IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Security Standard – Security Boundaries (SS-006)

Chief Security Office

Date: 26/05/2017

Department for Work & Pensions

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Version Control Table

Version	Date	Major Change

Updating policy

This Standard will be reviewed for continued completeness, relevancy and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Contents

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

1. Introduction

1.1. This security standard provides the list of controls that are required to secure the security boundaries implemented by the Department of Work and Pensions (DWP) to an approved level of security.

For the purpose of this standard – A security domain is considered to consist of a set of information assets that are subject to a common set of security characteristics and policies.
A security boundary is considered to be the point of demarcation and control between interconnected security domains.

1.2. Examples of typical scenarios where the standard will be applied are described below.

- Connectivity between the Department's internal infrastructure and Internet hosted services.
- Connectivity between the Department's internal network and third party networks.
- Connectivity between the various security Zones/Domains within the DWP environments.

This standard provides a list of security controls to protect citizen and operational data stored and processed within DWP system and to minimise the risk from known threats both physical and logical to an acceptable level for operations.

1.3. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all departmental technology.

1.4. Furthermore the security controls presented in this standard are aligned with the international best practice for Network Security Boundary controls described within NIST 800-53, ISO 27033 and have been tailored for departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements enabling solutions to be developed, deployed and managed to Departmental security standards.

2.2. Secondly, this standard provides a controls Checklist to conduct compliance based technical security audits against.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

3. Exceptions

3.1. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to an assigned Security Architect and considered for submission to the DWP Design Authority (DA) advisory or governance board, where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

3.2. Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this standard.

3.3. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

4. Audience

4.1. This standard is intended for Suppliers, Developers, project teams, security groups, and also IT staff such as Security Compliance Teams, involved in securing environments for DWP systems and applications.

5. Scope

5.1. This standard is to cover systems storing or processing data at the OFFICIAL tier of the Government Security Classification Policy (GSCP). All of the organisation's network security boundaries (including those deployed internally, facing externally and where logically extended – e.g into a Cloud provisioned service) 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.

5.2. The security control requirements laid out in this standard are product agnostic and applicable for all Security Boundaries systems that are provisioned for departmental use.

5.3. In the event of uncertainty on the controls laid out in this standard please contact the Security front door for guidance and support on items which require clarification.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

6. Security Controls Assurance

6.1. Controls presented in this standard or referred to via this standard may be subjected to a formalised IT Health Check to provide evidence of adequacy and effectiveness.

7. Technical Security Control Requirements

In this document the term MUST in upper case is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see section 3 Exceptions above).

7.1 Policy

Reference	Security Control requirement
10.1.1	A policy MUST be created for each security boundary being implemented. This policy MUST reflect the **Threat, and/or Vulnerability** that the controls within the boundary seek to address and the level of **Risk** that the threat presents. The policy MUST be informed by the output of a documented risk assessment.
10.1.2	The security policy MUST describe the ID and A (Identity and Authentication) requirements to be applied to the interactive user sessions entering or leaving the security boundary.
10.1.3	The security policy MUST describe the Authentication requirements for System to System connections entering or leaving the security boundary.
10.1.4	The Policy MUST define the endpoints that are allowed to communicate across the boundary
10.1.5	The policy MUST describe the Inspection requirements to be applied to traffic traversing the security boundary.
10.1.6	The policy MUST define transformation rules that need to be applied to data traversing the security boundary.
10.1.7	The policy MUST describe the requirements for session breaks and the use of proxy techniques within the security boundary.
10.1.8	The Boundary policy MUST describe the requirement for Data Loss Prevention (DLP) at the boundary. This will be accomplished by defining the information that the boundary service needs to identify and the action to be taken on its detection.
10.1.9	The policy MUST define the encryption related capabilities of the security boundary
10.1.10	The policy MUST describe the Monitoring and Alerting requirements to be applied to systems, activities and processes that are internal to the security boundary.
10.1.11	All changes to the security boundary policy MUST be implemented following a rigorous and consistent approvals process.

7.2 Implementation

Reference	Security Control requirement
10.2.1	Security boundaries MUST prevent the passing of traffic until their compliance with policy has been verified.
10.2.2	The outer perimeter of a security boundary, between any DWP trusted network and an untrusted network (non DWP managed) MUST be built upon an infrastructure that is physically separate from the network infrastructures to which it is connected
10.2.3	The configuration of the devices that form the security boundary MUST be reviewed and validated by performing a technical compliance check on a regular basis (at least annually)
10.2.4	The boundary MUST be built in accordance with the boundary security Policy.
10.2.5	The boundary MUST be able to support both virtualised and physical implementations

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

Reference	Security Control requirement
	of components
10.2.6	The security boundary MUST include the capability to consume CLOUD based security services where these are deemed appropriate (following the assessment in 10.1.1.)
10.2.7	Devices (both physical and virtual) performing the security enforcing functions MUST themselves be resistant to compromise. • The devices MUST expose only those services required to fulfil the required capability • Logging of all administrative events MUST take place. • Alerting of events MUST be sent to a host that resides outside the Boundary Service (to a secure service) • Consideration MUST be given to generating Alerts on changes to the device configuration. (Integrity Testing) • All administrative access to the devices MUST make use of 2 Factor Authentication Technology. (See SS-01 Access and Authentication) • Access MUST be granted in a granular fashion enforcing the principle of least privilege. • Where the devices themselves terminate traffic – such as devices used as proxies, bastion host and protocol breaks, Anti malware software MUST be installed on the device.
10.2.8	Where service load is required to be distributed across a number of components within the boundary, the load balancing capability MUST be provided from within the security boundary perimeter.

7.3 Network Perimeter Controls

Reference	Security Control Requirement
10.3.1	The Boundary service Must provide a filter service to ensure that only authorised endpoints may communicate across it.
10.3.2	Where content inspection is required by the boundary policy, The Inspection capability MUST include the ability to provide deep packet inspection and be cognisant of application layer protocols. (Must provide layer 2 to 7 inspection capability) the content analysis applied MUST consider as a minimum ;- • Protocol analysis; (layer 2 to 7 of the OSI model) • Signature-based scanning (searching for known patterns); • Behavioural analysis (analysing code for functions and behaviour known to be associated with malicious code); • Sandbox technology; (executing suspect code within a safe environment to assess the behaviour) • Message Structure and Format; (is the message structure as expected, - length, field structure, character set for example) • Message Payload. (Does the payload conform to allowed characteristics, file types, Size, for example)
10.3.3	Where the boundary service malware detection process triggers any deletion or quarantine actions they MUST take place within the security boundary.
10.3.4	The ability to identify and block the egress of specific data assets MUST be implemented where the boundary lies between a DWP trusted and an untrusted

Reference	Security Control Requirement
	network.
10.3.5	Where the policy has identified the need for Data and Message Transformation mechanisms to be employed, then these mechanisms MUST maintain the integrity of the transformed data.

7.4 Encryption

Reference	Security Control Requirement
10.4.1	Where content inspection is required by the boundary policy The boundary MUST provide the capability to inspect all encrypted traffic on ingress into the boundary.
10.4.2	Encryption capabilities within the boundary MUST support as a minimum, all the departmental approved encryption algorithms and implementations.
10.4.3	The boundary MUST not allow encrypted session parameters to be negotiated outside the approved values (e.g algorithm, key length,)
10.4.4	Where the boundary lies between the DWP and an external service that consumes DWP encryption capabilities. Then the boundary MUST support the ability to expose DWP encryption services to external consumers. Typically these services would include:- • CRL (Certification Revocation lists or an OCSP (Online Certificate Status Protocol service). • Key distribution service – to allow external consumption of keys mastered within the DWP.

7.5 Authentication

Reference	Security Control Requirement
10.5.1	The boundary MUST as a minimum support authentication of all sessions, connections and flows into the boundary using DWP approved authentication mechanisms.
10.5.2	Where appropriate the Boundary MUST support external consumption of Authentication tokens or other Federation mechanisms. The DWP network infrastructure is seen as the Identity Provider for DWP internal users.
10.5.3	All administrative access to the devices within the security boundary MUST make use of 2 Factor Authentication
10.5.4	All administrator access to the components within the boundary must be authenticated using individual accounts. The use of shared or service accounts being used to authenticate individuals is prohibited.

7.6 Authorisation

Reference	Security Control Requirement
10.6.1	The Boundary MUST have the capability to control access to end points based upon the access control policy applied to the user or service requesting access to the endpoint..
10.6.2	The Boundary MUST be able to provide administrative access to its components based upon authorised profiles of individual users. (RBAC Role Based Access Control)
10.6.3	All authorised access MUST be in accordance with the boundary policy

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

7.7 Service Restriction

Reference	Security Control Requirement
10.7.1	The Boundary MUST expose at its internal and external perimeters only the **minimum** set of services required to meet the boundary policy. (AC02)
10.7.2	Components within the boundary MUST only expose services that are required to meet the boundary policy

7.8 Logging and Monitoring

Reference	Security Control Requirement
10.8.1	Logging of activities relating to the services and systems within the security boundary MUST be carried out in accordance with the boundary policy and in accordance with the Protective Monitoring standard Ref 3 EV01
10.8.2	Where the security boundary provides an interface into an externally hosted DWP service e.g use of IaaS, PaaS or SaaS by the department the security boundary MUST be capable of relaying Logging and Event information from these external sources into the DWP monitoring service.
10.8.3	Logging MUST take place of all administrative activities carried out upon Boundary components.

7.9 Administration

Reference	Security Control Requirement
10.9.1	All services within the Boundary must be executing on supported hardware and software versions
10.9.2	All components within the boundary service MUST have an appropriate support contract with the Vendor.
10.9.3	All components within the boundary MUST be maintained to the latest appropriate patch level – and should be subject to an expedited patch process to cater for security critical patches.
10.9.4	Administration activities MUST take place over an administrative network that is separated from the production data paths within the boundary infrastructure.
10.9.5	Administration connectivity MUST not bypass any traffic separation measures established within the Boundary
10.9.6	All action undertaken by an Administrator **MUST** be logged

8. Compliance

Compliance with this standard MUST occur as follows:

Compliance	Due Date
On-going	From the first day of approval
Retrospective	Within 6 months of the approval of the standard.

9. Accessibility

No user interfaces are included in this standard and accessibility is not applicable as part of this standard. However it deemed that projects implementing this standard are obliged to incorporate accessibility functions where necessary.

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

10. Security Standards Reference List

Document Name	Location	Version
Exceptions Process		
Standards Master List	Standards Master list	n/a – most up to date version are accessed from Sharepoint / Blueprint Online

11. Reference Documents

ISO27033 part 4 Network Security

NIST SP800-41 Guidelines on firewalls and Firewall policy

NCSC Cloud Security Principles

12. Definition of Terms

Term	Definition
Cryptographic Items	All logical and physical items used to achieve confidentiality, integrity, non-repudiation and accountability; including, but not limited to: devices, products, systems, key variables and code systems.
Cryptographic Key Material	Any parameter passed to an encryption cipher which influences the output of the algorithm (with the exception of the message itself).

13. Glossary

Glossary	Definition
AES	Advanced Encryption Standard – defined in FIPS 197. Different modes of operation are covered in different documents.
CA	Certificate Authority
DA	Design Authority (DA)
DWP	Department of Work and Pensions (DWP)

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

14. Controls Catalogue Mapping

The table below shows how the controls in this standard map to the DWP Controls Catalogue and thereon to control points in international security standards including but not limited to ISO/IEC 27002:2013, NIST 800-53, and the OWASP ASVS.

SS-006 Secure Boundary Standard	**DWP Controls Catalogue - Baseline Control Set**	**DWP Controls Catalogue - Baseline Control Set**
10.1.1	DWP_NT03	Networks shall be managed and controlled to protect information in systems and applications.
10.1.2	DWP_AC16	Access to information and application system functions shall be restricted in accordance with the access control policy.
10.1.3	DWP_AC16	AS 10.1.2
10.1.4	DWP_NT05	Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This type of enhanced protection limits the potential harm from cyber-attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or sub-networks, cross-domain devices separating sub-networks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys
10.1.5	DWP_MW03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-006 Secure Boundary Standard	**DWP Controls Catalogue - Baseline Control Set**	**DWP Controls Catalogue - Baseline Control Set**
		network and systems components.
10.1.6	DWP_MW03	As 10.1.5
10.1.7	DWP_MW03	As 10.1.5
10.1.8	DWP_AC16	As 10.1.2
10.1.9	DWP_CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.1.10	DWP_EV01,DWP_EV05	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
10.1.11	DWP_OP03	Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.
10.2.1	DWP_SD13	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.
10.2.2	DWP_NT05	Organizations can isolate information system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and to more effectively control information flows between those components. This

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-006 Secure Boundary Standard	**DWP Controls Catalogue - Baseline Control Set**	**DWP Controls Catalogue - Baseline Control Set**
		type of enhanced protection limits the potential harm from cyber-attacks and errors. The degree of separation provided varies depending upon the mechanisms chosen. Boundary protection mechanisms include, for example, routers, gateways, and firewalls separating system components into physically separate networks or sub-networks, cross-domain devices separating sub-networks, virtualization techniques, and encrypting information flows among system components using distinct encryption keys.
10.2.3	DWP_CP09	Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.
10.2.4	DWP_CP09	As 10.2.3
10.2.5	DWP_AC14	Asset owners shall review users' access rights at regular intervals.
10.2.6		
10.2.7	DWP_OP01	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.
10.2.8	DWP_OP01	As 10.2.7
10.3.1	DWP_NT05,NT08	As 10.1.4 Groups of information services, users and information systems shall be segregated on networks.
10.3.2	DWP_MW01	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
10.3.3	DWP_MW03	As 10.1.5
10.3.4	DWP_TR01	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.
10.3.5	DWP_TR01,TR02	As 10.3.5

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-006 Secure Boundary Standard	**DWP Controls Catalogue - Baseline Control Set**	**DWP Controls Catalogue - Baseline Control Set**
		Information involved in electronic messaging shall be appropriately protected.
10.4.1	TR01	As 10.3.5
10.4.2	CY06	As 10.1.9
10.4.3	CY06	As 10.1.9
10.4.4	CY06	As 10.1.9
10.4.5		
10.5.1	AC16	As 10.1.2
10.5.2	AC16	As 10.1.2
10.5.3	AC16	As 10.1.2
10.5.4	AC16	As 10.1.2
10.5.5		
10.6.1	NT02	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.
10.6.2	AC02	Users should only be provided with access to the network and network services that they have specifically been authorised to use.
10.6.3	AC16	As 10.1.2
10.6.4		
10.7.1	AC02	As 10.6.2
10.7.2	AC02	As 10.6.2
10.8.1	EV01	As 10.1.10
10.8.2	EV03	The cloud service provider should provide logging capabilities to the cloud service customer.
10.8.3	EV05	As 10.1.10
10.9.1	PH10	Equipment shall be correctly maintained to ensure its continued availability and integrity.
10.9.2	PH10	As 10.9.1
10.9.3	PH10	As 10.9.1
10.9.4	NT05	As 10.1.4

IMPORTANT. DWP Security Policies and Standards apply to DWP suppliers and contractors where explicitly stated in the Security Schedule of the contract. DWP Standards are not a cross government requirement.

SS-006 Secure Boundary Standard	**DWP Controls Catalogue - Baseline Control Set**	**DWP Controls Catalogue - Baseline Control Set**
10.9.5	NT05	As 10.1.4
10.9.6	EV05	As 10.1.10