level of security management. An exploitable risk-based model for prioritizing remediation of identified vulnerabilities will be used. Changes will be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the Department's internally developed software.

1.4. This policy therefore adopts an exception-based risk management approach, whereby compliance is mandated unless an exception is granted – see section 5. Policy Compliance below.

1.5. The rationale for this policy is set out in the DWP Technical Vulnerability Strategy and the policy is in part supported by the DWP Security Standard – Security Patching (SS-033), which defines the minimum technical security measures that must be implemented to secure DWP systems via security patching, but which does not address the other aspects of technical vulnerability management covered by the strategy and this policy.

2. Definitions and Scope

Definitions

2.1. Technical Vulnerability Management is the ongoing, risk-informed process of addressing weaknesses within information technology (IT) infrastructure, operating systems, and applications, which if left untreated could allow malicious exploitation

leading to the compromise of Departmental assets. Such weaknesses should be addressed by counter measures such as the timely application of a patch or a change in the configuration of the system.

2.2. Patches - are software, firmware and operating system (OS) updates that address security vulnerabilities by modifying files or device settings within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features.

2.3. ITHC – an information technology health check or Penetration Testing is a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.

The internal systems should be tested to provide further assurance that no significant weaknesses exist on network infrastructure or individual systems that could allow one internal device to intentionally or unintentionally impact on the security of another.

2.4. Red Team Exercise (RTE) is when a group of people are authorised and organised to emulate a potential adversary's attack or exploitation capabilities against the Department's security posture. The RTE is an intelligence / threat-based assessment and will utilise methodologies used in an ITHC. The RTE will not just test the systems, but also the people and processes.

2.5. CVM – Continuous Vulnerability Monitoring is the use of automated tooling to maintain ongoing awareness of information security, vulnerabilities, and threats to support the Department's risk management decisions.

2.6. CVSS - Common Vulnerability Scoring System - provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help the Department to properly assess and prioritize vulnerability management processes.

2.7. Immutable infrastructure - is an approach to managing services and software deployments on IT resources wherein components are replaced rather than changed. An application or service is effectively rebuilt and redeployed each time any change occurs.

2.8. Offensive security is a proactive and adversarial approach to protecting computer systems, networks and individuals from attacks.

Scope

2.9. The scope of this policy covers the Department's requirement for the identification and remediation of technical vulnerabilities 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).

2.10. The policy covers the Department's requirement to detect known and new technical vulnerabilities using various methods including IT Health CHECKs (ITHCs), Red Teaming and Offensive Security testing, and Continuous Vulnerability Monitoring (CVM) for example, both to discover new weaknesses and to confirm that patches/configuration changes have been applied correctly.

2.11. The policy also covers the requirement to manage technical vulnerabilities. These may include:

- A missing security patch from a system, resulting in a security vulnerability. This can usually be resolved by applying the patch, but this may require proportionate testing and planned downtime to do so;
- A misconfiguration of a system meaning it could be open to being exploited – such misconfigurations include, but are not limited to: use of default passwords, deprecated communication channels, cross-site scripting and SQL injection vulnerabilities;
- Immutable infrastructure not being kept up to date. This can be resolved by continuously evaluating updates or upgrades, which achieve the same purpose as patching.

2.12. This policy does not replace any legal or regulatory requirements.

2.13. 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.

2.14. This policy also applies to:

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

b) all contracted third-party suppliers, whose systems or services may be required to provide timely identification, investigation, and remediation of technical vulnerabilities in business applications, systems, equipment, and devices to ensure the appropriate levels of assurance for the confidentiality, integrity, and availability of the Department's assets, including data.

3. Accountabilities and Responsibilities

3.1. The DWP Chief Security Officer is the accountable owner of the DWP Technical Vulnerability Management Policy and is responsible for ensuring its maintenance and review, through the DWP Deputy Director for Security Policy and Data Protection.

3.2. This policy requires DWP Digital, DWP Operations Functions, and any contracted accountable parties (*see below), to clearly agree accountabilities and responsibilities for establishing a continuous programme for the identification and remediation of technical vulnerabilities across:

a) IT infrastructure, including hardware, firmware, middleware and network devices;

b) operating systems;

c) applications; and

d) network appliances (anything connected to the corporate network not included above).

***Accountable parties are people and parties that run or host systems on behalf of DWP.**

3.3. This policy requires the DWP Digital Security and Digital Vulnerability Management Team to be accountable for the technical vulnerability management process, including the identification and remediation of vulnerabilities.

3.4. This policy also requires DWP Cyber Resilience Centre (CRC) and DWP Technical Vulnerability Assessment Team (TVAT) to be responsible for working with stakeholders in DWP Digital, DWP Operations Functions, and any contracted accountable parties to understand and deliver the requirement for identifying technical vulnerabilities associated with DWP assets including:

a) Commissioning appropriate technical vulnerability assessments (normally an ITHC, Vulnerability Scan or Red Team Exercise) on DWP assets to identify technical vulnerabilities;

b) Disseminating data and information on technical vulnerabilities to stakeholders;

c) Assisting stakeholders in understanding the technical vulnerability information provided;

d) Assessing and assuring that expected remediation work has been successfully undertaken.

4. Policy Statements

4.1. DWP Digital and DWP Operations Functions and any contracted accountable parties are required to ensure people and processes are in place to perform the activities required for technical vulnerability management as outlined in this policy.

4.2. DWP Cyber Resilience Centre (CRC) Technical Vulnerability Assessment Team (TVAT), working with Digital Security Vulnerability Management (DSVM) and other stakeholders in DWP Digital, DWP Operations Functions, and any contracted accountable parties are required to ensure processes are in place to monitor progress on technical vulnerability management, so that they are satisfied that the requirements of the policy are being fulfilled.

4.3. DWP Cyber Resilience Centre (CRC) Technical Vulnerability Assessment Team (TVAT), working with Digital Security Vulnerability Management (DSVM) and other stakeholders in DWP Digital, DWP Operations Functions, and any contracted accountable parties are required to develop and maintain processes which ensure that the following responsibilities are managed in a timely fashion:

a) technical vulnerability identification;

b) scanning for specific, identified technical vulnerabilities;

c) vulnerability tracking (including recording metrics)

d) technical vulnerability analysis;

e) prioritising vulnerabilities, taking account of severity ratings;

f) delivery of remediation to assets within defined timescales (e.g. through patching or other measures involving reconfiguration, such as closing ports), and including the testing of the remediation; and

g) mitigation of vulnerabilities, involving the implementation of internal controls that reduce the attack surface of DWP business applications, systems, equipment and devices. Examples of vulnerability mitigation include threat intelligence, and requiring strict access controls, even for those already inside the network perimeter

4.4. Security testing and technical vulnerability scanning of DWP business applications, operating systems and network devices – or those run or operated by contracted accountable parties on behalf of DWP – must take place and may include:

a) identification of new technical vulnerabilities, including updates or upgrades to immutable infrastructure;

b) disclose technical vulnerabilities that are discovered to relevant parties (e.g. report identified faults to software producers);

c) determine whether software code that can exploit a new vulnerability (often referred to as a zero-day exploit) is publicly available;

d) check if security measures have been applied correctly and successfully;

e) assist in the prioritisation of the remediation of vulnerabilities;

f) provide a view of vulnerabilities across the Department’s technical infrastructure (e.g. to make comparisons and identify trends).

4.5. Security testing and technical vulnerability scanning of business applications, operating systems and network devices must be:

a) performed on a regular basis, informed by a security risk assessment;

b) determine the extent to which they are exposed to threats (e.g. checking whether powerful system utilities/commands have been disabled or weak passwords/passphrases are being used)

c) identify what could be affected by specific vulnerabilities

4.6. The importance of business applications, systems, equipment and devices should be determined to help evaluate the criticality of identified technical vulnerabilities and define timescales/priorities for remediating them.

4.7. Security testing and technical vulnerability scanning must be proportionate to the value of the asset as defined by the security risk assessment. Security testing and technical vulnerability scanning is likely to include:

a) automated technical vulnerability scanning software or a commercial vulnerability scanning service;

b) penetration testing, ITHC, Red Team and / or Offensive Security testing;

c) manual scanning, which includes comparing software version numbers and configuration settings with those provided by suppliers.

4.8. Security testing and technical vulnerability scanning must be:

a) undertaken with the prior agreement of the DWP Digital Product Owner/Digital Product Development Leads, Digital Security Vulnerability Management and, where contractually required with the prior written permission of the DWP Digital Product Owner/Digital Product Development Leads or contracted accountable parties. The only admissible exceptions to this consent are:

i) a security test or technical vulnerability scan required by the DWP Security & Data Protection (S&DP) team, which will obtain the necessary permissions from the appropriate Accountable Digital Director; or

ii) a security test or technical vulnerability scan required to assist with the resolution of a live incident.

b) restricted to a limited number of authorised individuals (e.g. using a dedicated account that is only used for vulnerability scanning);

c) performed using approved and dedicated systems, (so that DWP Product Development Units / Technology Services do not mistake the activity for an attacker);

d) independently monitored (e.g. to identify misuse by authorised individuals or help detect unauthorised scanning)

e) reviewed regularly, taking account of possible contradictory or misleading results.

4.9. Where remediation can be undertaken that is straightforward and with a low risk of impacting availability, confidentiality or integrity, then it must be carried out as a matter of course.

4.10. The process for remediating technical vulnerabilities must be developed and undertaken following consultation between an assigned Authority / DWP Digital Security Risk Manager or DWP Security Architect, DWP Product Owners / Digital Product Development Leads, Technology Services and Operational Service Owners.

4.11. Remediation processes must include:

a) an assessment of the risk, and a documented decision-making process on how the risk will be managed, including regularity and frequency of remedial actions. If the risk process is above tolerance there must be a mechanism or procedure for escalating the risk through the Department's Security Risk Management governance bodies;

b) a patch management process in alignment with the DWP Security Standard–Security Patching (SS-033), which involves identifying and obtaining patches for known vulnerabilities (including patch bundles, critical updates and service packs) from authorised sources, as soon as they are available.

c) also ensuring immutable infrastructure is kept up to date continuously, via updates or upgrades, which achieve the same purpose as patching;

d) a way of recording the patches that have been applied (e.g. in a specialised patch management tool or a Configuration Management Database (CMDB));

e) a procedure for testing patches against known criteria prior to deployment, or applying for and receiving an exception to this part of the policy;

f) installing patches and making necessary changes to system configuration in accordance with hardware or software vendor guidance;

g) deploying patches in a timely manner (e.g. grouping multiple patches and using software distribution tools);

h) a means of deploying patches to systems that are not accessible via the DWP or accountable party's corporate network (e.g. standalone computers) or devices that connect to the corporate network infrequently (e.g. mobile / home workers);

i) a procedure for dealing with the failed deployment of a patch (e.g. redeployment of the patch);

j) a process for reporting on the status of patch deployment and the status of immutable infrastructure in respect of updates or upgrades – the frequency and content to be agreed with DWP asset owner leads, their suppliers, and

Digital Security Risk Management requirements, in alignment with the DWP Security Patching Standard;

k) an exception process to protect information when a technical vulnerability cannot be remediated with a patch, or an available patch cannot be applied e.g. by disabling services, adding additional access controls and performing detailed monitoring;

l) monitoring and reporting patching statistics to identify potential weaknesses and improve the patching process.

5. Policy Compliance

5.1. 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 Policy Owner

5.2. For a new project, where vulnerability management and technical remediation is not able to be carried out in compliance with the requirements of this policy, this must be presented to an assigned Authority / DWP Digital Security Risk Manager or Security Architect in the first instance, who will inform the Risk Owner. If necessary and appropriate, the mitigation / remediation risk assessment will be considered as part of the project submission to the DWP Digital Design Authority (DDA) advisory or governance board.

This presentation and possible submission must be carried out prior to deployment for new systems or services and managed through the design caveats or exception process.

5.3. For existing systems and services, the issue must also be raised with an assigned Authority / DWP Digital Security Risk Manager or Security Architect in the first instance, who must inform the Risk Owner. If necessary and appropriate an exception to this policy and/ or the DWP Security Patching Standard must be sought from the DWP Standards Review Group.

5.4. Such exception requests will invoke the DWP Security Risk Management process to clarify the potential impact of any deviation to the measure's detailed in this policy and it's associated standard.

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

5.6. Accountable and responsible parties must be prepared and willing to evidence compliance to this policy for audit purposes, if appropriate with security log audit records from their systems and services.

Mandatory Security Outcomes

The security measures mandated in this policy contribute to the achievement of NIST CSF security outcomes described in the table below, using controls such as CIS V8.

Ref	CIS Controls V8	NIST - CSF Category - Outcome	NIST – CSF Sub-Category
7.1	Establish and Maintain a Vulnerability Management Process	ID.RA-2 ID.RA-3 ID.RA-4 PR.IP-12 DE.CM-8 DE.DP-2 RS.AN-5	Threat and vulnerability information is received from information sharing forums and sources Threats, both internal and external, are identified and documented Potential business impacts and likelihoods are identified A vulnerability management plan is developed and implemented. Vulnerability scans are performed Detection activities comply with all applicable requirements Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
7.2	Establish and Maintain a Remediation Process	RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks

7.3	Perform Automated Operating System Patch Management		
7.4	Perform Automated Application Patch Management		
7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets	DE.CM-8	Vulnerability scans are performed
7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	DE.CM-8	Vulnerability scans are performed
7.7	Remediate Detected Vulnerabilities	RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks