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

Chief Security Office

Date: 04/07/2017

Department for Work & Pensions

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

Version Control Table

Version	Date	Major Change

Updating policy

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

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

Contents

1. Introduction

1.1. This Voice and Video Communications Security Standard provides the list of controls that are required to secure voice and video communication implementations to a Department for Work and Pensions (DWP) approved level of security. This standard provides a list of security controls to protect citizen and operational data. It is to minimise the risk from known threats both physical and logical to an acceptable level for operations

1.2. 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 DWP 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 Departmental data (e.g. 802.1Q double-tagging to hop VLANs)

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

4.4. Furthermore the security controls presented in this standard are taken from examples of international best practice for voice and video communications security and have been tailored for Departmental suitability.

2. Purpose

2.1. The purpose of this document is to enable teams to work to a defined set of security requirements which enable solutions to be developed, deployed and managed to Departmental security standards, which are based upon international best practice for voice and video communication deployments.

2.2. This standard is intended to have three uses:

- To be used when developing/procuring a new voice and/or video communication solution for DWP
- To be used to assist in providing advice and guidance on secure voice and video communication;
- To provide a means to conduct compliance based technical security audits.

3. Exceptions

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

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

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

4. Audience

4.1. This standard is intended for Security/Technical Architects, Product Development Units (PDU), Hosting Teams, Suppliers, DWP Software delivery projects or External Software delivery projects (developing/delivering voice & video communications (based) solutions), security groups and also IT staff such as Security Compliance Teams involved in securing environments for DWP systems and applications

5. Scope

5.1. This standard is to cover systems handling data within the OFFICIAL tier of the Government Security Classification Policy (GSCP). All of the organisation's voice and video communications falling within this category will be subject to the requirements specified within this security standard. The requirements will be applied to new and existing installations.

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

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

5.4. The standard applies to the following;

- Voice and Video communication solutions' managed by DWP or Third Party Supplier or other support function for internal DWP use.
- Any voice and video communication solutions used to support DWP services and/or data by a third party provider.

5.5. In the In the event of uncertainty on the controls laid out in this standard please contact the Security Advice Centre for guidance and support on items which require clarification or as a pointer for other more technical support.

6. Security Controls Assurance

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

7. Security Requirements

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

10.1. VoIP/Video Communications General Requirements

Reference	Security Control Requirement
10.1.1	All VoIP/Video Communications MUST ensure interoperability - Session Initiation Protocol (SIP), the latest H.323 standard or the Secure Chorus standard are all viable options.
10.1.2	Where deemed appropriate and practical, VoIP and Video communication (including signalling traffic) MUST be encrypted - if possible utilising VOIP-aware crypto-engine/crypto-scheduler (see SS-07 Security Standard – Use of Cryptography).
10.1.3	Session Border Controller or other similar assured solutions MUST be used to filter VoIP traffic on the network
10.1.4	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).
10.1.5	All relevant VOIP/Video communications systems MUST ensure security is in place to protect against malicious software and to restrict access (in line with the Security Standard - Malware Protection). Especially “Softphone” (pc based VOIP) MUST be adequately protected.
10.1.6	There MUST be consideration to determine whether the functionality for call-processing managers to provide an automatic phone registration feature should be turned off. There should be specific logical controls at the device level. Where possible, use recognised private static IP addresses for each device. Additionally, where appropriate, all network segments should be filtered to restrict which devices can connect to the call-processing manager or the voice-mail system.
10.1.7	All VoIP/Video Communications platform (especially those based on common operating systems such as Windows or Linux) and equipment MUST be ‘hardened’. 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.
10.1.8	Where deemed appropriate and practical, only 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.

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

Reference	Security Control Requirement
10.1.9	ALL relevant VoIP/Video Communications software/hardware (operational, support and administrative) MUST be maintained with the latest approved patches and current versions in line with DWP Patching Policy.
10.1.10	There MUST be appropriate knowledge and training in the introduction of new VOIP/Video Communications systems and updated security practices, controls, policies, and architectures.

10.2. VoIP/Video communications H.323 and SIP Requirements

Reference	Security Control Requirement
10.2.1	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 should be restricted. This requirement does not apply for unified communications, softphone or similar solutions where this is not possible.
10.2.2	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.
10.2.3	At the voice gateway, which interfaces with the Public Switched Telephone Network (PSTN), H.323, SIP, or Media Gateway Control Protocol (MGCP) connections MUST be disallowed from the data network. This requirement does not apply for unified communications, softphone or similar solutions where this is not possible.
10.2.4	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 DWP Security Architecture.
10.2.5	There MUST be consideration to determine the necessity of signalling traffic being encrypted to prevent eavesdropping and reconnaissance during call establishment.
10.2.6	Where determined necessary and practicable, VoIP communication MUST use IPsec 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 3771) using a suitable cryptography method in compliance with SS-07 Security Standard – Use of Cryptography.

10.3. General Video Conferencing Requirements

Reference	Security Control Requirement
10.3.1	A security policy MUST be produced/exist on the use of the Video Conferencing facilities. The policy should include, but is not limited to, the authentication of users who are allowed to use the facility, the type and (maximum) sensitivity of information that can be discussed, times when an endpoint can place or receive calls and sites to which Video Conferencing is permitted or forbidden.
10.3.2	The security limitations of the session MUST be communicated in line with the security operating procedures and the overarching security policy, e.g., display

Reference	Security Control Requirement
	appropriate warning notices and the highest Protective Marking or information sensitivity that may be discussed, at the start of the session. Consider producing an “acceptable use policy” that users have to read and sign up to. Label relevant equipment prominently with the maximum information sensitivity or Protective Marking that is permitted.
10.3.3	Video Conferencing configuration controls MUST be assessed for inclusion under the corporate protective monitoring policy in order to detect any unauthorised or unusual use; advice is in Security Standard - Protective Monitoring.

10.4. VOIP/Video Conferencing Softphone Requirements

Reference	Security Control Requirement
10.4.1	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 or SS-017 Mobile Device Security Standard).
10.4.2	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 risk assessment.
10.4.3	Where higher (sensitivity) requirements exist, 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.
10.4.4	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.
10.4.5	Unauthorised connections or authentication requests to the softphone ‘environment’ MUST be disallowed or blocked.
10.4.6	The softphone MUST be pre-configured on all endpoint client devices to disable unnecessary services, features and functionality that may pose unnecessary security risks. The user must not be able to change these settings.
10.4.7	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.
10.4.8	A client software version management policy MUST be used by to monitor and manage software versions on endpoint clients.

10.4.9	There MUST be access control in place so users can only use features/functionality which they are authorised to use for a legitimate business purpose.
10.4.10	Only authorised parties MUST be able to view the directories or be able to initiate communication via the softphone.
10.4.11	Where applicable, the 'softphone' solution should be subject to regular penetration tests (at least once annually). Any detected vulnerabilities must be fixed by patching applications, OS and devices or by using secure configurations and hardening devices.

10.5. Video Conferencing in Meeting Rooms Requirements

Reference	Security Control Requirement
10.5.1	Where applicable, the network configuration MUST disallow the Multipoint Control Unit (MCU) to act as a bypass for the Session Border Controllers. Ensure that the protective controls afforded to the MCU reflect the highest sensitivity of the conferences it hosts.
10.5.2	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: • 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
10.5.3	Communications links MUST be protected. Often this will involve cryptographic protection of the links (see SS-07 Security Standard – Use of Cryptography) and is not trivial and therefore MUST be subject to risk assessment if required.
10.5.4	Video Conferencing devices, when not in use, MUST be located away from any area in which sensitive matters are often discussed or displayed.
10.5.5	Cameras and microphones MUST be disabled when not in use, as far as practicable.
10.5.6	In shared Video Conferencing meeting rooms, privileged user configuration changes MUST be strictly controlled., i.e. access to the VC facility configuration functions MUST be controlled via authorised management interfaces,.
10.5.7	The remote control of Video Conferencing equipment from a less trusted domain MUST be disallowed.

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

Reference	Security Control Requirement
10.5.8	Community access to call directories MUST be strictly controlled and use a booking service that is auditable.

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

10.6. VOIP/Video Communication over IP connectivity

Reference	Security Control Requirement
10.6.1	VOIP/Video Communication over IP connectivity MUST use secure networks which are in accordance with SS-018 Network Security Design Standard.

10.7. Voice and Video Data Traversal over Less Trusted Networks

Reference	Security Control Requirement
10.7.1	Where deemed appropriate, there MUST be a Session Border Control solution (or other similar solution) between the DWP IP network and ISDN (PSTN) and other less trusted networks that access the telephony/video conferencing infrastructure.
10.7.2	Data traversal over network boundaries MUST also adhere to the relevant requirements in SS-006 Secure Boundaries standard.

10.8. VOIP Supply Chain Security

Reference	Security Control Requirement
10.8.1	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.
10.8.2	Connectivity of VoIP technologies to service providers or third parties for management purposes MUST be sufficiently protected or avoided altogether. Where this is absolutely necessary, organisations will require assurance from the service provider or third party that the associated risks are adequately managed.

10.9. VOIP Device Physical Controls

Reference	Security Control Requirement
10.9.1	The VoIP 'base station' and 'handset' procured MUST have hardening such that minimal logical and programmable functions are available.
10.9.2	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, this should be disabled.

10.10. VOIP/Video Communications Access Control

Reference	Security Control Requirement
10.10.1	Where there is user authentication and login phones/devices, all default passwords MUST be changed and set in accordance with DWP User Access Control Policy.
10.10.2	Administrative privileges and permissions MUST be set according to user needs with appropriate privilege separation and must be reviewed at regular intervals. Access to management functions should be restricted to authorised users.
10.10.3	There MUST be adequate physical security in place to restrict access to VOIP/Video Communications network components. They must be adequately

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

Reference	Security Control Requirement
	locked and secured – and accessible only by authorized personnel. This MUST be in accordance with the minimum protection standards for physical security outlined in Security Standard – Network Security Design.
10.10.4	Unattended phones/devices in insecure/high-risk areas MUST be logged out.
10.10.5	The IP telephony system MUST have a feature to allow telephony permissions, call permissions and voice mail permissions to be controlled by administrators.
10.10.6	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, 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 the Security Standard - Remote Access.
10.10.7	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.
10.10.8	There MUST be proper physical countermeasures in place to mitigate risks such as insertion of sniffers or other network monitoring devices.
10.10.9	Authentication and access control must be in accordance with the appropriate controls in SS-001 Access and Authentication for all relevant VOIP/Video Communications systems

10.11. VOIP/Video Communications Logging Requirements

Reference	Security Control Requirement
10.11.1	Call control logging on the call-processing manager/ IP PBX MUST be enabled in accordance with the Protective Monitoring Standard.
10.11.2	All VoIP/Video Communications systems MUST be configured to receive accurate time from an appropriate time source, in compliance with Security Standard - Protective Monitoring.

10.12. Emergency Location

Reference	Security Control Requirement
10.12.1	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.

8. Compliance

Compliance with this standard MUST occur as follows:

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

9. Accessibility

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

10. Security Standards Reference List

Document Name	Location	Version
Exceptions Process		
Security Standards Master List		

11. Reference Documents

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

12. Definition of Terms

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.

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

Term	Definition
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.

13. Glossary

Abbreviation	Definition
DA	Design Authority
DHCP	Dynamic Host Configuration Protocol
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

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

Abbreviation	Definition
TLS	Transport Layer Security
VoIP	Voice-over Internet Protocol

14. Controls Catalogue Mapping

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

SS-022 Voice and Video Communications STANDARD	**DWP Controls Catalogue - Baseline Control Set**	
Control Statement	**Control Reference**	**Descriptor**
10.1.1	CY09	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.
10.1.2	CY06	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
10.1.3	NT02	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.
10.1.4		
10.1.5	MW01	Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.
10.1.6		
10.1.7		
10.1.8		
10.1.9		

SS-022 Voice and Video Communications STANDARD	**DWP Controls Catalogue - Baseline Control Set**	
10.1.10	HR01	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
10.2.1	NT08	Groups of information services, users and information systems shall be segregated on networks.
10.2.2		
10.2.3		
10.2.4		
10.2.5		
10.2.6		
10.3.1		
10.3.2		
10.3.3		
10.4.1		
10.4.2		
10.4.3		
10.4.4		
10.4.5		
10.4.6		
10.4.7		
10.4.8		
10.4.9		
10.4.10		
10.4.11		
10.5.1		
10.5.2		
10.5.3		
10.5.4		

SS-022 Voice and Video Communications STANDARD	**DWP Controls Catalogue - Baseline Control Set**	
10.5.5		
10.5.6		
10.5.7		
10.5.8		
10.6.1	NT03 NT04	Networks shall be managed and controlled to protect information in systems and applications. Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defence-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.
10.7.1		
10.7.2		
10.8.1		
10.8.2		
10.9.1		
10.9.2		
10.10.1	AC19 AC20	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure. Password management systems shall be interactive and shall ensure quality passwords.
10.10.2	AC02 AC14	Users should only be provided with access to the network and network services that they have specifically been authorised to use. Asset owners shall review users' access rights at regular intervals.
10.10.3	PH02	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

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

SS-022 Voice and Video Communications STANDARD	**DWP Controls Catalogue - Baseline Control Set**	
10.10.4	PH16	Users shall ensure that unattended equipment has appropriate protection.
10.10.5	AC08	The allocation and use of privileged access rights shall be restricted and controlled.
10.10.6		
10.10.7	AC04	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.
10.10.8		
10.10.9		
10.11.1	EV01	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.
10.11.2	EV07	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source. A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.
10.12.1		