

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 – Network Security Design (SS-018)

Chief Security Office

Date: September 2017



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

1.	Introduction	4
2.	Purpose	4
3.	Exceptions	4
4.	Audience.....	5
5.	Scope	5
6.	Security Controls Assurance.....	5
7.	Technical Security Control Requirements	5
8.	Generic Network Security Requirements	6
8.1.	Policy	6
8.2.	Network Perimeter Requirements	6
8.3.	Protecting data.....	7
8.4.	Protecting the enterprise network.....	7
8.5.	Segmentation.....	8
8.6.	Securing Network Services and Devices.....	8
8.7.	Maintaining Network Security.....	9
8.8.	Access Control.....	9
8.9.	Patching & Testing.....	10
8.10.	Redundancy.....	10
8.11.	Administration & Management	10
8.12.	Protective Monitoring	11
8.13.	Users Instructions and Training.....	12
8.14.	Roles and Responsibilities	12
8.15.	Incident management.....	12
8.16.	Physical Security.....	12
9.	Office Local Area Network (LAN)	12
9.1.	Additional LAN Requirements	13
9.2.	Wireless Networking	13
10.	Wide Area Network (WAN)	13
10.1.	Core WAN Requirements.....	13
10.2.	Internet Access	13
10.3.	Routing Security.....	13
10.4.	Service Resilience	14
11.	Datacentre	14
11.1.	General Requirements	14
11.2.	Network and Boundary Controls	15
11.3.	Network Storage Devices.....	15
11.4.	Physical Security.....	16
12.	Virtual Private Networks (VPNs)	16
12.1.	VPN Core Requirements.....	16
12.2.	VPN Gateway	17
12.3.	VPN Endpoint Devices.....	17
13.	Compliance.....	17
14.	Accessibility	17
15.	Security Standards Reference List.....	17
16.	Reference Documents	17
17.	Definition of Terms.....	18
18.	Glossary	19
19.	Controls Catalogue Mapping.....	20

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 Network Design Security Standard provides the list of controls that are required to secure networks to a Department for Work and Pensions (DWP) approved level of security. This standard provides a list of security controls to protect citizen and operational data. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations.
- 1.2. For further clarity and relevance, this standard is aligned to the DWP Digital Blueprint, which defines the direction for all departmental technology.
- 1.3. Furthermore the security controls presented in this standard are taken from the international best practice for network security 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 which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for network deployments.
- 2.2. Secondly, this standard provides a baseline requirement to inform compliance based technical security audits.

3. Exceptions

- 3.1. 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 as detailed below.
- 3.2. 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.
- 3.3. 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.
- 3.4. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to senior management.

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.

4. Audience

- 4.1. This standard is intended for Security and Technical Architects, Suppliers, Database Administrators, developers, 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 relates to the network infrastructure and components that provide connectivity for internal users of the DWP information systems within the OFFICIAL tier of the Government Security Classification Policy (GSCP). This standard covers office LAN infrastructure supporting desktops and mobile devices that have a wired connection to the DWP network. This includes services that support the office LAN but are located within DWP datacenters. This standard also covers wide area infrastructure which provides connectivity between these office locations and business applications hosted within or externally to the DWP Hosted infrastructure. 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 network 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 Advice Centre for guidance and support on items which require clarification.

6. Security Controls Assurance

- 6.1. Controls presented in this standard or referred to via this standard may be the subject of a formalised IT Health Check or Penetration Test 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).

Any reference to sensitive data in the security requirements refers to data that has been classified at the OFFICIAL or OFFICIAL-SENSITIVE tier or otherwise data that could be useful for malicious actors intending to attack the network.

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.

8. Generic Network Security Requirements

8.1. Policy

Reference	Security Control Requirement
8.1.1.	There MUST be a DWP information security policy that considers network connections/network security (it must cover use of all DWP network services and system operating procedures for admins).

8.2. Network Perimeter Requirements

Network perimeter controls MUST be deployed in accordance with SS-006 Secure Boundaries standard. The following controls are the principal, best practice requirements required to secure an external physical network perimeter from outside networks. For further details and requirements, please refer to the Secure Boundaries standard.

Reference	Security Control Requirement
8.2.1.	Access to ports, protocols and applications MUST be managed by filtering and inspecting all possible traffic at the network perimeters to ensure that only authorised, minimum necessary, traffic which is required to support DWP business is being exchanged.
8.2.2.	All inbound and outbound connections to the DWP network MUST be examined and managed (including encrypted data, where applicable) using network security enforcing components.
8.2.3.	Packet filtering (i.e. with the use of a packet filtering/screening router) MUST be conducted at the network perimeter to filter out unwanted packets.
8.2.4.	Firewalls MUST be used to create a demilitarised (DMZ) zone between the Internet (and other untrusted networks) and the networks used by DWP, in compliance with SS-013 Firewall Security Standard and the DWP Firewall Security Policy. The firewall rule set MUST deny incoming traffic by default, returning traffic only for established connections and a whitelist MUST be applied that only allows authorised protocols, ports and applications to exchange data across the boundary.
8.2.5.	All encrypted traffic from outside the DWP network MUST firstly be decrypted and passed through a content checker before being directed to its intended recipient. Similarly where required, encrypted data MUST only be allowed to leave the network after being content checked.
8.2.6.	There MUST be malware checking solutions (and where required, subject to risk assessment, reputation-based scanning services) to examine both inbound and outbound data at the perimeter in addition to protection deployed internally (in accordance with SS-015 Malware Protection Security Standard). Using different antivirus and malware solutions is good practice to protect the enterprise network and systems in order to provide some additional defence in depth.
8.2.7.	There MUST be no direct connectivity between inside the enterprise network and external networks. All incoming and outgoing traffic MUST pass through some form of security boundary before being allowed onto the enterprise network. An application proxy could be used to ensure that there is no direct connection between enterprise client systems and systems hosted on the Internet. The application proxy is used to check inbound and outbound packets and to: <ul style="list-style-type: none"> a. Hide the details of network internals to the external interface (details of IP addresses, user details, software, etc.) and deny this information to potential external attackers. b. Provide a Protective Monitoring point for user activity that can be used to make users accountable for their use of the connection. c. Provide session breaking and malware scans (A session is an open connection between two endpoints)
8.2.8.	There MUST be filters for mobile code on the gateways to the Internet, with mobile code accepted only from uncritical, white listed sites or only digital signed mobile code signed from approved Certification Authorities or from approved vendors

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
	(enable the respective configuration options on the client side, e.g. actively manage and implement a white list of allowed code signing Certification Authorities).
8.2.9.	Network infrastructure devices on the perimeter MUST be hardened (in accordance with the relevant security standards and patterns) to avoid unauthorised access and compromise - this should include the use of secure protocols, disabling unused services, limiting access to necessary ports and protocols and the enforcement of authentication and access control where appropriate.

8.3. Protecting data

Reference	Security Control Requirement
8.3.1.	Appropriate cryptographic controls, MUST be used to protect sensitive data in transit over the network in accordance with SS-007 Use of Cryptography.
8.3.2.	Appropriate cryptographic controls MUST be used to protect sensitive data at rest within network components including temporary storage buffers in accordance with SS-007 Use of Cryptography.

8.4. Protecting the enterprise network

The enterprise network covers services, network devices and interconnections between the different parts of the organisation within DWP controlled locations and management of the whole network (where consuming cloud services outside these traditional locations, also see SS-023 Cloud Computing Security Standard).

Reference	Security Control Requirement
8.4.1.	Anti-virus and malicious code checking solutions with signature-based capabilities MUST be on the internal enterprise network in accordance with SS-015 Malware Protection Security Standard. Heuristic scanning methods MUST be considered as well.
8.4.2.	The network MUST be segregated into zones and appropriate controls should be applied between the zones (see section 11.5).
8.4.3.	Administrator access to any network component MUST use multi-factor authentication and strong authorisation controls (see SS-001 Access and Authentication Standard).
8.4.4.	Default administrative passwords for network equipment MUST be changed and default accounts MUST be removed. Authentication credentials MUST not be shared between users or devices. Passwords MUST be set in line with <u>DWP User Access Control Policy</u> (also see SS-001 Access and Authentication for further guidelines).
8.4.5.	Any error messages returned to enterprise or external systems or users MUST not include sensitive information that may be useful to attackers (except encrypted messages as part of event logging – see requirement 11.12.3).
8.4.6.	Intrusion detection and prevention systems MUST be deployed on appropriate areas of the network (e.g. network boundary, CNI systems, and significant critical applications) and MUST be configured by authorised and qualified staff (in compliance with SS-015 Malware Protection Security Standard and SS-012 Protective Monitoring). Alerts generated by the system MUST be promptly managed by appropriately trained staff.
8.4.7.	Network Address Translation MUST be used. The enterprise network IP address range should be 'non-routable' from the Internet.
8.4.8.	All configuration details of network devices (e.g. IP address) MUST be registered against the DWP CMDB.
8.4.9.	Deploy ACLs, where appropriate, to limit access to known and trusted communication partners.
8.4.10.	Traffic routing MUST be identified during design to avoid transiting insecure network environments.

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
8.4.11.	There must be hardening of security controls on network devices and supporting infrastructure including servers (see SS-008 Server Operating System Security Standard for servers). Unnecessary software, protocol, ports and services on the enterprise network MUST be disabled.
8.4.12.	Warning banners MUST be displayed to enforce legal and regulatory requirements. These should be presented on privileged and normal user access accounts.
8.4.13.	Remote access into the enterprise network MUST be in accordance with SS-016 Remote Access Security Standard

8.5. Segmentation

Boundaries between the security zones should conform to the requirements within the SS-006 Secure Boundaries Security Standard.

Reference	Security Control Requirement
8.5.1.	Networks of different risk profiles MUST be located in different security zones: <ul style="list-style-type: none"> • Devices and computer systems providing services for external networks (e.g., the Internet) MUST be located in different zones (De-Militarized Zone – DMZ) than internal network devices and computer systems. • Application or data assets with higher protective requirement MUST be located in dedicated security zones. • Devices and computer systems of low trust level such as remote access servers and wireless network access points MUST be located in dedicated security zones
8.5.2.	Networks of different types MUST be located in separate security zones: <ul style="list-style-type: none"> • User workstations MUST be located in different security zones than servers • Network and security management systems MUST be located in dedicated security zones • Systems in development stage MUST be located in different zones than production systems
8.5.3.	Network segmentation MUST be used to: <ul style="list-style-type: none"> • segregate administrative and maintenance capabilities from routine user access to business applications; • segregate applications with higher protective requirements from other applications; • segregate databases from ordinary users who do not have business requirements for access.

8.6. Securing Network Services and Devices

Reference	Security Control Requirement
8.6.1.	Switches MUST be secured and hardened in accordance with manufacturer and industry best practices
8.6.2.	There MUST be Anti-ARP spoofing technologies to protect network devices.
8.6.3.	Network services including Domain Name System (DNS), Network Time Protocol (NTP) and Dynamic Host Configuration Protocol (DHCP) must be secured in accordance with manufacturer and industry best practices or in accordance with relevant standards/patterns.

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.

8.7. Maintaining Network Security

Reference	Security Control Requirement
8.7.1.	Network Configurations MUST be audited at least annually (or after significant changes that occur earlier) and include network scanning. These checks must reference against group policy and network configuration rule-base(s).
8.7.2.	There MUST be regular back up of network configuration, network devices, and other critical servers or devices. Frequency and retention of the backups should be established according to service delivery requirements or otherwise risk assessment advice. The backed up data MUST be protected to the same level as the live devices that the backups reflect.
8.7.3.	Access to network configuration including backup, authentication databases and administrative services MUST only be available to authorised personnel. The network configuration MUST be protected from unauthorised modification.
8.7.4.	A security template providing a baseline configuration of the network MUST be maintained and not kept on the network – this is to facilitate recovery after a major outage or security incident.
8.7.5.	A formal change process MUST be established and all changes must be reviewed and authorised – this process should link to CMDB management.
8.7.6.	There MUST be a regular IT health check, at least once annually or at the point of major change or following changes that may have a significant effect on the network security controls. This is required to ensure that network security posture has not been weakened by the change.

8.8. Access Control

Reference	Security Control Requirement
8.8.1.	There MUST be a well-defined policy for access management (see SS-001 Access and Authentication and User Access Control Policy).
8.8.2.	Access to the enterprise network MUST only be granted to managed endpoints and devices.
8.8.3.	User access to the network MUST be via strong and agreed authentication (this can be via device authentication given there was prior authentication of user to device), with the use of multi-factor authentication where appropriate.
8.8.4.	Users MUST only be provided with access to the network and network services that they have specifically been authorised to use.
8.8.5.	As part of a privileged user management regime, the allocation and use of privileged access rights of the network infrastructure MUST be restricted and controlled to authorised administrators. They must be appropriately trained and cleared network administrators. Privileges MUST be periodically reviewed and removed where no longer required.
8.8.6.	The network MUST be designed to provide authentication and access controls for systems connecting to them. Unauthorised or noncompliant devices MUST be placed in a quarantine area where remediation can occur prior to gaining access to the network. This can be done by using the 802.1X protocol to secure the physical ports where end users connect.
8.8.7.	There MUST be consideration if a Network Admission Control (NAC) Appliance should be deployed on the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources.
8.8.8.	Infrastructure device access MUST be secured. This includes: <ul style="list-style-type: none"> • The accessible ports and access services MUST be limited. • Access to authorised services MUST be restricted from authorised originators only. • Session management MUST be enforced (e.g. enforce idle timeouts, time to live)

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
	<ul style="list-style-type: none"> Vulnerability to dictionary and DoS attacks MUST be minimised (e.g. Limit the rate of login attempts, Restrict the maximum number of concurrent sessions, enforce a lockout period upon multiple authentication failure attempts, enforce the use of strong passwords, log and monitor user login authentication failures) Access MUST only be granted to authenticated users, groups, and services. The principle of least privilege MUST be adopted for all authorised users. Deny outgoing access unless explicitly required There MUST be role based access control to limit the function the user is permitted to perform.

8.9. Patching & Testing

Reference	Security Control Requirement
8.9.1.	There MUST be regular patching and update of network components, applications and services in accordance with the DWP patching policy.
8.9.2.	Vulnerability management MUST be on all systems. Particular focus should be given to those receiving internet traffic, either on transport or application level, which includes all systems used in the context of the gateways used towards the Internet as well as end user systems used for accessing internet.
8.9.3.	Steps MUST be taken to annually audit existing security controls against established benchmarks (i.e. policies, standards, procedures and compliance obligations), including by security testing, vulnerability scanning etc.

8.10. Redundancy

Reference	Security Control Requirement
8.10.1.	The network MUST meet availability requirements (in accordance with the SLA requirement for that part of the network). Ideally, it should have no single point of failure.

8.11. Administration & Management

Reference	Security Control Requirement
8.11.1.	System and service management channels MUST be appropriately secured and separated from the data channels (i.e. in-band or out-of-band).
8.11.2.	<p>Management access to infrastructure devices MUST be secured. This includes:</p> <ul style="list-style-type: none"> Restricting access to authorised terminal and management ports Restricting access to authorised services and protocols only Only granting access to authenticated and authorised users <p>Also depending on the network, the following options are available and must be considered:</p> <ul style="list-style-type: none"> In large, dispersed networks where management terminals or systems are on a dedicated or sensitive architecture use Access Control Lists (ACL) to identify devices allowed to access management interfaces to prevent unauthorised access
8.11.3.	<p>The management network access MUST be deployed using the following best practices:</p> <ul style="list-style-type: none"> Enforce access control using a management boundary firewall Classify and prioritize management traffic

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
	<ul style="list-style-type: none"> • Provide network isolation using NAT • Enforce the use of encrypted, secure access, and reporting protocols
8.11.4.	Administrators must be prohibited from conducting 'normal' day-to-day business from their high privilege account.
8.11.5.	Administration and management MUST enforce individual user accounts.
8.11.6.	Administrators MUST use different passwords for their high-privilege and low-privilege accounts.
8.11.7.	Management traffic MUST be encrypted and MUST use agreed and secure protocols.
8.11.8.	Remote management MUST use tools which ensure strong and multi-factor authentication and which provide adequate integrity and confidentiality functions should be used.

8.12. Protective Monitoring

Reference	Security Control Requirement
8.12.1.	A protective monitoring solution for the network MUST be implemented in accordance with SS-012 Protective Monitoring.
8.12.2.	Audit logs MUST be drawn from a number of sources, such as routers, firewalls, IDS, and sent to a central audit server for consolidation and thorough analysis.
8.12.3.	Audit logs or error messages with sensitive data MUST be encrypted.
8.12.4.	There MUST be visibility and awareness into what is occurring on the network at any given time. This should include traffic statistics, system utilisation/status information, Syslog, SNMP, ACL logging, accounting, archive configuration change logger, packet capture, device access information etc.
8.12.5.	<p>Audit logs MUST be maintained that include the following types of event:</p> <ul style="list-style-type: none"> • a record of who accessed network infrastructure components, what occurred, and when, • Logging of all critical/non-critical transactions by users, • remote failed log-on attempts with dates and times, • failed re-authentication (or token usage) events, • security gateway traffic breaches, • remote attempts to access audit logs, • system management alerts/alarms with security implications (e.g. IP address duplication, bearer circuit disruptions), • configuration control changes including altering permissions for management interfaces and altering routing tables.
8.12.6.	<p>On-going monitoring MUST include coverage of the following:</p> <ul style="list-style-type: none"> • audit logs from firewalls, routers, servers, etc., • alerts/alarms from such as audit logs pre-configured to notify certain event types, from such as firewalls, routers, servers, etc., • output from IPS/IDS, • results from network security scanning activities, • information on events and incidents reported by users and support personnel, (as well as results from security compliance reviews)
8.12.7.	There MUST be the use of analysis tools to help to identify when network systems are behaving in an unexpected way or providing indications that systems are under attack or have been.

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
8.12.8.	There MUST be audit of the use of import and export services. Users can be provided with the means to 'self-audit' their use of import and export services.
8.12.9.	All network devices MUST be synchronised to the same network clock by using Network Time Protocol (NTP) to enable accurate and effective event correlation.
8.12.10.	Remote Monitoring MUST be enabled where appropriate.

8.13. Users Instructions and Training

Reference	Security Control Requirement
8.13.1.	Users MUST be provided with appropriate security training and documented security operating instructions on acceptable and secure use of networks.
8.13.2.	There MUST be appropriate knowledge and training of network systems and up-to-date security practices, controls, procedures, and architectures.
8.13.3.	Systems administrators and security managers MUST keep up-to-date with the latest information on vulnerabilities.

8.14. Roles and Responsibilities

Reference	Security Control Requirement
8.14.1.	Roles and responsibilities MUST be established and defined for personnel responsible for the security of the network including connections to the internet.
8.14.2.	There MUST be separation of duties for personnel responsible for the security of the network and personnel responsible for the security boundaries. Sensitive security operations MUST not be implemented by a single individual
8.14.3.	Only trained and authorised staff MUST be permitted to carry out network security tasks.

8.15. Incident management

Reference	Security Control Requirement
8.15.1.	A security incident management process for the network MUST be implemented in compliance with SS-014 Security Incident Management Standard.

8.16. Physical Security

Reference	Security Control Requirement
8.16.1.	All network devices (including communication cables) MUST be physically protected.
8.16.2.	There MUST be policies and practices governing physical security in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise.
8.16.3.	When network equipment is to be reused, disposed of or sent for repair outside of DWP security management boundary domain all sensitive data MUST be sanitised as described in HMG IA Standard No.5 (IS5), Secure Sanitisation or NCSC guidance

9. Office Local Area Network (LAN)

For Office LAN, all relevant requirements specified in Section 11 – Generic Network Security apply in addition to all the requirements below

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.

9.1. Additional LAN Requirements

Reference	Security Control Requirement
9.1.1.	Consideration MUST be given to whether it is appropriate for there to be content checking of incoming and outgoing traffic to the internet at the application layer and if there should be safeguards against potential bypass The content checking can include: <ul style="list-style-type: none"> • recursive checking • strict file type identification and filtering
9.1.2.	In addition to the anti-malware solutions deployed on the network, tiered anti-malware controls must be deployed to protect the LAN devices.

9.2. Wireless Networking

Reference	Security Control Requirement
9.2.1.	Wireless Networking MUST be in compliance with SS-019 Wireless Networking Security Standard and SS-016 Remote Access Security Standard. Wireless networks access points MUST be treated as untrusted and network controls must be implemented accordingly

10. Wide Area Network (WAN)

For Wide Area Network, all relevant requirements specified in Section 11 – Generic Network Security and Section 12 – Office LAN apply in addition to all the requirements below

10.1. Core WAN Requirements

Reference	Security Control Requirement
10.1.1.	Where there is a shared WAN backbone, enterprise WAN traffic MUST be separated from other traffic that may be on the WAN to enable the confidentiality and integrity of data.
10.1.2.	WAN network domains MUST be secured against attacks. For example, to protect against Layer 3-based network attacks this could include device hardening, anti-spoofing filtering, routing protocol security, protective monitoring, firewalls, and intrusion prevention systems.
10.1.3.	There MUST be data/file integrity verification using algorithms such as hash/checksums, certificates, validating all critical device configurations on the WAN network.

10.2. Internet Access

Reference	Security Control Requirement
10.2.1.	All exports to the Internet MUST be authorised by a user. Export authorisation should be traceable to the user who conducted the export. Validity checks MUST be conducted on users export authority (e.g. check for any revocation) and protect the integrity of exports. This could be achieved using digital signatures.

10.3. Routing Security

Reference	Security Control Requirement
10.3.1.	Routing sessions MUST be restricted to trusted peers and the origin and integrity of routing updates must be validated. This should include authenticating all routing peers and disabling routing on all unauthorised interfaces by default.

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
10.3.2.	Only legitimate networks MUST be advertised and propagated.
10.3.3.	Neighbour status changes that may indicate network connectivity and stability issues (due to an attack or general operations problems) MUST be detected and logged.
10.3.4.	Appropriate filters MUST be deployed at WAN edges where invalid routing information may be introduced.
10.3.5.	There MUST be IP spoofing protection that includes source address validation

10.4. Service Resilience

Reference	Security Control Requirement
10.4.1.	WAN resources MUST be protected from exhaustion attacks
10.4.2.	It MUST be ensured any limited resources at a remote site, such as a low bandwidth WAN link or a low performance platform, are not overwhelmed, and their utilization is optimised. This to preserve and optimise remote site services
10.4.3.	Device, link, and geographical diversity MUST be deployed to eliminate single points of failure.

11. Datacentre

For Datacentre, all relevant requirements specified in Section 11 – Generic Network Security Section 12 – Office LAN and Section 13 – Wide Area Network apply in addition to all the requirements below

11.1. General Requirements

Reference	Security Control Requirement
11.1.1.	There MUST be a firewall for datacentre ingress and egress traffic. The firewall must be in accordance with SS-013 Firewall Security Standard and the DWP Firewall Security Policy.
11.1.2.	The use of shared, virtualised network, server and storage infrastructure to host applications and databases containing OFFICIAL classified data must be in compliance with SS-025 Virtualisation Security Standard
11.1.3.	Virtualised network, server, storage machines and other virtualised network components MUST be provide the same level of security controls as per their physical counterparts.
11.1.4.	There MUST be the use of security controls (e.g. access control list) to prevent unauthorised user access.
11.1.5.	There MUST be platform and system security with the use of antivirus and malware protection (see SS-015 Malware Protection Security Standard) and HIDS/HIPS where considered necessary
11.1.6.	A separate services segment is required which can offer firewalling, application delivery scanning/control and additional security inspection capabilities to the hosting segments as appropriate
11.1.7.	Separate domains MUST be used to manage and monitor from a service and security perspective. There are four possible domains: <ol style="list-style-type: none"> 1. Management - common management components for managing the hosting service. 2. Security - similar to Management domain, but instead provides access to the security enforcing components. Accessed from a secure environment 3. Service Monitoring –Receives and stores all non-security alerts and monitoring feeds. Provides a platform for initial processing of events to provide de-duplication and event enrichment. Only accepts traffic

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
	(unidirectional) from hosted and supporting domains. Security monitoring and management treated within separate domains. 4. Security Monitoring –Receives (unidirectional), stores and forwards logs and events to the SOC via a secure channel.
11.1.8.	Network management tools MUST be hardened – this includes infrastructure orchestration tools to manage the configuration of network, compute or storage fabric.

11.2. Network and Boundary Controls

Reference	Security Control Requirement
11.2.1.	There MUST be physically separate external security boundary controls to inspect ingress/egress traffic to the data centre (configured in accordance with SS-006 Secure Boundaries Security Standard).
11.2.2.	There MUST be clear demarcation between different hosting segments enabling them to be supported independently.
11.2.3.	All inbound traffic MUST only come from an authorised source and must be forwarded to an authorised destination on the core datacentre network
11.2.4.	The datacentre MUST provide the ability for applications and data to be hosted in separate hosting segments to provide segregation of data and to control interactions between them
11.2.5.	Segregated network, compute and storage facilities MUST be provided to manage and monitor the datacentre infrastructure.
11.2.6.	Consideration MUST be given to determine which components of the datacentre infrastructure must be built using dedicated infrastructure components physically discrete from the overall shared network for added security.
11.2.7.	Consideration MUST be given to inform the extent and need for (traffic) filtering/separation for each of the layers 2, 3, 4 and 7 (of the OSI model) and the need for IPS/IDS either on the host and/or between segments.
11.2.8.	Infrastructure and application “Call Home” data flows (i.e. for updating) MUST be subject to risk assessment for protocol break and inspection in transit across boundaries with untrusted networks.

11.3. Network Storage Devices

Reference	Security Control Requirement
11.3.1.	There MUST be a firewall to protect storage devices from users on the network, with ACL where appropriate to enforce further separation. These measures should be backed up by implementing effective privilege management controls.
11.3.2.	If a SAN is being implemented using fibre channel (FC), then the following controls MUST be implemented: <ul style="list-style-type: none"> Any unnecessary accesses, ports or services MUST be appropriately locked down (i.e. set/configure FC switch ports, zones (subsets of servers and storage arrays), Logical Unit Number (LUN) masks, and any present proprietary access control mechanisms (such as virtual SANs)) An assured secure authentication mechanisms MUST be used between all FC devices (servers, switches and storage arrays) and make the authentication mutual Data-in-transit and all communications between FC devices MUST be encrypted

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.

11.4. Physical Security

Reference	Security Control Requirement
11.4.1.	The datacentre MUST have resilient diverse communications. In the event of a power failure, there MUST be provision to maintain continuity of power supply.
11.4.2.	Physical access to the servers, switches, routers, cables and other network devices MUST be restricted – for example, with the use of secure rooms and lockable cabinets.
11.4.3.	Networking equipment MUST be physically secured such that they cannot be disconnected, interfered or removed without authorisation.
11.4.4.	Where appropriate, hardware ports in networking equipment MUST be physically protected so that there can be no unauthorised connection.
11.4.5.	Ingress and egress to secure areas where network devices reside MUST be protected by appropriate entry controls and monitored using surveillance.

12. Virtual Private Networks (VPNs)

12.1. VPN Core Requirements

Reference	Security Control Requirement
12.1.1.	The confidentiality of data and code in transit in the tunnel between trusted and untrusted networks MUST use encryption of the data when it is in transit, to prevent compromise (see SS-007 Use of Cryptography).
12.1.2.	The integrity of data and code in transit in the tunnel MUST not be compromised. The mechanisms used to implement the VPN tunnel should support integrity checking of data and code in transit, using techniques such as message verification codes, message authentication codes and anti-replay mechanisms or integrity protection controls should be implemented in the end-systems.
12.1.3.	Authenticity of information crossing public IP networks MUST be provided between participating peers in a VPN.
12.1.4.	The tunnel establishment and operating process MUST be supported by authorisation controls and should include Access Control Lists.
12.1.5.	Security controls to counter denial of service attacks which are specific to tunnel mechanisms MUST be incorporated wherever necessary
12.1.6.	Split tunnelling MUST be prohibited.
12.1.7.	The VPN solution MUST maintain appropriate audit logs for the analysis of all actions at that endpoint.
12.1.8.	Technical vulnerability management MUST be present for all VPN devices. This means that the device must be kept in a hardened configuration and management arrangements must be in place to manage vulnerabilities.
12.1.9.	There MUST be hardening of VLANs against hopping and other attacks. This could be mitigated by applying best industry and manufacturer practices
12.1.10.	In VPN architectures where endpoint obfuscation is a requirement, controls MUST be implemented to mask source and destination locations of VPN users. The chosen solution will have to be approved by a DWP Security Architect or by Design Authority.
12.1.11.	The VPN MUST be in compliance with all relevant controls specified in SS-015 Malware Protection Security Standard and SS-016 Remote Access Security Standard.
12.1.12.	VPN deployment using portable media such as CD-ROMs, diskettes, etc. MUST be controlled, e.g. by creating delivery and receipt log(s) and by implementing restrictions on re-use of media such as a date/time expiration or limitation on the number of times an execution can be performed.

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.

12.2. VPN Gateway

Reference	Security Control Requirement
12.2.1.	The VPN gateway, which terminates any encryption used to protect the link from the endpoint, MUST be located in the security boundary.
12.2.2.	The VPN gateway MUST mutually authenticate with the device (with prior authentication of user to device having occurred) before allowing access.
12.2.3.	A VPN gateway MUST be set up by configuring it to the network configuration and port/application access required, installation of certificates (e.g. for Higher Layer VPNs), and the continuing network monitoring of the VPN gateway enabled.
12.2.4.	The VPN gateway MUST be protected against network layer attacks (e.g. through the use of firewalls). Ensure that only VPN traffic (nominally identified by destination port and protocol number) reaches the VPN gateway.

12.3. VPN Endpoint Devices

Reference	Security Control Requirement
12.3.1.	VPN endpoint MUST be configured to ensure that there is only communications between an always-on VPN and the hosting network.
12.3.2.	There MUST only be authorised endpoint connectivity to other networks or devices to avoid an uncontrolled device from another network compromising the VPN.

13. 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.

14. Accessibility

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

15. Security Standards Reference List

Document Name	Location	Version
Exceptions Process	TBD	N/A
DWP Baseline Control Set	DWP SharePoint	1.0
Standard Master List	TBD	N/A

16. Reference Documents

Centre for the Protection of National Infrastructure: Protection of Data Centres, April 2010

CESG Good Practice Guide 8 – Protecting External Connections to the Internet, Issue 1.0, March 2009

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.

CESG Good Practice Guide 35 – Protecting an Internal ICT Network, Issue 2.0, August 2011

[Cisco: Network Security Baseline](#)

[Cisco SAFE Reference Guide, July 8 2010](#)

[PSN Code of Connection, Version 1.31, March 2017](#)

[NCSC: Network Security Guidance](#)

ISO 27033: Network Security – Parts 1 -5

17. Definition of Terms

Term	Definition
Denial of service (DoS)	Prevention of authorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users
Demilitarised Zone (DMZ)	perimeter network (also known as a screened sub-net) inserted as a “neutral zone” between networks
Firewall	Type of security barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorised traffic, as defined by the local security policy, is allowed to pass.
Filtering	process of accepting or rejecting data flows through a network, according to specified criteria
Intrusion Detection System	technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks
Intrusion Prevention System	variant on intrusion detection systems that are specifically designed to provide an active response capability
Network Perimeter	physical or logical subnetwork that contains and exposes an organization’s external services to a public network
Network Zoning	the concept that system resources of different sensitivity levels (i.e., different risk tolerance values and threat susceptibility) should be located in different security zones
Network Telemetry	process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis
Router	network device that is used to establish and control the flow of data between different networks by selecting paths or routes based upon routing protocol mechanisms and algorithms
Security Domain	set of assets and resources subject to a common security 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.

Term	Definition
Security Gateway	Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy.
Switch	device which provides connectivity between networked devices by means of internal switching mechanisms, with the switching technology typically implemented at layer 2 or layer 3 of the OSI reference model
Security Boundary	the basic means of keeping network traffic flowing where you want and restricting it where you do not is a security boundary: dedicated firewall devices, firewall functions in IPS devices, and access control lists in network routers and switches
Tunnel	data path between networked devices which is established across an existing network infrastructure
Virtual Local Area Network	independent network created from a logical point of view within a physical network
VPN Gateway	A type of networking device that connects two or more devices or networks together in a VPN infrastructure. It is designed to bridge the connection or communication between two or more remote sites, networks or devices and/or to connect multiple VPNs together.

18. Glossary

Abbreviation	Definition
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard – defined in FIPS 197 . Different modes of operation are covered in different documents.
ARP	Address Resolution Protocol
DAM	Database Activity Monitoring
DHCP	Domain Host Configuration Protocol
DLP	Data Loss Protection
DMZ	Demilitarised Zone
DNS	Domain Name Service
DA	Design Authority (DA)
DoS	Denial of Service
DWP	Department for Work and Pensions (DWP)
DMZ	De-militarised Zone
FTP	File transfer protocol
HIPS/HIDS	Host-based Intrusion Protection/Detection System
HTTP/HTTPS	Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure
IPS/IDS	Intrusion Protection/Detection System
LAN	Local Area Network
MAC	Media Access Control
MITM	Man-in-the-middle
MPLS	Multi-protocol label switching

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.

Abbreviation	Definition
NAC	Network Admission Control
NAT	Network Address Translation
NAS	Network Attached Storage
NCSC	National Cyber Security Centre
NIPS/NIDS	Network Intrusion Protection/Detection System
NTP	Network Time Protocol
OOB	Out of Band
PKI	Public Key Infrastructure
PSN	Public Sector Network
QoS	Quality of Service
SAN	Storage Area Network
SNMP	Simple Network Management Protocol
SOC	Security Operations Centre
SQL	Structured Query Language
STP	Spanning Tree Protocol
SSD	Solid State Drive
SSH	Secure Shell
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross-Site Scripting

19. 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 Application Security Verification Standard (ASVS).

<i>SS-018 Network Security Design STANDARD</i>	DWP Controls Catalogue - Baseline Control Set	
Control Statement	Control Reference	Descriptor
11.1.1.		
11.2.1.		
11.2.2.		
11.2.3.		
11.2.4.		
11.2.5.		
11.2.6.	MW02	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

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-018 Network Security Design STANDARD	DWP Controls Catalogue - Baseline Control Set	
11.2.7.		
11.2.8.		
11.2.9.		
11.3.1.	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.
11.3.2.		
11.4.1.	MW02	See 11.2.6
11.4.2.	NT08	Groups of information services, users and information systems shall be segregated on networks.
11.4.3.		
11.4.4.		
11.4.5.		
11.4.6.		
11.4.7.		
11.4.8.	AS01	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
11.4.9.		
11.4.10.		
11.4.11.		
11.4.12.		
11.4.13.		
11.5.1.	NT08	See 11.4.2
11.5.2.	NT08	See 11.4.2
11.5.3.	NT08	See 11.4.2
11.6.1.		

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-018 Network Security Design STANDARD	DWP Controls Catalogue - Baseline Control Set	
11.6.2.	MH02	Media shall be disposed of securely when no longer required, using formal procedures to ensure data cannot be recovered.
11.6.3.		
11.7.1.		
11.7.2.	BC05	Back-up copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.
11.7.3.		
11.7.4.		
11.7.5.	<p>AP07</p> <p>CC01</p> <p>GV01</p>	<p>Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.</p> <p>Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.</p> <p>Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment,</p>

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-018 Network Security Design STANDARD	DWP Controls Catalogue - Baseline Control Set	
	OP03	<p>provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.</p> <p>Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.</p>
11.7.6.	AP03	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
11.8.1.	AC01	An access control policy shall be established, documented, and reviewed based on business and information security requirements.
11.8.2.		
11.8.3.	AC19	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.
11.8.4.	AC02	Users should only be provided with access to the network and network services that they have specifically been authorised to use.
11.8.5.	AC05 AC08	<p>A formal user registration and de-registration process shall be implemented to enable assignment of access rights.</p> <p>The allocation and use of privileged access rights shall be restricted and controlled.</p>
11.8.6.		
11.8.7.		
11.8.8.		
11.9.1.	AP07	See 11.7.5
11.9.2.	AP07 AP03	<p>See 11.7.5</p> <p>See 11.7.6</p>
11.9.3.	AU02	Audit plans shall be developed and maintained to address business process

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-018 Network Security Design STANDARD	DWP Controls Catalogue - Baseline Control Set	
	<p>AU03</p> <p>GV01</p> <p>AP03</p>	<p>disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.</p> <p>Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.</p> <p>See 11.7.5</p> <p>See 11.7.6</p>
11.10.1.	BC04	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.
11.11.1.		
11.11.2.		
11.11.3.		
11.11.4.		
11.11.5.		
11.11.6.		
11.11.7.		
11.11.8.		
11.12.1.		
11.12.2.	EV01	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
11.12.3.		
11.12.4.		
11.12.5.	EV05	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
11.12.6.		

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-018 Network Security Design STANDARD	DWP Controls Catalogue - Baseline Control Set	
11.12.7.		
11.12.8.		
11.12.9.	EV07	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source. A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.
11.12.10.		
11.13.1.	MW02	See 11.2.6
11.13.2.	HR01	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
11.13.3.		
11.14.1.	OR01	All information security responsibilities shall be defined and allocated.
11.14.2.	OR02	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.
11.14.3.		
11.15.1.		
11.16.1.		
11.16.2.		
11.16.3.	PH13	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
12.1.1.		
12.1.2.	MW02	See 11.2.6
12.2.1.		
13.1.1.		

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-018 Network Security Design STANDARD	DWP Controls Catalogue - Baseline Control Set	
13.1.2.		
13.1.3.		
13.2.1.		
13.3.1.		
13.3.2.		
13.3.3.		
13.3.4.		
13.3.5.		
13.4.1.		
13.4.2.		
13.4.3.		
14.1.1.		
14.1.2.		
14.1.3.		
14.1.4.		
14.1.5.		
14.1.6.		
14.1.7.		
14.1.8.		
14.2.1.		
14.2.2.		
14.2.3.		
14.2.4.		
14.2.5.		
14.2.6.		
14.2.7.		
14.2.8.		

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-018 Network Security Design STANDARD	DWP Controls Catalogue - Baseline Control Set	
14.3.1.		
14.3.2.		
14.4.1.	PH09	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.
14.4.2.		
14.4.3.		
14.4.4.		
14.4.5.	PH02	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
15.1.1.		
15.1.2.		
15.1.3.		
15.1.4.		
15.1.5.		
15.1.6.		
15.1.7.		
15.1.8.		
15.1.9.		
15.1.10.		
15.1.11.		
15.1.12.		
15.2.1.		
15.2.2.		
15.2.3.		
15.2.4.		
15.3.1.		
15.3.2.		