# Security Standard Network Security Design (SS-018)

## Chief Security Office

**Date: March 2020**

Department for Work & Pensions

## 1. Revision History

| Version | Author | Description | Date |
|---|---|---|---|
| 0.0a | | First Draft | 08/05/17 |
| 0.0b | | Amended to include early review feedback, added additional controls | 09/06/17 |
| 0.0c | | Amended to include feedback from Standard & Pattern Team | 29/06/17 |
| 0.0d | | Amended to include feedback from SME review | 26/07/17 |
| 0.0e | | Pre-approval draft | 14/08/17 |
| 1.0 | | First published version | 18/09/17 |
| 1.1 | | Document updated to include sections on Risk Management and Network Security Architecture. Authority Control References included. A small number of duplicate requirements have been removed. | 14/01/19 |
| 1.2 | | Incorporated comments from Security Architecture Team review. | 30/01/19 |
| 1.3 | | Following external review by Security Policy, Risk and Digital | 04/03/19 |
| 1.4 | | Version for external publication | 30/03/20 |

## 2. Distribution

| Version | Role/Area | Role | Date |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 3. Approval History

| Version | Approver Title | Role | Date |
|---|---|---|---|
| 1.0 | | Chief Security Officer | 18/09/17 |
| 1.3 | | Chief Security Officer | 04/03/19 |
| 1.4 | | Chief Security Officer | 30/03/20 |

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

# Contents

## 4. Introduction

4.1. This Network Security Design Standard provides the list of controls that are required to secure networks to an Authority 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.

4.2. Furthermore, the security controls presented in this standard are taken from the international best practice for network security and have been tailored for Authority suitability.

## 5. Purpose

5.1. The purpose of this document is to enable Suppliers to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Authority security standards, which are based upon international best practice for network deployments.

5.2. Secondly, this standard provides a baseline requirement to inform compliance based technical security audits.

## 6. Exceptions

6.1. 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.

6.2. Any exceptions to the application of this standard or where controls cannot be adhered to MUST be presented to the Authority where appropriate. This MUST be carried out prior to deployment and managed through the design caveats or exception process.

6.3. 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.

6.4. Exceptions to this standard MUST be maintained on a risk register for accountability, traceability and security governance reporting to the Authority.

## 7. Audience

7.1. This standard is intended for Security and Technical Architects, Suppliers, Database Administrators, Security Operations, Network Designers and Administrators, Developers, Security Groups and also IT staff such as

Security Compliance Teams involved in securing environments for Authority systems and applications.

## 8. Scope

8.1. This standard relates to the network infrastructure and components that provide connectivity for internal users of the Authority 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 Authority network. This includes services that support the office LAN but are located within Authority datacenters. This standard also covers wide area infrastructure which provides connectivity between these office locations and business applications hosted within or externally to the Authority Hosted infrastructure. The requirements will be applied to new and existing installations.

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

8.3. In the event of uncertainty on the controls laid out in this standard please contact the Authority for guidance and support on items which require clarification.

## 9. Security Controls Assurance

9.1. 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.

## 10. 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 [6. 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.

## 11. Generic Network Security Requirements

11.1. Policy

| Reference | Security Control Requirement |
|---|---|
| 11.1.1. | There MUST be an information security policy that considers network connections/network security (it MUST cover connection to all Authority network services and system operating procedures for admins). |
| 11.1.2. | The Authority will use ISO27033 as its framework for Network Security Design. |

11.2 Risk Management

| Reference | Security Control Requirement |
|---|---|
| 11.2.1 | Documentation MUST be available to describe the current network and planned changes to the network. This MUST be sufficiently detailed to describe connections and services and form a basis for consideration of network-related risks. |
| 11.2.3 | Characterise the network on the basis of the community of users:<br>- Unknown community of users<br>- A known community of users from a closed business community comprising members from more than one organisation<br><br>Then consider whether they are using a public or private network. |
| 11.2.4 | Consider the type of network:<br>Data, voice or hybrid. Also packet, switched or Multi-Protocol Label Switching (MPLS) |
| 11.2.5 | Collect other information to scope the network security design, as follows:<br>- Information types<br>- Business processes<br>- Actual or potential hardware components; software, services and connections<br>- Potential environments (locations and facilities)<br>- Activities (Operations) |
| 11.2.6 | The network security design MUST take account of the following types of risks;<br>Loss of-<br>- Confidentiality of information and code<br>- Integrity of information and code<br>- Availability of information and network services<br>- Non-repudiation of network transactions<br>- Accountability of network transactions<br>- Authenticity of information, users and administrator |

| Reference | Security Control Requirement |
|---|---|
| | - Reliability of information and code<br>- Ability to control unauthorised use of information and resources<br>- Ability to control abuse of authorised access |

## 11.3 Network Security Architecture

| Reference | Security Control Requirement |
|---|---|
| 11.3.1 | Different protocols have different security characteristics and should be afforded special consideration |
| 11.3.2 | The approach to Network Security Architecture MUST take account of ITU-T X.805. |
| 11.3.3 | The network Security Architecture MUST support the following security dimensions:<br>- Access control<br>- Authentication<br>- Non-repudiation<br>- Data confidentiality<br>- Communication security<br>- Data integrity<br>- Availability<br>- Privacy |
| 11.3.4 | Security protection MUST be provided for all three security layers as defined in X.805: the infrastructure layer, the services layer and the application layer. |
| 11.3.5 | It MUST be possible to separate the security concerns associated with each of the planes as defined in X.805: the planes are management, control and end-user. For example, if there is a flood of packets related to the end-user plane these MUST not interfere with the ability of the network administrator to correct the problem in the management plane. Take account of the security objectives for each plane as they are documented in X.805. |
| 11.3.6 | Network Security Design MUST include the following inputs:<br>- The Authority's documented service requirements<br>- Documentation of any planned architecture, design and implementation<br>- Current network security policy (or relevant parts of the information security policy) preferably based on a risk assessment combined with a management review<br>- Definition of the assets that should be protected<br>- Current and planned performance requirements |

| Reference | Security Control Requirement |
|---|---|
| | - Current information regarding the products which implement the network infrastructure |
| 11.3.7 | Network Security Design MUST include the following outputs:<br>- The network technical security architecture<br>- Service access requirements for each of the security gateways (including firewall rulesets)<br>- Security operating procedures<br>- Conditions for secure connection of Suppliers<br>- User guidelines for Suppliers |
| 11.3.8 | The Network Security Design MUST consider the following scenarios:<br>- Internet access for employees<br>- Enhanced collaboration services<br>- Business to business services<br>- Business to customer services<br>- Outsourced services<br>- Network segmentation (segregation)<br>- Mobile communication<br>- Networking support for travelling users<br>- Networking support for home users |
| 11.3.9 | The Network Security Design MUST consider the following technology topics:<br>- Local area networks<br>- Wide area networks<br>- Wireless networks<br>- Radio networks<br>- Broadband networks<br>- Security gateways<br>- Virtual Private Networks<br>- Voice networks<br>- IP convergence<br>- Web hosting<br>- Internet email<br>- Routed access to Suppliers<br>- Data centres |
| 11.3.10 | ISO27033 Part 2 contains guidelines for the design of network security. These guidelines should be followed. The design MUST take account of legal and regulatory requirements |
| 11.3.11 | The Network Security Design MUST define the roles and responsibilities which relate to network security |

| Reference | Security Control Requirement |
|---|---|
| 11.3.12 | Steps MUST be taken to audit of the effectiveness of Network Security controls. This MUST include IT Health Checks and other forms of security testing including vulnerability scanning. |
| 11.3.13 | The following design principles MUST be considered:<br>• Provide for defence-in-depth – create layered security controls such that, if one control fails, other controls will protect valuable assets<br>• Keep solutions simple – the objective of the design process is to produce the simplest possible outcome. Simple solutions are easier to explain to people and most likely to be reliable, deliverable and maintainable.<br>• Reduce Attack Surface - every feature that is added to an application adds a certain amount of risk to the overall application. The aim for secure development is to reduce the overall risk by reducing the attack surface area.<br>• Fail securely - When a system fails, it should do so securely. This typically involves several things: secure defaults (default is to deny access); on failure undo changes and restore to a secure state; always check return values for failure; and in conditional code/filters make sure that there is a default case that does the right thing. The confidentiality and integrity of a system should remain even though availability has been lost. Attackers must not be permitted to gain access rights to privileged objects during a failure that are normally inaccessible. Upon failing, a system that reveals sensitive information about the failure to potential attackers could supply additional knowledge for creating an attack. Determine what may occur when a system fails and be sure it does not threaten the system. |

## 11.4 Network Perimeter Requirements

Network perimeter controls MUST be deployed in accordance with SS-006 Security Boundaries Security 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 Security Boundaries Security Standard.

| Reference | Security Control Requirement |
|---|---|
| 11.4.1 | 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 Authority business is being exchanged. |

| Reference | Security Control Requirement |
|---|---|
| 11.4.2 | All inbound and outbound connections to the Authority network MUST be examined and managed (including encrypted data, where applicable) using network security enforcing components. |
| 11.4.3 | 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. |
| 11.4.4 | Firewalls MUST be used to create a demilitarised (DMZ) zone between the Internet (and other untrusted networks) and the networks used by the Authority, in compliance with SS-013 Firewall Security Standard. 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. |
| 11.4.5 | All encrypted traffic from outside the Authority 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. If it is not possible to decrypt the traffic it MUST be blocked. |
| 11.4.6 | 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. |
| 11.4.7 | 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:<br>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.<br>b. Provide a Protective Monitoring point for user activity that can be used to make users accountable for their use of the connection.<br>c. Provide session breaking and malware scans (A session is an open connection between two endpoints) |
| 11.4.8 | 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 (enable the respective configuration options on the client side, e.g. actively manage and implement a white list of allowed code signing Certification Authorities). |

| Reference | Security Control Requirement |
|---|---|
| 11.4.9 | Network infrastructure devices on the perimeter MUST be hardened (in accordance with the relevant security standards) 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. |

### 11.5 Protecting data

| Reference | Security Control Requirement |
|---|---|
| 11.5.1 | Appropriate cryptographic controls, MUST be used to protect sensitive data in transit over the network in accordance with SS-007 Use of Cryptography Security Standard. |
| 11.5.2 | 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 Security Standard. |

### 11.6 Protecting the enterprise network

The enterprise network covers services, network devices and interconnections between the different parts of the organisation within Authority 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 |
|---|---|
| 11.6.1 | 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. |
| 11.6.2 | The network MUST be segregated into zones and appropriate controls should be applied between the zones (see section 11.5). |
| 11.6.3 | Administrator access to any network component MUST use multi-factor authentication and strong authorisation controls (see SS-001 Access and Authentication Controls Security Standard). |
| 11.6.4 | 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 the Authority's User Access Control Policy (also see SS-001 Access and Authentication Controls Security Standard for further guidelines). |
| 11.6.5 | 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). |
| 11.6.6 | 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- |

| Reference | Security Control Requirement |
|---|---|
| | 015 Malware Protection Security Standard and SS-012 Protective Monitoring Security Standard). Alerts generated by the system MUST be promptly managed by appropriately trained staff. |
| 11.6.7 | Network Address Translation MUST be used. The enterprise network IP address range should be 'non-routable' from the Internet. |
| 11.6.8 | All configuration details of network devices (e.g. IP address) MUST be registered. |
| 11.6.9 | Deploy ACLs, where appropriate, to limit access to known and trusted communication partners. |
| 11.6.10 | Traffic routing MUST be identified during design to avoid transiting insecure network environments. |
| 11.6.11 | There MUST be hardening of security controls on network devices and supporting infrastructure including servers (see SS-008 Server Operating System Security Standard). Unnecessary software, protocol, ports and services on the enterprise network MUST be disabled. |
| 11.6.12 | Warning banners MUST be displayed to enforce legal and regulatory requirements. These should be presented on privileged and normal user access accounts. |
| 11.6.13 | Remote access into the enterprise network MUST be in accordance with SS-016 Remote Access Security Standard |

### 11.7 Segmentation

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

| Reference | Security Control Requirement |
|---|---|
| 11.7.1 | Networks of different risk profiles MUST be located in different security zones:<br>• 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.<br>• Application or data assets with higher protective requirement MUST be located in dedicated security zones.<br>• 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 |
| 11.7.2 | Networks of different types MUST be located in separate security zones:<br>• User workstations MUST be located in different security zones than servers<br>• Network and security management systems MUST be located in dedicated security zones |

| Reference | Security Control Requirement |
|---|---|
| | • Systems in development stage MUST be located in different zones than production systems |
| 11.7.3 | Network segmentation MUST be used to:<br>• segregate administrative and maintenance capabilities from routine user access to business applications;<br>• segregate applications with higher protective requirements from other applications;<br>• segregate databases from ordinary users who do not have business requirements for access. |

11.8 Securing Network Services and Devices

| Reference | Security Control Requirement |
|---|---|
| 11.8.1 | Switches MUST be secured and hardened in accordance with manufacturer and industry best practices |
| 11.8.2 | There MUST be Anti-ARP spoofing technologies to protect network devices. |
| 11.8.3 | 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. |
| 11.8.4 | Network products and services MUST be purchased through a process where security is one of the evaluation criteria. They MUST NOT be purchased if the risks of adoption are outside risk appetite and every effort MUST be made to choose more secure alternatives. |

11.9 Maintaining Network Security

| Reference | Security Control Requirement |
|---|---|
| 11.9.1 | 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). |
| 11.9.2 | 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. |
| 11.9.3 | 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. |
| 11.9.4 | 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. |

| Reference | Security Control Requirement |
|---|---|
| 11.9.5 | A formal change process MUST be established and all changes MUST be reviewed and authorised – this process should also link to configuration management. |
| 11.9.6 | 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. |

11.10 Access Control

| Reference | Security Control Requirement |
|---|---|
| 11.10.1 | There MUST be a well-defined policy for access management (see SS-001 Access and Authentication Controls Security Standard and User Access Control Policy). |
| 11.10.2 | Access to the enterprise network MUST only be granted to managed endpoints and devices. |
| 11.10.3 | 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. |
| 11.10.4 | Users MUST only be provided with access to the network and network services that they have specifically been authorised to use. |
| 11.10.5 | 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. |
| 11.10.6 | 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. |
| 11.10.7 | 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. |
| 11.10.8 | Infrastructure device access MUST be secured. This includes:<br>• The accessible ports and access services MUST be limited.<br>• Access to authorised services MUST be restricted from authorised originators only.<br>• Session management MUST be enforced (e.g. enforce idle timeouts, time to live)<br>• 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 |

| Reference | Security Control Requirement |
|---|---|
| | period upon multiple authentication failure attempts, enforce the use of strong passwords, log and monitor user login authentication failures)<br>• Access MUST only be granted to authenticated users, groups, and services.<br>• The principle of least privilege MUST be adopted for all authorised users.<br>• Deny outgoing access unless explicitly required<br>• There MUST be role based access control to limit the function the user is permitted to perform. |

11.11 Patching & Testing

| Reference | Security Control Requirement |
|---|---|
| 11.11.1 | There MUST be regular patching and update of network components, applications and services in accordance with the Authority's SS-033 Patching Security Standard andTechnical Vulnerability Management Policy. |
| 11.11.2 | 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. |
| 11.11.3 | 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. |

11.12 Redundancy

| Reference | Security Control Requirement |
|---|---|
| 11.12.1 | 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. |

11.13 Administration & Management

| Reference | Security Control Requirement |
|---|---|
| 11.13.1 | System and service management channels MUST be appropriately secured and separated from the data channels (i.e. in-band or out-of-band). |
| 11.13.2 | Management access to infrastructure devices MUST be secured. This includes:<br>• Restricting access to authorised terminal and management ports<br>• Restricting access to authorised services and protocols only |

| Reference | Security Control Requirement |
|---|---|
| | • Only granting access to authenticated and authorised users<br><br>Also depending on the network, the following options are available and MUST be considered:<br>• 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 |
| 11.13.3 | The management network access MUST be deployed using the following best practices:<br>• Enforce access control using a management boundary firewall<br>• Classify and prioritize management traffic<br>• Provide network isolation using NAT<br>• Enforce the use of encrypted, secure access, and reporting protocols |
| 11.13.4 | Administrators MUST be prohibited from conducting 'normal' day-to-day business from their high privilege account. |
| 11.13.5 | Administration and management MUST enforce individual user accounts. |
| 11.13.6 | Administrators MUST use different passwords for their high-privilege and low-privilege accounts. |
| 11.13.7 | Management traffic MUST be encrypted and MUST use agreed and secure protocols. |
| 11.13.8 | Remote management MUST use tools which ensure strong and multi-factor authentication and which provide adequate integrity and confidentiality functions should be used. |

## 11.14 Protective Monitoring

| Reference | Security Control Requirement |
|---|---|
| 11.14.1 | A protective monitoring solution for the network MUST be implemented in accordance with SS-012 Protective Monitoring Security Standard. |
| 11.14.2 | Audit logs MUST be drawn from a number of sources, such as routers, firewalls, IDS etc., and sent to a central audit server for consolidation and thorough analysis. |
| 11.14.3 | Audit logs or error messages with sensitive data MUST be encrypted. |
| 11.14.4 | 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. |
| 11.14.5 | Audit logs MUST be maintained that include the following types of event:<br>• a record of who accessed network infrastructure components, what occurred, and when,<br>• Logging of all critical/non-critical transactions by users,<br>• remote failed log-on attempts with dates and times,<br>• failed re-authentication (or token usage) events,<br>• security gateway traffic breaches,<br>• remote attempts to access audit logs,<br>• system management alerts/alarms with security implications (e.g. IP address duplication, bearer circuit disruptions),<br>• configuration control changes including altering permissions for management interfaces and altering routing tables. |
| 11.14.6 | On-going monitoring MUST include coverage of the following:<br>• audit logs from firewalls, routers, servers, etc.,<br>• alerts/alarms from such as audit logs pre-configured to notify certain event types, from such as firewalls, routers, servers, etc.,<br>• output from IPS/IDS,<br>• results from network security scanning activities,<br>• information on events and incidents reported by users and support personnel, (as well as results from security compliance reviews) |
| 11.14.7 | 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. |
| 11.14.8 | 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. |

| Reference | Security Control Requirement |
|---|---|
| 11.14.9 | All network devices MUST be synchronised to the same network clock by using Network Time Protocol (NTP) to enable accurate and effective event correlation. |
| 11.14.10 | Remote Monitoring MUST be enabled where appropriate. |

11.15 Users Instructions and Training

| Reference | Security Control Requirement |
|---|---|
| 11.15.1 | Users MUST be provided with appropriate security training and documented security operating instructions on acceptable and secure use of networks. |
| 11.15.2 | There MUST be appropriate knowledge and training of network systems and up-to-date security practices, controls, procedures, and architectures. |
| 11.15.3 | Systems administrators and security managers MUST keep up-to-date with the latest information on vulnerabilities. |

11.16 Roles and Responsibilities

| Reference | Security Control Requirement |
|---|---|
| 11.16.1 | Roles and responsibilities MUST be established and defined for personnel responsible for the security of the network including connections to the internet. |
| 11.16.2 | 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 |
| 11.16.3 | Only trained and authorised staff MUST be permitted to carry out network security tasks. |

11.17 Incident management

| Reference | Security Control Requirement |
|---|---|
| 11.17.1 | A security incident management process for the network MUST be implemented in compliance with SS-014 Security Incident Management Security Standard. |

11.18 Physical Security

| Reference | Security Control Requirement |
|---|---|
| 11.18.1 | All network devices (including communication cables) MUST be physically protected. |
| 11.18.2 | There MUST be policies and practices governing physical security in place to protect personnel, hardware, programs, networks and data from loss, damage or compromise. |
| 11.18.3 | When network equipment is to be reused, disposed of or sent for repair all sensitive data MUST be sanitised as described in HMG IA Standard No.5 (IS5), Secure Sanitisation or NCSC guidance |

## 12 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

12.6Additional LAN Requirements

| Reference | Security Control Requirement |
|---|---|
| 12.6.1 | 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<br>The content checking can include:<br>• recursive checking<br>• strict file type identification and filtering |
| 12.6.2 | In addition to the anti-malware solutions deployed on the network, tiered anti-malware controls MUST be deployed to protect the LAN devices. |

12.7 Wireless Networking

| Reference | Security Control Requirement |
|---|---|
| 12.7.1 | 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 |

## 13 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

13.6 Core WAN Requirements

| Reference | Security Control Requirement |
|---|---|
| 13.6.1 | 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. |
| 13.6.2 | 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. |
| 13.6.3 | There MUST be data/file integrity verification using algorithms such as hash/checksums, certificates, validating all critical device configurations on the WAN network. |

### 13.7 Internet Access

| Reference | Security Control Requirement |
|---|---|
| 13.7.1 | 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. |

### 13.8 Routing Security

| Reference | Security Control Requirement |
|---|---|
| 13.8.1 | 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. |
| 13.8.2 | Only legitimate networks MUST be advertised and propagated. |
| 13.8.3 | Neighbour status changes that may indicate network connectivity and stability issues (due to an attack or general operations problems) MUST be detected and logged. |
| 13.8.4 | Appropriate filters MUST be deployed at WAN edges where invalid routing information may be introduced. |
| 13.8.5 | There MUST be IP spoofing protection that includes source address validation |

### 13.9 Service Resilience

| Reference | Security Control Requirement |
|---|---|
| 13.9.1 | WAN resources MUST be protected from exhaustion attacks |
| 13.9.2 | 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 |
| 13.9.3 | Device, link, and geographical diversity MUST be deployed to eliminate single points of failure. |

## 14 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

14.6 General Requirements

| Reference | Security Control Requirement |
|---|---|
| 14.6.1 | There MUST be a firewall for datacentre ingress and egress traffic. The firewall MUST be in accordance with SS-013 Firewall Security Standard |
| 14.6.2 | 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 |
| 14.6.3 | Virtualised network, server, storage machines and other virtualised network components MUST provide the same level of security controls as per their physical counterparts. |
| 14.6.4 | 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 |
| 14.6.5 | Separate domains MUST be used to manage and monitor from a service and security perspective. There are four possible domains:<br>1. Management - common management components for managing the hosting service.<br>2. Security - similar to Management domain, but instead provides access to the security enforcing components. Accessed from a secure environment<br>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 (unidirectional) from hosted and supporting domains. Security monitoring and management treated within separate domains.<br>4. Security Monitoring – Receives (unidirectional), stores and forwards logs and events to the SOC via a secure channel. |
| 14.6.6 | Network management tools MUST be hardened – this includes infrastructure orchestration tools to manage the configuration of network, compute or storage fabric. |

14.7 Network and Boundary Controls

| Reference | Security Control Requirement |
|---|---|
| 14.7.1 | There MUST be physically separate external security boundary controls to inspect ingress/egress traffic to the data centre (configured in accordance with SS-006 Security Boundaries Security Standard). |
| 14.7.2 | There MUST be clear demarcation between different hosting segments enabling them to be supported independently. |

| Reference | Security Control Requirement |
|---|---|
| 14.7.3 | All inbound traffic MUST only come from an authorised source and MUST be forwarded to an authorised destination on the core datacentre network |
| 14.7.4 | 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 |
| 14.7.5 | Segregated network, compute and storage facilities MUST be provided to manage and monitor the datacentre infrastructure. |
| 14.7.6 | 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. |
| 14.7.7 | 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. |
| 14.7.8 | 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. |

### 14.8 Network Storage Devices

| Reference | Security Control Requirement |
|---|---|
| 14.8.1 | 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. |
| 14.8.2 | If a SAN is being implemented using fibre channel (FC), then the following controls MUST be implemented:<br>• 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))<br>• An assured secure authentication mechanism MUST be used between all FC devices (servers, switches and storage arrays) and make the authentication mutual<br>• Data-in-transit and all communications between FC devices MUST be encrypted |

14.9 Physical Security

| Reference | Security Control Requirement |
|---|---|
| 14.9.1 | The datacentre MUST have resilient diverse communications. In the event of a power failure, there MUST be provision to maintain continuity of power supply. |
| 14.9.2 | 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. |
| 14.9.3 | Networking equipment MUST be physically secured such that they cannot be disconnected, interfered or removed without authorisation. |
| 14.9.4 | Where appropriate, hardware ports in networking equipment MUST be physically protected so that there can be no unauthorised connection. |
| 14.9.5 | Ingress and egress to secure areas where network devices reside MUST be protected by appropriate entry controls and monitored using surveillance. |

## 15 Virtual Private Networks (VPNs)

15.6 VPN Core Requirements

| Reference | Security Control Requirement |
|---|---|
| 15.6.1 | 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). |
| 15.6.2 | 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. |
| 15.6.3 | Authenticity of information crossing public IP networks MUST be provided between participating peers in a VPN. |
| 15.6.4 | The tunnel establishment and operating process MUST be supported by authorisation controls and should include Access Control Lists. |
| 15.6.5 | Security controls to counter denial of service attacks which are specific to tunnel mechanisms MUST be incorporated wherever necessary |
| 15.6.6 | Split tunnelling MUST be prohibited. |
| 15.6.7 | The VPN solution MUST maintain appropriate audit logs for the analysis of all actions at that endpoint. |
| 15.6.8 | 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. |
| 15.6.9 | There MUST be hardening of VLANs against hopping and other attacks. This could be mitigated by applying best industry and manufacturer practices |

| Reference | Security Control Requirement |
|---|---|
| 15.6.10 | In VPN architectures where endpoint obfuscation is a requirement, controls MUST be implemented to mask source and destination locations of VPN users. |
| 15.6.11 | 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. |
| 15.6.12 | VPN deployment using portable media such as USBs, 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. |

### 15.7 VPN Gateway

| Reference | Security Control Requirement |
|---|---|
| 15.7.1 | The VPN gateway, which terminates any encryption used to protect the link from the endpoint, MUST be located in the security boundary. |
| 15.7.2 | The VPN gateway MUST mutually authenticate with the device (with prior authentication of user to device having occurred) before allowing access. |
| 15.7.3 | 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. |
| 15.7.4 | 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. |

### 15.8 VPN Endpoint Devices

| Reference | Security Control Requirement |
|---|---|
| 15.8.1 | VPN endpoint MUST be configured to ensure that there is only communications between an always-on VPN and the hosting network. |
| 15.8.2 | There MUST only be authorised endpoint connectivity to other networks or devices to avoid an uncontrolled device from another network compromising the VPN. |

## 16 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. |

## 17 Accessibility

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

## 18 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

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 - 6

Authority Technical Vulnerability Management Policy

## 19 Definition of Terms

| | |
|---|---|
| **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 |
| **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. |

## 20 Glossary

| | |
|---|---|
| **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 |
| **Authority** | The Authority is the 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 |
| **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 |
| **SUPPLIER** | Is inclusive of Contractor, their employees or any sub-contractors used |
| **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 |