
Security Standard - Voice & Video Communications (SS-022)

Chief Security Office

Date: 27/04/2023



This Voice and Video Communications Security Standard is part of a suite of standards, designed to promote consistency across the Department for Work and Pensions (DWP), and supplier base with regards to the implementation and management of security controls. For the purposes of this standard, the term DWP and Department are used interchangeably.

Technical security standards form part of the DWP Digital Blueprint which is a living body of security principles, architectural patterns, code of practice, practices and radars, that aim to support Product Delivery Units (PDUs) and suppliers in delivering the DWP and HMG Digital Strategy. Security standards and policies considered appropriate for public viewing are published here:

<https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards>

Technical security standards cross-refer to each other where needed, so can be confidently used together. They contain both mandatory and advisory elements, described in consistent language (see table below).

Table 1 – Terms

Term	Intention
must	denotes a requirement: a mandatory element.
should	should denotes a recommendation: an advisory element.
may	denotes approval.
might	denotes a possibility.
can	denotes both capability and possibility.
is/are	is/are denotes a description.

1. Contents

1. Contents	3
2. Revision History	4
3. Approval History	5
4. Compliance	6
5. Exceptions Process	6
6. Audience	6
7. Accessibility Statement	6
8. Introduction	7
9. Purpose	8
10. Scope	8
11. Minimum Technical Security Measures	9
11.1 VoIP/Video Communications General Requirements	9
11.2 VoIP/Video Communications H.323and SIP Requirements	11
11.3 General Video Conferencing Requirements	13
11.4 VoIP/Video Conferencing Softphone Requirements	13
11.5 Video Conferencing in Meeting Rooms Requirements	15
11.6 Voice and Video Data Traversal over Untrusted Networks	16
11.7 Service Provider / External Third Party VoIP Security	16
11.8 VoIP Device & Network Physical Controls	17
11.9 VoIP/Video Communications Access Control	18
11.10 VoIP/Video Communications Logging Requirements	19
11.11 Emergency Location	19
12 Appendices	20
Appendix A – Security Outcomes	20
Appendix B Internal References	22
Appendix C External References	23
Appendix D Abbreviations	23
Appendix E Definition of Terms	24
Appendix F Accessibility artefacts	25

2. Revision History

Version	Author	Description	Date
1.0		First published version	04/07/2017
2.0		<p>Full update in line with current best practices and standards;</p> <ul style="list-style-type: none">• Updated Intro, purpose, audience, scope; added reference to CIS v8 security controls• Added NIST CSF references <p>11.1.1 Replaced Secure Chorus with ETSI; added H.264 and WebRTC</p> <p>11.1.3 Demarcation boundary added</p> <p>11.1.6 Registration services, gateways and gatekeepers added</p> <p>11.1.7 & 1.1.8 Entries split from 11.1.6</p> <p>11.1.9 Clarified Authority devices</p> <p>11.1.10 Reference added to Use of Cryptography Security Standard, and physical IP phones</p> <p>11.1.13 Requirement added for protecting unencrypted data</p> <p>11.1.14 Reference added to Network Security Design Security Standard</p> <p>11.2.4 Malformed packet filtering and preventing DDoS attacks</p> <p>11.2.5 Prevention of diverting real time streams, and dual media streaming</p> <p>11.2.6 Should</p> <p>11.3.1 Differentiated between internal and external users. Reference added to Access & Authentication Security Standard</p> <p>11.3.3 Reworded</p> <p>11.3.4 Additional physical protection</p> <p>11.4.1 Within device limitations</p> <p>11.4.3 When in use</p> <p>11.4.4 Where possible</p> <p>11.4.5 & 11.4.7 Requirement clarified for Authority users and devices</p> <p>11.4.9 Clarified Authority staff and its appointed agents only</p> <p>11.5.1 Or other such gateways</p> <p>11.5.5 Disallowed from any domain</p> <p>11.6 Untrusted networks</p> <p>11.7.1 Statement added for security assurance reviews</p> <p>11.7.2 Requirement added for clear terms and conditions regarding data usage in service provider contract</p> <p>11.7.3 Ofcom licencing requirements</p>	27/04/2023

		11.8.2 Added unauthorised recording requirements 11.8.3 Reference added to Physical and Electronic Security Standard 11.8.4 & 11.8.5 Entries moved here from other sections 11.8.6 Added reference to sanitisation and destruction standard 11.9.2 Reference added to Privileged User Access Security Standard 11.9.4 Minimal permissions 11.9.6 Revocation of certificates 11.9.7 Added reference to 802.1x for authentication 11.11.1 Non-office locations	
--	--	--	--

3. Approval History

Version	Name	Role	Date
1.0		Chief Security Officer	04/07/2017
2.0		Chief Security Officer	27/04/2023

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

4. Compliance

Compliance with this standard will be verified through various methods, including but not limited to;

- controls tests performed by first-line teams and by 2nd line activities (e.g. security testing teams)
- security assurance activities to ensure that Architectural Design and delivery are appropriate and aligned to applicable Authority Security Standards. [See Security Assurance Strategy – Ref. O].
- independent external audit

Results of these will be fed back to the appropriate Authority Risk and System Owners.

5. Exceptions Process

In this document the term “**must**” is used in bold letters to indicate a mandatory security measure. Any exceptions to the application of this standard, or where specific security measures cannot be adhered to, **must** be presented to the Authority. This **must** be carried out prior to deployment and managed through the design caveats or exception process.

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

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

6. Audience

This document is intended for, but not necessarily limited to, technical architects, engineers, developers, security teams, project teams, including suppliers engaged in the design, development, implementation and operation of systems, services and applications.

7. Accessibility Statement

Users of this standard **must** consider accessibility design requirements as appropriate. Further information on accessibility standards can be found in Appendix F.

8. Introduction

This Voice and Video Communications Security Standard defines the minimum technical security measures that **must** be implemented for use within the Authority.

Video/voice data is just as important as other data that is protected, and it is likely to prove harder to predict the sensitivity of discussions in advance. Voice and video data in the Authority are subject to a number of key threats. These are summarised here:

- Video/voice calls are placed to or received from an attacker and the user doesn't realise, resulting in compromise of spoken data
- attacker with privileged network access can access all call content and metadata for a user on that network
- attacker compromises a VOIP/Video communications base station, or uses a false base station, and gains access to all call content and metadata for all users on that base station
- An insider could introduce a malicious VoIP/video device into the network and potentially compromise other VoIP/video sessions and even Authority data (e.g. 802.1Q double-tagging to hop VLANs)

As this standard only provides minimum measures, they **should** be exceeded as appropriate depending on the threats and risks that need to be addressed, the sensitivity of the data, and in keeping with latest security enhancements.

The security measures are derived from industry best practice i.e. guidance published by NIST, NCSC, CIS and OWASP (see Appendix C for full list external references) and support the implementation of appropriate security controls as selected by the Authority or our third party providers, such as the CIS Critical Security Controls v8 controls set. [see External References]

Every effort has been made to ensure the security measures are vendor and technology agnostic as far as possible; this is to ensure greater applicability of the standard regardless of the technologies used. The security measures **may** be implemented in different ways, depending on the technology choices and business requirements in question.

The aim of this standard is to:

- ensure security controls that are applicable to voice and video communications are implemented consistently across the Authority and by third party providers where applicable.
- mitigate risks from common threats and vulnerabilities associated with voice and video communications, to an acceptable level for operation.
- support the achievement of security outcomes described in Appendix A.

Technical security standards ultimately support the achievement of security outcomes sought by the Authority. They set the expectations for what needs to be done to achieve them and why, and provide an objective, measurable statement of the Authority's existing security posture in a number of important areas. The outcomes are based on the official NIST sub-categories where possible to ensure close alignment with the NIST Cyber Security Framework (CSF), and are enabled by the implementation of controls from the CIS Critical Security Controls v8 controls set. [see External References]. Those relevant to the subject of each standard can be found in Appendix A of every technical security standard.

9. Purpose

The purpose of this standard is to ensure that Authority systems and services are designed, configured, deployed, and managed consistently to protect against typical threats at the OFFICIAL tier.

This standard is intended to be used;

- When developing/procuring a new voice and/or video communication solution for the Authority
- To assist in providing advice and guidance on secure voice and video communication;
- To provide a baseline in which assurance and compliance activities can be carried out, so that the Authority can be assured that security obligations are being met or exceeded.

10. Scope

This standard applies to all voice and video communications deployments within the Authority and supplier base (contracted third party providers), for the purposes of delivering services that handle Authority data.

For clarity, the two types of real time communications within the scope of this security standard are Voice over IP (VoIP) and secure video communications

The standard applies to the following;

- Voice and Video communication solutions managed by Authority or third party Supplier or other support function for internal Authority use, e.g. video conferencing, person to person video and voice calling
- VoIP and video communications between the Authority and citizens (e.g. work coach interviews), where the call is initiated by the Authority either directly or by invitation – VoIP or video calling initiated by citizens is NOT covered
- Any voice and video communication solutions used to support Authority services and/or data by a third party provider.

Any queries regarding the security measures laid out in this standard **should** be sent to the Authority.

11. Minimum Technical Security Measures

The following section defines the minimum security measures that **must** be implemented to achieve the security outcomes described in Appendix A. For ease of reference, the official NIST sub-category ID is provided against each security measure e.g. PR.PT-3, to indicate which outcome(s) it contributes towards. Refer to Appendix A for full description of outcomes.

11.1 VoIP/Video Communications General Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.1.1	All VoIP/Video Communications must ensure interoperability - Session Initiation Protocol (SIP), the appropriate H.323 or H.264 standard, the European Telecommunication Standards Institute standard or WebRTC are all viable options. For internal communications, a proprietary signalling protocol may be utilised, in conjunction with gateways to interface with other standards.	n/a
11.1.2	Where deemed appropriate and practical, VoIP and Video communication, especially signalling traffic, must be encrypted - if possible utilising VOIP-aware crypto-engine/crypto-scheduler (see SS-007 Use of Cryptography Security Standard [Ref. A]). Where possible, any signalling or control traffic must not be exposed across open public networks	PR.DS-2
11.1.3	Session Border Controllers or other similar assured solutions must be implemented to protect and regulate communication sessions. They must be used at any demarcation boundary and ensure that all traffic i.e. signalling and real time payload traverses said device.	PR.DS-2
11.1.4	There must be consideration to determine the necessity for additional technical countermeasures required such as intrusion detection/prevention system (e.g. network and/or host). (See SS-018 Network Security Design Security Standard [Ref. H]).	PR.PT-4
11.1.5	All softphone (pc & smartphone based VOIP) communications systems must ensure security is in place to protect against malicious software and to restrict access (in line with the SS-015 Malware Protection Security Standard [Ref. B]).	PR.AC-4 DE.CM-4

11.1.6	There must be consideration to determine whether the functionality for registration servers, registration proxies and other such devices providing registration style services to devices are not open to unknown device registration. Consideration must be given to services offered by registration servers, gateways and gatekeepers to ensure that only the minimal service offering is provided.	PR.PT-4
11.1.7	Where possible, specific logical controls must be implemented at the device level, using recognised private static IP addresses for each device, where these are present.	PR.PT-4
11.1.8	Where appropriate, all network segments must be filtered to restrict which devices can connect to the call-processing manager or the voice-mail system.	PR.AC-5 PR.PT-4
11.1.9	All Authority owned/managed VoIP/Video Communications platforms (especially those based on common operating systems such as Windows or Linux) and equipment must be 'hardened' in line with SS-008 Server Operating System Security Standard [Ref. M]. This includes disabling unnecessary features or applications/services, hardening the OS and locking/closing ports. Disable any features on the voice servers and on VoIP equipment that is not in active use.	PR.AC-5 PR.PT-4
11.1.10	Where deemed appropriate and practical, only physical IP phones that can load and process digitally (cryptographically) signed images must be utilised to guarantee the integrity of the software loaded onto the IP phone. Similarly, where deemed appropriate for softphones, the product must be distributed via a cryptographically protected mechanism such that the authenticity of software can be ensured, and must be in line with SS-007 Use of Cryptography Security Standard [Ref. A].	PR.DS-2 PR.DS-6
11.1.11	All relevant VoIP/Video Communications software/hardware (operational, support and administrative) must be maintained with the latest and approved vendor signed patches and current versions in line with SS-033 Security Patching Standard [Ref. C].	PR.MA-1
11.1.12	There must be appropriate knowledge and training in the introduction of new VoIP/Video Communications systems and updated security practices, controls, policies, and architectures.	PR.AT-1

11.1.13	The level of protection for network nodes that have access to unencrypted data must be commensurate with the communications traffic traversing them. A service that encrypts data as it travels through (or resides at) network nodes must be utilised if the appropriate level of protection required for network nodes cannot be reached.	PR.DS-2
11.1.14	Where appropriate, VOIP/Video Communication over IP connectivity must use secure networks that are in accordance with SS-018 Network Security Design Standard [Ref. H].	PR.DS-2

11.2 VoIP/Video Communications H.323and SIP Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.2.1	<p>Voice/Video and data must be on logically separate networks – different subnets with separate RFC 1918 blocks should be used for voice and data traffic, with separate Dynamic Host Configuration Protocol (DHCP) servers for each. Traffic between voice and data network components must be restricted.</p> <p>This requirement does not apply for unified communications, softphone, or similar solutions where this is not possible.</p>	PR.AC-5 PR.PT-4
11.2.2	The call-process manager and IP phones must reside in separate voice segments. The management of the service must be kept separate from the operational service.	PR.AC-5 PR.PT-4
11.2.3	<p>At the interface between the voice gateway and the Public Switched Telephone Network (PSTN), H.323, H.264 SIP, or Media Gateway Control Protocol (MGCP) et al, connections must be disallowed from the data network.</p> <p>This requirement does not apply for unified communications, softphone or similar solutions where this is not possible.</p>	PR.AC-5 PR.PT-4

11.2.4	<p>There must be a suitable Session Border Control which can track and inspect the state of connections, denying packets that are not part of a properly originated call while enabling VoIP traffic flow through the network. The solution must be assessed as secure and suitable for deployment by the Authority.</p> <p>The Session Border Controller at any boundary must filter malformed packets both in the signalling path and the real time path.</p> <p>The Session Border Controller used at any point in the network must be configured to prevent attempts at a DDoS style attack e.g. registration storms.</p>	PR.PT-4 DE.CM-4
11.2.5	<p>There must be consideration to determine the necessity of signalling traffic being encrypted to prevent eavesdropping and reconnaissance during call establishment.</p> <p>There must also be consideration to prevent signalling traffic being manipulated to prevent diversion of real time streams.</p> <p>Consideration should be given to prevent dual media streaming unless there is a specific need e.g. simring, voice recording.</p>	PR.DS-2
11.2.6	<p>Where determined necessary and practicable, VoIP communication should use IPsec ESP tunnelling at the IP level or the packets must be encrypted at the application level with SRTP/SRTCP, the secure real-time transport protocol (RFC 3711) using a suitable cryptography method in compliance with SS-007 Use of Cryptography Security Standard [Ref. A].</p>	PR.DS-2

11.3 General Video Conferencing Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.3.1	All users who use the facility must use authentication commensurate with the sensitivity requirements of the call. Internal Authority users must be authenticated in line with SS-001 Access and Authentication Security Standard pt1 [Ref. D].	PR.AC-7
11.3.2	The security limitations of the session must be communicated in line with the security operating procedures e.g., display appropriate warning notices and the highest Security Classification or information sensitivity that may be discussed, at the start of the session.	PR.AT-1
11.3.3	Relevant equipment must be prominently labelled with the maximum information sensitivity or Security Classification that is permitted and in alignment with the Authority Security Classification Scheme and Authority Information Management Policy.	ID.AM-1 ID.AM-5
11.3.4	Video Conferencing configuration controls must be assessed for inclusion under the SS-012 Protective Monitoring Security Standard [Ref. E] in order to detect any unauthorised or unusual use. Where a specific video conferencing room is not used, consideration must be given to protection of other items that may be in view e.g. other citizens, Authority colleagues, notice boards, and other such items.	DE.AE-3 DE.CM-2

11.4 VoIP/Video Conferencing Softphone Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.4.1	Any managed endpoint client device which has been added with the functionality to be used as a softphone must have been hardened according to the relevant security standard (see SS-010 Desktop Operating System Security Standard [Ref. F] or SS-017 Mobile Device Security Standard [Ref. G]), or within the limitations of that device.	PR.DS-2 PR.DS-5

11.4.2	The softphone must not have the capability to bypass existing network security controls. Where this is not practicable to implement, there must be parallel security controls (as applicable) put in place for the softphone 'traffic' as informed by a risk assessment.	PR.DS-2 PR.DS-5
11.4.3	When in use, if the softphone is being used to make calls to a client who does not support encryption and/or authentication then these calls must either be disallowed, or the user must be (made) aware of this prior to the call. This requirement does not apply to PSTN calls, where standard business procedures will be applied.	PR.DS-5
11.4.4	Connections/calls must be authenticated at both/all ends where this feature is supported. Use credentials secured by hardware or Multi-Factor Authentication (MFA) for all identities where possible, although this is not required for conference rooms or group accounts. Unauthorised connections or authentication requests to the softphone 'environment' must be disallowed or blocked.	PR.AC-7
11.4.5	The softphone must be pre-configured on all Authority managed endpoint client devices to use only the minimum services required for the connection, disabling unnecessary services, features and functionality that may pose unnecessary security risks. Authority standard users must not be able to change these softphone settings.	PR.DS-2 PR.DS-5
11.4.6	If the softphone has instant messaging and file sharing functionality, then there must be filtering and security controls in place to avoid forbidden/malicious content being shared between clients.	DE.CM-4
11.4.7	A client software version management policy must be used to monitor and manage software versions on Authority managed endpoint clients.	ID.AM-2
11.4.8	There must be access controls in place on Authority managed endpoints so Authority users can only use features/functionality which they are authorised to use for a legitimate business purpose.	PR.AC-4
11.4.9	Only authorised Authority staff or its appointed agents must be able to view the directories or be able to initiate or receive communications via the softphone, and then only within the scope of their authorised role.	PR.AC-4

11.4.10	Where applicable, the 'softphone' solution must be subject to regular penetration tests (at least annually). Any detected vulnerabilities must be fixed by patching applications, OS and devices or by using secure configurations and hardening devices.	DE.CM-4 RS.AN-5
---------	---	--------------------

11.5 Video Conferencing in Meeting Rooms Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.5.1	Where applicable, the network configuration must disallow the Multipoint Control Unit (MCU) to act as a bypass for the Session Border Controllers or other such gateways. Ensure that the protective controls afforded to the MCU reflect the highest sensitivity of the conferences it hosts.	PR.DS-2
11.5.2	<p>The corporate lockdown policy must be applied; this is especially important in situations where the video conferencing equipment is part of a feature-rich suite. If a facility is not needed, then remove or disable it. For example:</p> <ul style="list-style-type: none"> • Auto-answer features – if this feature cannot be removed configure the system to answer with the audio muted • Execution of script/URL/file-based commands • Scripting and extended media content embedded in web pages • Cookies • Auto-update of the media player • Automatic codec downloads • Automatic acquisition of DRM rights data for DRM content • Broadcast streaming • Far end camera controls • Wireless capability 	PR.PT-3
11.5.3	Communications links must be protected. Often this will involve cryptographic protection of the links (see SS-007 Use of Cryptography Security Standard [Ref. A]) and is not trivial and therefore must be subject to a risk assessment if required.	PR.DS-2

11.5.4	In shared video conferencing meeting rooms, privileged user configuration changes (i.e. for administrative changes only) must be strictly controlled i.e. access to the VC facility configuration functions must be controlled via authorised management interfaces.	PR.AC-4
11.5.5	The remote control of video conferencing equipment from any domain, trusted or untrusted must be disallowed, except in the case of remote support or troubleshooting.	PR.AC-3
11.5.6	Community access to call directories must be strictly controlled and use a booking service that is auditable.	PR.AC-4

11.6 Voice and Video Data Traversal over Untrusted Networks

Reference	Minimum Technical Security Measures	NIST ID
11.6.1	There must be a Session Border Control solution (or other similar solution) between the Authority IP network and the PSTN, and other untrusted networks that access the telephony/video conferencing infrastructure.	PR.DS-2
11.6.2	Data traversal over network boundaries must also adhere to the relevant requirements in SS-006 Security Boundaries Standard [Ref. I].	PR.DS-2

11.7 Service Provider / External Third Party VoIP Security

Reference	Minimum Technical Security Measures	NIST ID
11.7.1	Connectivity of VoIP technologies to service providers or third parties for management purposes must be sufficiently protected. The Authority will require assurance from the service provider or third party that the associated risks are adequately managed in line with commercial agreements, and can be subject to independent security assurance reviews.	ID.SC-3 ID.SC-4
11.7.2	The terms and conditions for the communications service must be explicit and clear, outlining the content and metadata that will be collected, processed, and for what purpose.	ID.SC-3
11.7.3	Where services are obtained from a 3 rd party for PSTN style access, the Communication Provider (CP) must be a Licensed Operator, licenced by the relevant Licencing Authority, e.g. OfCom. This applies to circuits, call routing and transmission services, interconnects, Intelligent Networks etc.	ID.SC-2

11.8 VoIP Device & Network Physical Controls

Reference	Minimum Technical Security Measures	NIST ID
11.8.1	The VoIP 'base station' and 'handset' procured must have hardening such that minimal logical and programmable functions are available.	PR.PT-3
11.8.2	<p>A physical disconnection function must be available, so that when the handset is placed on the base unit there is no possibility of any remote eavesdropping. If the base unit contains remote microphone/speaker functionality, there must be a physical call disconnection capability.</p> <p>Where a softphone is in use i.e. any software phone installed on a physical device e.g. Smartphone, PC etc. consideration must be given protect the softphone from unauthorised recording or audio redirection</p>	PR.DS-5
11.8.3	There must be adequate physical security in place to restrict access to VOIP/Video Communications network components. They must be adequately locked and secured – and accessible only by authorised personnel. This must be in accordance with the minimum protection standards for physical security outlined in the Physical and Electronic Security Standard [Ref. K].	PR.AC-2
11.8.4	There must be effective physical countermeasures in place to mitigate risks such as insertion of sniffers or other network monitoring devices.	PR.AC-2
11.8.5	Secure procedures must be in place for the repair and servicing of handsets in sensitive working areas. E.g. The use of escorted or sufficiently cleared service engineers.	PR.AC-2 PR.MA-1
11.8.6	Physical handsets must be disposed of in line with the requirements contained in SS-036 Secure Sanitisation and Destruction [Ref. N].	PR.AC-2

11.9 VoIP/Video Communications Access Control

Reference	Minimum Technical Security Measures	NIST ID
11.9.1	Where there is user authentication and login phones/devices, all default passwords must be changed and set in accordance with Authority User Access Control Policy.	PR.AC-1 PR.AC-6
11.9.2	Administrative privileges and permissions must be set according to user needs with appropriate privilege separation and must be reviewed at regular intervals, at least every 12 months. Access to management functions must be restricted to authorised users and must be in line with the SS-001-2 Privileged User Access Security Standard [Ref. L].	PR.AC-4
11.9.3	Unattended phones/devices in insecure/high-risk areas must be logged out.	PR.DS-5
11.9.4	The IP telephony system must have a feature to allow telephony permissions, call permissions and voice mail permissions to be controlled by administrators. When such services are in use, such permissions must be allowed on a minimal compliance basis only.	PR.AC-4
11.9.5	Only assured versions of Internet Protocol Security (IPsec), Secure Shell (SSH) or Hyper-Text Transfer Protocol over Transport Layer Security (HTTPs) must be used to protect all remote management and auditing access. SSH must ONLY be used for issuing remote admin commands, and not for any actual transfer of data. If practical, and where appropriate, avoid using remote management at all and do IP Private Branch Exchange (PBX) access from a physically secure system. Remote administration must be carried out in accordance with SS-016 Remote Access Security Standard [Ref. J].	PR.DS-2 PR.MA-2
11.9.6	There must be a facility for enterprise revocation of user credentials and/or access to the call process manager to be prevented from a lost, stolen, or compromised device. There must be a facility for enterprise revocation of any certificates used as part of any authentication process.	PR.AC-1
11.9.7	Authentication and access control must be in accordance with SS-001 pt.1 Access and Authentication Security Standard [Ref. D] for all relevant VOIP/Video Communications systems [Ref. D]. Where possible, any device e.g. PC softphone, physical IP phone should be authenticated onto the Authority network by a network authentication mechanism e.g. 802.1x	PR.AC-1

11.10 VoIP/Video Communications Logging Requirements

Reference	Minimum Technical Security Measures	NIST ID
11.10.1	Call control logging on the call-processing manager/ IP PBX must be enabled in accordance with the SS-012 Protective Monitoring Security Standard [Ref. E].	DE.AE-3
11.10.2	All VoIP/Video Communications systems must be configured to receive accurate time from an appropriate time source, in compliance with SS-012 Protective Monitoring Security Standard [Ref. E].	DE.AE-3

11.11 Emergency Location

Reference	Minimum Technical Security Measures	NIST ID
11.11.1	Where possible, the IP telephony must be configured in such a way that when a 999/112/101/111 call is made from a site, the Calling Line Identity/Identification (CLI) presented to the emergency operator is representative of the site originating the call. In addition, a VoIP flag may be used to alert an operator to ask for a location. When that device is used in a homeworker, “mobile” or remote location consideration must be given for alternative access to 999/112/101/111	n/a

12 Appendices

Appendix A – Security Outcomes

The minimum security measures defined in this standard contribute to the achievement of security outcomes described in the table below. For consistency, the official NIST Sub-category IDs have been carried through to the standards.

Table 1 – List of Security Outcomes Mapping

NIST Ref	Security Outcome (sub-category)	Related Security measure
ID.AM-1	Physical devices and systems within the organization are inventoried	11.3.3
ID.AM-2	Software platforms and applications within the organization are inventoried	11.4.7
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	11.3.3
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	11.7.3
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	11.7.1, 11.7.2
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	11.7.1
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	11.9.1, 11.9.6, 11.9.7

PR.AC-2	Physical access to assets is managed and protected	11.8.3, 11.8.4, 11.8.5, 11.8.6
PR.AC-3	Remote access is managed	11.5.5
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	11.1.5, 11.4.8, 11.4.9, 11.5.4, 11.5.6, 11.9.2, 11.9.4
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	11.1.8, 11.1.9, 11.2.1, 11.2.2, 11.2.3,
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	11.9.1
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	11.3.1, 11.4.4
PR.AT-1	All users are informed and trained	11.1.12, 11.3.2
PR.DS-2	Data-in-transit is protected	11.1.2, 11.1.3, 11.1.10, 11.1.13, 11.1.14, 11.2.5, 11.2.6, 11.4.1, 11.4.2, 11.4.3, 11.4.5, 11.5.1, 11.5.3, 11.6.1, 11.6.2, 11.9.5
PR.DS-5	Protections against data leaks are implemented	11.4.1, 11.4.2, 11.4.5, 11.8.2, 11.9.3
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	11.1.10
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	11.1.11, 11.8.5, 11.9.5
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	11.5.2, 11.8.1

PR.PT-4	Communications and control networks are protected	11.1.4, 11.1.6, 11.1.7, 11.1.8, 11.1.9, 11.2.1, 11.2.2, 11.2.3, 11.2.4
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	11.3.4, 11.10.1, 11.10.2
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	11.3.4
DE.CM-4	Malicious code is detected	11.1.5, 11.2.4, 11.4.6, 11.4.10
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	11.4.10

Appendix B Internal References

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

Table 2 – Internal References

Ref	Document	Publicly Available*
A	SS-007 Use of Cryptography Security Standard	Yes
B	SS-015 Malware Protection Security Standard	Yes
C	SS-033 Security Patching Security Standard	Yes
D	SS-001 Access and Authentication Security Standard pt1.	Yes
E	SS-012 Protective Monitoring Standard	Yes
F	SS-010 Desktop Operating System Security Standard	Yes
G	SS-017 Mobile Device Security Standard	Yes
H	SS-018 Network Security Design Standard	Yes
I	SS-006 Security Boundaries standard	Yes
J	SS-016 Remote Access Security Standard	Yes
K	Physical and Electronic Security Standard	No
L	SS-001-2 Privileged User Access Security Standard	Yes
M	SS-008 Server Operating System Security Standard	Yes
N	SS-036 Secure Sanitisation and Destruction	Yes
O	Security Assurance Strategy	No

Requests to access non-publicly available documents **should be made to the Authority.*

Appendix C External References

The following publications and guidance were considered in the development of this standard and **should** be referred to for further guidance.

Table 3 – External References

External Documents List
CIS Critical Security Controls v8 controls set
NCSC Guidance on Secure Voice at Official CESG Good Practice Guide No.21: Video Conferencing, Issue No: 1.1, February 2014
CESG Architectural Pattern No.6, Voice Communications between Security Domains, Issue No.1, February 2013
CESG Information Assurance Notice 2013/05: Adoption of VoIP Technologies in Sensitive Working Environments
NIST Special Publication 800-58: Security Considerations for Voice over IP Systems
CISCO SAFE White Paper: IP Telephone Security in Depth
Cisco Video and TelePresence Architecture Design Guide – Security for Video Communications

Appendix D Abbreviations

Table 4 – Abbreviations

Abbreviation	Definition
PDU	Product Delivery Units
DDA	Digital Design Authority
DHCP	Dynamic Host Configuration Protocol
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
IP	Internet Protocol
IP-PBX	Internet Protocol Private Branch Exchange
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
MGCP	Media Gateway Control Protocol
PSTN	Public Switched Telephone Network
RTP	Real-time Transport Protocol
RTCP	Real-time Transport Control Protocol
SIP	Session Initiation Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VoIP	Voice-over Internet Protocol

Appendix E Definition of Terms

Table 5 – Glossary

Term	Definition
Call-process manager	Provides call setup/establishment and customizable user-based configurations; also known as "IP PBX." This system is the server that provides call control and configuration management for IP telephony devices in the network. It provides bootstrap information for IP telephony devices, call setup, and call routing throughout the network to other voice-enabled devices such as voice gateways and voice-mail systems.
Firewall (Stateful)	Stateful packet-filtering device that maintains state tables for IP-based protocols. Traffic is allowed to cross the firewall only if it conforms to the access-control filters defined, or if it is part of an already established session in the state table.
Host Intrusion Detection/Prevention System	Host intrusion detection system is a software application that monitors activity on an individual host. Monitoring techniques can include validating operating system and application calls, checking log files, file system information, and network connections. Host intrusion detection systems protect servers and databases against buffer overflow attacks and other malicious activity. A prevention system proactively blocks attacks as they occur
Multipoint Control Unit (MCU)	To support a multi-party Video Conferencing service. A MCU is sometimes referred to as a video bridge. The MCU receives the video stream from each endpoint, combining them into a single screen image.
Network Intrusion Detection/Prevention System	Typically used in a nondisruptive manner, Network intrusion detection system captures traffic on a LAN segment and tries to match the real-time traffic against known attack signatures. Signatures range from atomic (single packet and direction) signatures to composite (multipacket) signatures requiring state tables and Layer 7 application tracking. A prevention system proactively blocks attacks as they occur.
Session Border Control	A Session Border Controller is a device used in select VoIP networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down calls. The SBC enforces security, quality of service and admission control mechanism over the VoIP sessions.
Softphone	Any application that has the ability to reside on a user system (for example, desktop) and place calls to other IP telephony systems over the IP network.

Voice gateway	This is a generic term that refers to any gateway that provides voice services, such as IP packet routing, backup call processing, Public Switched Telephone Network (PSTN) access, and other voice services. This device is the interface between the legacy voice systems that can provide backup for the IP telephony network in case of failure. This device is typically not a full-featured call-processing manager; it supports a subset of the call-processing functionality provided by the call-processing manager.
Voice-mail system	This system primarily provides IP-based voice-mail storage services. In addition, it can provide user directory lookup capabilities and call-forwarding features.
VoIP	Voice over Internet Protocol (also called IP telephony), is a method and group of technologies for the delivery of voice communications over Internet Protocol (IP) networks, such as the internet, rather than via the public switched telephone network (PSTN).

Appendix F Accessibility artefacts

A variety of accessibility guidance is available from the below URL, that includes:

<https://www.gov.uk/guidance/guidance-and-tools-for-digital-accessibility>

<https://www.gov.uk/guidance/accessibility-requirements-for-public-sector-websites-and-apps>