Security Standard – Security Patching (SS-033)

Chief Security Office

Date: 25/07/2024

Department for Work & Pensions

This Security Patching 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 Authority 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. Table of Contents

2. Revision history

Version	Author	Description	Date
1.0		First published version	16/12/2019
1.1		Minor amendments in sections; 10.1.1 to cover automated patching 10.5.2 to cover both automated and manual patches 15. definition of endpoints.	26/08/2020
1.2		Added references to automated patching and immutable infrastructure in sections 8.3; 10.3.2; 10.3.3; 10.3.5; 10.4.1; 10.5.1; 10.5.2; Minor amendments in sections; 10.1.1 Greater emphasis on automated patching 10.1.3 Added applicability to manual patches 10.1.6 Added reference to evergreening modern infrastructure 10.2.3 Criticality/Timeframe amendments 10.2.4 Updated for zero day exploits 10.2.5 Further detail on dealing with emergency patches 10.3.2 Risk assessment, triage function and review requirements added 10.3.4 Specified that entitlement refers to manual patching 10.4.4 Added reference to Blue/Green deployment model. 10.5.4 Added reference to application updates 10.6.2 Added rationale for scanning Definition of terms updated Glossary updated	15/01/2021
2.0		Added NIST CSF references; Introduction – Added references to CIS v8 Controls Set; further information added regarding risk assessment and risk ownership. Scope – Clarification added to highlight that patching is only one component of vulnerability management. 11.1.4 Clarified application of security patches for new connections. 11.1.7 Differentiate between functional and security patches for delivery 11.2.2 Patch criticality changed to vulnerability; added a statement about assessing exploitability in addition to criticality. 11.2.3 Added statements about mitigating vulnerabilities to within risk appetite; added reference to medium vulnerabilities 11.6.4 Requirements added for coverage of reporting.	07/12/2022

2.1		All NIST references reviewed and updated to reflect NIST 2.0 All security measures reviewed in line with risk and threat assessments Scope: Applications, software, infrastructure, network & security appliances; environments 11.1.1 ‘should’ changed to ‘must’ 11.2.1 Threat intel from known, trusted third parties; trusted feeds; ‘should’ changed to ‘must’ 11.2.2 risk appetite, threat profile, exploitability; EPSS; prioritisation considering environmental factors; considered in triage 11.2.3 Critical vulnerability prioritisation criteria and timescales; independent monitoring function 11.2.4 High vulnerability timescales; independent monitoring function 11.2.5 Medium/Low vulnerability timescales; independent monitoring function 11.2.6 ‘should’ changed to ‘must’; supporting sources added 11.3.1 Systems to be assessed; relevant teams 11.3.2 ‘should’ changed to ‘must’; Incident/problem mgmt. processes and risk assessment 11.3.3 Risk register removed 11.3.4 Product 11.3.5 & 11.4.2 Types of repositories removed 11.4.3 Change mgmt. processes 11.4.4 Emergency patches 11.4.5 vulnerability triage process 11.4.6 Types of repositories removed 11.5.3 prioritisation that considers business criticality, exploitability, triage actions, risk analysis etc.	25/07/2024

3. Approval history

Version	Name	Role	Date
1.0		Chief Security Officer	16/12/2019
1.1		Chief Security Officer	26/08/2020
1.2		Chief Security Officer	15/01/2021
2.0		Chief Security Officer	07/12/2022
2.1		Chief Security Officer	25/07/2024

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 first-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. D].
- independent external audit

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, technical engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications that manager security patching.

7. Accessibility statement

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in **Error! Reference source not found.**F.

8. Introduction

This standard defines the minimum technical security measures that **must** be implemented to secure Authority systems via security patching. It is also aligned to the overarching Technical Vulnerability Management Policy, [Ref. B] which details management of all technical vulnerabilities including patching.

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 patching requirements are clearly articulated and can be implemented consistently across the Department and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities to an acceptable level for operation.
- Ensure that risk assessments include consideration of asset value and business criticality, with priority given to vulnerabilities that are exploitable both now, and in the future if threat intelligence indicates this.
- Ensure that identified risks are owned and managed by appropriate Risk Owners.
- support the implementation of security controls that enable the achievement of security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Department. 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 systems and services operated in the Authority or on behalf of the Authority are updated, maintained 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 applies to all applications, software and infrastructure (including network and security appliances) in all environments (i.e. Production, Pre-Production, Test and Development etc.) within the Department and supplier base (contracted third party providers), for the purposes of delivering applications and services that handle Authority data.

It also supports the Authority's Technical Vulnerability Management Policy [Ref. B] which drives the requirements contained in this standard. It should however be noted that security patching is only one component of vulnerability management – the related vulnerability management strategy and policy describe additional vulnerabilities around system misconfiguration and physical, personnel or process weaknesses that could be exploited.

It is also important to highlight that security patching is only one way to address vulnerabilities, and that reducing the overall risk to the Department of vulnerabilities being exploited may be achieved through deployment of other controls, as part of effective risk management, which is highlighted in section 11.2.3.

This standard also applies to immutable infrastructure, but via updates and upgrades rather than patching.

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 Security Patch Control Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	Patching **MUST** be automated wherever possible and should utilise dedicated service accounts with elevated privileges where appropriate. Manual patching **MUST** only be conducted by users with enhanced access and/or privileged users. (SS-001 – pt 2 Privileged User Access Security Standard). [Ref. C]	PR.AA-05
11.1.2	Standard business users **MUST NOT** have the ability to install unauthorised patches on any departmental end points.	PR.AA-05 PR.PS-05

11.1.3	Any manually applied patches found to have bypassed control mechanisms for installation **MUST** be subject to a formal review and uninstallation if deemed necessary.	ID.RA-07 PR.PS-05
11.1.4	Upon connection to the production network, all systems **MUST** have up to date security patches applied to software or applications that are in vendor support.	PR.PS-01 PR.PS-02
11.1.5	The patching and update process **MUST** ensure that both the offline (stored) and runtime virtual images are updated.	PR.PS-02
11.1.6	Patch levels **MUST** be maintained for the lifespan of the system. For modern infrastructure, this is achieved by 'evergreening' i.e. via continuous updates being applied.	PR.PS-02 ID.RA-01 ID.AM-08
11.1.7	Patches that only deliver functional change and **do not** fix a vulnerability **MUST NOT** be delivered as security patches, although can be delivered via the same mechanisms at the same time.	ID.RA-07 PR.PS-02

11.2 Threat Intelligence

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	Threat intelligence from known, trusted third parties regarding system vulnerabilities **MUST** be collected at least weekly and reviewed. These **MUST** be analysed and processed and distributed to a relevant Triage Team. *This **MUST** be delivered via a triage function as specified in NCSC guidance on vulnerability management.*	ID.RA-02 ID.RA-03 ID.RA-04 ID.RA-05

11.2.2	Vulnerabilities **MUST** be based on a defined criticality using the latest Common Vulnerability Scoring System (CVSS) or where applicable, Common Weakness Enumeration (CWE) scoring calculations, where this is available. However, it should be noted that CVSS and CWE only provide a generic view on the criticality of discovered vulnerabilities, and do not take into account an individual organisation's security capability, risk appetite, threat profile, or the exploitability of a vulnerability in individual systems. Other tools (for example Exploit Prediction Scoring System (EPSS)) may also be used to augment this information, e.g. to assess exploitability to aid prioritisation, but these **MUST NOT** be used as the sole source of information in assessing risk. The prioritisation of a patch **MUST** consider all attack vector information, as well as the following environmental factors: • **Threat Level** - Is the System or Infrastructure which requires vulnerability treatment located in an environment which is susceptible to an exploit from known attack vectors ? • **Likelihood of Compromise** - What is the likelihood of a compromise occurring within the System or Infrastructure ? Does the System or Infrastructure exist in an environment where a deployed and tested security control would reduce the risk of compromise ? • **Consequences of Compromise** – What are the consequences of a compromise ? Is the System or Infrastructure critical to business operations or contains sensitive data ? • **Environmental Characteristics** – Will the security controls deployed and tested within an environment in which the vulnerable System or Infrastructure resides, reduce the likelihood of a vulnerability exploit occurring ? Do the System or Infrastructure use cases reduce the likelihood of the exploit occurring ? These **MUST** be considered as part of the triage process.	ID.RA-01 ID.RA-04 ID.RA-05 ID.RA-08 GV.RM-06

11.2.3	For vulnerabilities that CVSS define as critical, and have one or more of the following characteristics (which **MUST** be considered during the triage process); • The vulnerability is exploitable via any attack vector (local, network, physical, adjacent) • The vulnerability is locally exploitable i.e. can be exploited with local access • The vulnerability does not require any authentication or bypasses normal user authentication (i.e. the user is not aware) • The vulnerability directly enables the execution of code on a vulnerable device • Exploit code is either publicly available or the existence of an exploit has been detected by other sources • The affected system(s) are in a sensitive area (i.e. Internet Facing, Network Security Zone with Critical Applications) • The vulnerability is present in the 'CISA Known Exploited Vulnerabilities Catalog' [see External References]; ***And;*** • There are no Enterprise perimeter mitigations and no effective internal mitigations in place; ***Or;*** • Threat Intelligence indicates a heightened threat level ; applications, systems and devices **MUST** be patched within **7** days of an update being released. In exceptional circumstances (which must be agreed, declared and tracked by an independent central monitoring function), if the patch cannot be applied within 7 days, the risk **MUST** be mitigated to a level where the residual risk for both the service and the Departmental Enterprise risk is within appetite. If the above characteristics are <u>not present</u>, then applications, systems and devices **MUST** be patched **(or the vulnerability mitigated to a level where the residual risk** (which must be agreed by an independent central monitoring function) **for both the service and the Departmental Enterprise risk is within appetite)** within **14** days of an update being released.	GV.RM-06 ID.RA-01 ID.RA-04 ID.RA-05 ID.RA-06 ID.RA-08 PR.PS-02

11.2.4	Where a security patch fixes a vulnerability that the CVSS or CWE score defines as '**high'**, applications, systems and devices **MUST** be patched **(or the vulnerability mitigated to a level where the residual risk** (which must be agreed by an independent central monitoring function) **for both the service and the Departmental Enterprise risk is within appetite)** within **14** days of an update being released.	GV.RM-06 ID.RA-01 ID.RA-04 ID.RA-05 ID.RA-06 ID.RA-08 PR.PS-02
11.2.5	Where a security patch fixes a vulnerability that the CVSS or CWE score defines as '**medium' or 'low'**, applications, systems and devices **MUST** be patched **(or the vulnerability mitigated to a level where the residual risk** (which must be agreed by an independent central monitoring function) **for both the service and the Departmental Enterprise risk is within appetite)** within **45** days of an update being released.	GV.RM-06 ID.RA-01 ID.RA-04 ID.RA-05 ID.RA-06 ID.RA-08 PR.PS-02
11.2.6	Where applicable, the risk owner **MUST** consider advice on what mitigating actions can be taken to minimise the threat from zero-day exploits (which by definition do not have a patch available) from sources such as; • Threat Intelligence • Vulnerability Management • Security Architects • Engineering • Vendors/industry	ID.RA-05 ID.RA-06
11.2.7	In exceptional circumstances, the Security and Data Protection function may advise that a patch needs to be implemented **faster than those requirements outlined at para 11.2.3**. That advice will be based on an assessment of the threat and the vulnerability in question. In such circumstances, the response **MUST** be treated under the Security Incident Management Policy as an Emergency Patch. The decision on invoking those procedures may be taken by the Head of the Security Incident Response Team, the Head of the Cyber Resilience Centre or by the Chief Security Officer. In the absence of such a decision, the provisions of paragraph 11.2.3 apply and **MUST** be complied with.	ID.AM-05 ID.RA-05 ID.RA-06

11.3 Patch Assessment

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	All patches **MUST** be assessed by the relevant teams responsible for maintaining the affected systems.	ID.RA-04 ID.RA-06
11.3.2	Patching **MUST** be conducted as standard but where a risk to service delivery is identified, an assessment is required that considers the risk of: • Not deploying the patch • The risk of implementing the patch (i.e. destabilising a system or business process). • The availability or lack of compensating security controls that may impact the CVSS score. This **MUST** be delivered through a 'vulnerability triage group', consisting of staff with knowledge of cyber security risk, business risk and IT estate management, supported by incident / problem management and risk assessment processes for technical remediation as appropriate. Where a decision is made **not** to fix the issue but to acknowledge it, a timeframe for reviewing this decision needs to be made, which **MUST** be no more than 3 months. This decision **MUST** be made by a suitable responsible person within the accountable business area.	ID.RA-04 ID.RA-05 ID.RA-06
11.3.3	A record of the decision to apply or reject manual patches, **MUST** be documented as part of the Risk Assessment process. For automated patching via upgrades, a record of the reason for rejecting a product update must be maintained and reviewed on a regular basis, along with a risk assessment.	ID.RA-07 PR.PS-02
11.3.4	The *entitlement* to patch a product manually **MUST** be confirmed before applying a patch e.g. open source products that do not have a support package or service wrapper.	ID.AM-02 ID.RA-07

11.3.5	A record of all assets **MUST** be maintained along with their patch status, history, and next review date (which may be set as part of a regular, scheduled activity) where appropriate. For automated patching via upgrades, a record of the reason for rejecting a product update **MUST** be maintained and reviewed on a regular basis, along with a risk assessment.	ID.AM-02

11.4 Patch Testing

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	All patches **MUST** be tested in a suitable environment (meets live conditions) prior to being applied to the enterprise, wherever possible. This is also applicable to immutable infrastructure, which goes through a development environment and Continuous Integration pipelines. Where automated testing is employed, any remediation of vulnerabilities will follow the standard approach for software changes.	ID.RA-07 PR.PS-02
11.4.2	Accountable parties **MUST** test the patch to check for compatibility and integration, and create a back-up or restore point, which can be managed via version control or container repositories where appropriate. This detail must be documented.	PR.DS-11
11.4.3	The patch becomes approved once testing has been concluded satisfactorily.	ID.RA-07
11.4.4	Delivery of the approved patch across the estate **MUST** be in stages to reduce impact. The 'Blue/Green' deployment model can also be utilised to achieve this. This requirement may be waived in the case of emergency patches.	ID.RA-07 PR.PS-02
11.4.5	Approved patches **MUST** be applied across the Enterprise in a timeframe based on their criticality (defined by the vulnerability triage process).	ID.RA-05 ID.RA-06
11.4.6	Where testing is not feasible, this **MUST** be risk assessed.	ID.RA-06

11.5 Patch Delivery

Reference	Minimum Technical Security Measures	
11.5.1	Where possible, accountable parties **MUST** automate patch deployment across end points. Immutable infrastructure is kept up to date continuously, via updates or upgrades, which achieve the same purpose as patching.	ID.RA-08 PR.PS-02
11.5.2	All patches, both manual and automated, **MUST** be recorded. For automated patching via upgrades, a record of the reason for rejecting a product update **MUST** be maintained and reviewed on a regular basis, along with a risk assessment.	ID.RA-01 ID.AM-02 ID.AM-08 ID.RA-07
11.5.3	Where appropriate, accountable parties **MUST** patch systems and end points based on their criticality and associated prioritisation that considers business criticality, exploitability, triage actions, risk analysis etc.	ID.AM-05 ID.RA-05 ID.RA-06 GV.OC-05
11.5.4	Where appropriate, accountable parties **MUST** ensure all patching is applied across the enterprise where necessary. This includes applying application updates or upgrades that include security updates.	ID.AM-08 PR.PS-01 GV.OC-05

11.6 Reporting

Reference	Minimum Technical Security Measures	
11.6.1	When patches have been deployed, reporting **MUST** be run to confirm their deployment.	ID.RA-01 PR.PS-02
11.6.2	Automated scanning **MUST** be deployed to report patch status on a regular basis, to correlate current patch status against vulnerabilities.	ID.RA-01 ID.RA-08
11.6.3	Patches that have not been implemented **MUST** be reported to the system and risk owner who remains responsible for the exposure caused by the inability to patch.	GV.RM-05 GV.RR-02 ID.RA-05
11.6.4	Vulnerability/Patching status reporting **MUST** cover the entirety of the estate, and not just specific domains or environments.	ID.RA-01

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 which can also be cross referenced against the CIS Critical Security Controls set. [see External References]

Table 2 – List of Security Outcomes Mapping

Ref	Security Outcome (Sub-category)	Related Security Measure
GV.OC-05	Outcomes, capabilities, and services that the organization depends on are understood and communicated	11.5.3, 11.5.4
GV.RM-05	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	11.6.3
GV.RM-06	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	11.2.2, 11.2.3, 11.2.4, 11.2.5
GV.RR-02	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	11.6.3
ID.AM-02	Inventories of software, services, and systems managed by the organization are maintained	11.3.4, 11.3.5, 11.5.2
ID.AM-05	Assets are prioritized based on classification, criticality, resources, and impact on the mission	11.2.7, 11.5.3

ID.AM-08	Systems, hardware, software, services, and data are managed throughout their life cycles	11.1.6, 11.5.2, 11.5.4
ID.RA-01	Vulnerabilities in assets are identified, validated, and recorded	11.1.6, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.5.2, 11.6.1, 11.6.2, 11.6.4
ID.RA-02	Cyber threat intelligence is received from information sharing forums and sources	11.2.1
ID.RA-03	Internal and external threats to the organization are identified and recorded	11.2.1
ID.RA-04	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.3.1, 11.3.2,
ID.RA-05	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.3.2, 11.4.5, 11.5.3, 11.6.3
ID.RA-06	Risk responses are chosen, prioritized, planned, tracked, and communicated	11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 11.3.1, 11.3.2, 11.4.5, 11.4.6, 11.5.3
ID.RA-07	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked	11.1.3, 11.1.7, 11.3.3, 11.3.4, 11.4.1, 11.4.3, 11.4.4, 11.5.2
ID.RA-08	Processes for receiving, analyzing, and responding to vulnerability disclosures are established	11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.5.1, 11.6.2

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	11.1.1, 11.1.2
PR.DS-11	Backups of data are created, protected, maintained, and tested	11.4.2
PR.PS-01	Configuration management practices are established and applied	11.1.4, 11.5.4
PR.PS-02	Software is maintained, replaced, and removed commensurate with risk	11.1.4, 11.1.5, 11.1.6, 11.1.7, 11.2.3, 11.2.4, 11.2.5, 11.3.3, 11.4.1, 11.4.4, 11.5.1, 11.6.1
PR.PS-05	Installation and execution of unauthorized software are prevented	11.1.2, 11.1.3

Appendix B. Internal references

Below, is a list of internal documents that **should** be read in conjunction with this standard.

Table 3 – Internal References

Ref	Document	Publicly Available*
A	DWP Architectural Blueprint	No
B	Technical Vulnerability Management Policy	Yes
C	SS-001 – pt 2 Privileged User Access Security Standard	Yes
D	DWP Security Assurance Strategy	No

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 4 – External References

External Documents List
CIS Critical Security Controls set.
NIST – Cyber security Framework – 2018-04-16
NIST – 800-53 – Rev 5 – Security and Privacy Controls for Information
CISA Known Exploited Vulnerabilities Catalog

Appendix D. Abbreviations

Table 5 – Abbreviations

Abbreviation	Definition	Owner
CIS	Centre for Internet Security	Industry body
CMDB	Configuration Management Database	Industry term
CVSS	Common Vulnerability Scoring System - The Common Vulnerability Scoring System (CVSS) 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 organizations properly assess and prioritize their vulnerability management processes.	Industry term
CWE	The Common Weakness Scoring System (CWSS) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry.	Industry term
DDA	Digital Design Authority	Internal body
DWP	Department of Work and Pensions.	UK Government
GSCP	Government Security Classification Policy	UK Government
NIST	National Institute of Standards and Technology	US Government
NIST – CSF	National Institute of Standards and Technology – Cyber Security Framework	US Government
OS	Operating System	Industry term
OWASP	Open Web Application Security Project	Open source

Appendix E. Glossary

Table 6 – Glossary

Term	Definition
Patch	In the context of this document, a Security Patch or Patch is any fix that remediates a vulnerability within the system. Patches that only update or make functional changes are out of scope of patching. Patches that make both functional and security changes are in the scope of this document. Immutable infrastructure is kept up to date continuously, via updates or upgrades, which achieve the same purpose as patching.
Emergency Patch	For the purposes of this document, these are typically out of cycle, irregular patches that have not yet been applied. They fix vulnerabilities that could have an enterprise wide impact where there is clear evidence they are being actively exploited in other organisations, or, where the threat is deemed imminent, it is believed existing compensating controls will not provide mitigation.
Authorised patch	A patch authorised by the Triage team which may or may not come from the vendor.
CVSS	Common Vulnerability Scoring System - The Common Vulnerability Scoring System (CVSS) 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 organizations properly assess and prioritize their vulnerability management processes.
CWE	The Common Weakness Scoring System (CWSS) provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry.
End point	Servers, laptops, tablets, mobile phones, printers, multi-function devices, network device or other devices which connect to corporate networks.
IDS/ IPS	Intrusion Detection System/ Intrusion Prevention System.
ISM	Information Security Management.
Immutable Infrastructure	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.

Blue/Green Deployment	Blue green deployment is an application release model that gradually transfers user traffic from a previous version of an app or microservice to a nearly identical new release. The old version can be called the blue environment while the new version can be known as the green environment. Once traffic is fully transferred from blue to green, blue can stand by in case of rollback or pulled from production and updated to become the template upon which the next update is made.
Evergreening	Evergreening refers to running services comprised of components that are always up to date. Evergreen IT encompasses not only the services at the user level, but all of the underlying infrastructures, whether on-site or outsourced.
Risk Register	DWP ESRM Risk Register (GRC).
Vendor	A vendor patch is an update to a program provided by a software vendor to fix a problem with the software. A patch is typically a small update that does not significantly change the functionality. Typically, patches are deployed to fix bugs that have been discovered in a program, especially security vulnerabilities. The term distinguishes patches from the vendor from unofficial patches from users.
Zero Day Exploits	A zero-day exploit is a vulnerability (weakness) in software. It is called Zero-day because it is exploited before the vulnerability fix is made available by the vendor.

Appendix F. Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:
https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility
https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps