Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

SEPTEMBER 2019

Guidelines for Communications Systems

Telephone systems

Telephone systems usage policy

All non-secure telephone systems are subject to interception. Accidentally or maliciously revealing sensitive or classified information over a public telephone network can lead to the compromise of such information.

Security Control: 1078; Revision: 2; Updated: Aug-19; Applicability: O, P, S, TS; Priority: Must
A telephone systems usage policy is developed and implemented.

Personnel awareness

As there is a potential for unintended disclosure of information when using telephone systems, it is important that personnel are made aware of what they can discuss on particular telephone systems, as well as security risks associated with the use of non-secure telephone systems in sensitive or classified areas.

Security Control: 0229; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Personnel are advised of the permitted sensitivity or classification of information that can be discussed over both internal and external telephone systems.

Security Control: 0230; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.

Visual indication

When single telephone systems are approved to hold conversations at different levels, alerting the user to the sensitivity or classification of information that can be discussed will assist in reducing the likelihood of unintended disclosure of information.

Security Control: 0231; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
When permitting different levels of conversation for different kinds of connections, telephone systems give a visual indication of what kind of connection has been made.

Protecting conversations

When sensitive or classified conversations are to be held using telephone systems, the conversation needs to be appropriately protected through the use of encryption.

Security Control: 0232; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.

Cordless telephone systems

Cordless telephone systems have minimal transmission security and are susceptible to interception. Using cordless telephone systems can result in disclosure of information to an unauthorised party through interception.

Security Control: 0233; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Cordless telephone systems are not used for sensitive or classified conversations.

Speakerphones

As speakerphones are designed to pick up and transmit conversations in the vicinity of the device, using speakerphones in TOP SECRET areas presents a number of security risks. However, if an organisation is able to reduce security risks through the use of an audio secure room that is secured during conversations, then they may be used.

Security Control: 0235; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Speakerphones are not used on telephone systems in TOP SECRET areas unless the telephone system is located in a room rated as audio secure, the room is audio secure during conversations and only personnel involved in discussions are present in the room.

Off-hook audio protection

Providing off-hook security minimises the chance of background conversations being accidentally coupled into handsets and speakerphones. Limiting the time an active microphone is open minimises this security risk.

Security Control: 0236; Revision: 4; Updated: Sep-18; Applicability: O, P; Priority: Should
In PROTECTED areas, off-hook audio protection features are used on all telephones that are not authorised for the transmission of PROTECTED information.

Security Control: 0931; Revision: 4; Updated: Sep-18; Applicability: O, P, S; Priority: Should
In SECRET areas, push-to-talk handsets are used on all telephones that are not authorised for the transmission of SECRET information.

Security Control: 0237; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
In TOP SECRET areas, push-to-talk handsets are used on all telephones that are not authorised for the transmission of TOP SECRET information.

Further information

Further information on Internet Protocol (IP) telephony can be found in the video conferencing and Internet Protocol telephony section of these guidelines.

Further information on mobile phones can be found in the ***Guidelines for Enterprise Mobility***.

Further information on encryption can be found in the ***Guidelines for Using Cryptography***.

Video conferencing and Internet Protocol telephony

Video and voice-aware firewall requirement

Where a video conferencing or IP telephony network is connected to another video conferencing or IP telephony network belonging to a different security domain the gateways section of the ***Guidelines for Gateway Management*** applies.

Where an analog telephone network, such as the Public Switched Telephone Network (PSTN), is connected to a data network the gateways section of the ***Guidelines for Gateway Management*** does not apply.

Hardening video conferencing and Internet Protocol telephony infrastructure

Video conferencing and IP telephony traffic in a data network consists of IP packets and should be treated the same as any other data. As such, hardening can be applied to video conferencing units, handsets, software, servers, firewalls and gateways. For example, additional security could be added by using a Session Initiation Protocol (SIP) server that:

- has a fully patched operating system
- has fully patched software
- runs only required services
- uses encrypted non-replayable authentication
- applies network restrictions that only allow secure SIP traffic and secure Real-time Transport Protocol (RTP) traffic from video conferencing units and IP phones on a Virtual Local Area Network (VLAN) to reach the server.

Video and voice-aware firewalls

The use of video and voice-aware firewalls ensures that only video and voice traffic (e.g. signalling and data traffic) is allowed for a given call and that the session state is maintained throughout the transaction.

The requirement to use a video or voice-aware firewall does not necessarily require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. If possible, organisations are encouraged to implement one firewall that is video and data-aware; voice and data-aware; or video, voice and data-aware depending on their needs.

Security Control: 0546; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Where a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video or voice-aware firewall is used.

Protecting video conferencing and Internet Protocol telephony traffic

Video conferencing and IP telephony traffic is vulnerable to eavesdropping but can be protected with encryption. When encrypting video conferencing and IP telephony traffic, voice control signalling can be protected using Transport Layer Security and the 'sips://' identifier to force the encryption of all legs of the connection. Similar protections are available for RTP and the Real-time Control Protocol.

Security Control: 0547; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Video conferencing and IP telephony signalling and data is encrypted.

Establishment of secure signalling and data protocols

Use of secure signalling and data protocols protect against eavesdropping, some types of denial of service, person-in-the-middle attacks and call spoofing attacks.

Security Control: 0548; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Video conferencing and IP telephony functions are established using secure signalling and data protocols.

Video conferencing unit and Internet Protocol phone authentication

Blocking unauthorised or unauthenticated devices by default will reduce the likelihood of unauthorised access to a video conferencing or IP telephony network.

Security Control: 0554; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.

Security Control: 0553; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.

Security Control: 0555; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Authentication and authorisation is used for all actions on a IP telephony network, including registering a new IP phone, changing phone users, changing settings and accessing voicemail.

Security Control: 0551; Revision: 5; Updated: Sep-18; Applicability: O, P; Priority: Should
IP telephony is configured such that:

- *IP phones authenticate themselves to the call controller upon registration*
- *auto-registration is disabled and only a whitelist of authorised devices is allowed to access the network*
- *unauthorised devices are blocked by default*
- *all unused and prohibited functionality is disabled.*

Security Control: 0552; Revision: 5; Updated: Sep-18; Applicability: S, TS; Priority: Must
IP telephony is configured such that:

- *IP phones authenticate themselves to the call controller upon registration*
- *auto-registration is disabled and only a whitelist of authorised devices is allowed to access the network*
- *unauthorised devices are blocked by default*
- *all unused and prohibited functionality is disabled.*

Security Control: 1014; Revision: 5; Updated: Sep-18; Applicability: S, TS; Priority: Should
Individual logins are used for IP phones.

Traffic separation

Video conferencing and IP telephony networks should be logically or physically separated from data networks to ensure availability and sufficient quality of service.

Security Control: 0549; Revision: 3; Updated: Sep-18; Applicability: O, P; Priority: Should
Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.

Security Control: 0550; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Must
Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.

Security Control: 0556; Revision: 4; Updated: Sep-18; Applicability: O, P; Priority: Should
Workstations are not connected to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.

Security Control: 0557; Revision: 4; Updated: Sep-18; Applicability: S, TS; Priority: Must
Workstations are not connected to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.

Lobby and shared area phones

Lobby IP phones in public areas may give an adversary the opportunity to access the internal data network) by replacing the IP phone with another device or installing a device in line. Alternatively, the IP phone could be used for social engineering purposes (since the call may appear to be internal) or to access poorly protected voicemail boxes.

Security Control: 1015; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Traditional analog phones are used in lobby and shared areas.

Security Control: 0558; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
If IP phones are used in lobby and shared areas, their ability to access data networks, voicemail and directory services are prevented.

Microphones and webcams

Microphones (including headsets and Universal Serial Bus [USB] handsets) and webcams can pose a security risk in classified areas. An adversary can email or host a malicious application on a compromised website and use social engineering techniques to convince users into installing the application on their workstation. Such malicious applications may then activate microphones or webcams that are attached to the workstation to act as remote listening and recording devices.

Security Control: 0559; Revision: 4; Updated: Sep-18; Applicability: O, P, S; Priority: Should
Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.

Security Control: 1450; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas.

Developing a denial of service response plan

Telephony is considered a critical service for any organisation. A denial of service response plan will assist in responding to a video conferencing and IP telephony denial of service, signalling floods, and established call teardown and RTP data floods.

Resources and services that can be used to monitor for signs of a denial of service can include:

- router and switch logging and flow data
- packet captures
- proxy and call manager logs and access control lists
- video and voice-aware firewalls and gateways
- network redundancy
- load balancing
- PSTN failover.

Security Control: 1019; Revision: 7; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A denial of service response plan is developed and implemented that includes:

- *how to identify signs of a denial of service*
- *how to identify the source of a denial of service*
- *how capabilities can be maintained during a denial of service*
- *what actions can be taken to clear a denial of service.*

Further information

Further information on the use of telephones and telephone systems can be found in the telephone systems section of these guidelines.

Further information on the use of mobile devices can be found in the ***Guidelines for Enterprise Mobility***.

Further information on encryption can be found in the ***Guidelines for Using Cryptography***.

Further information on firewalls and gateways can be found in the ***Guidelines for Gateway Management***.

Fax machines and multifunction devices

Using cryptographic equipment with fax machines and multifunction devices

Specific information regarding the process and procedures for sending classified fax messages using High Assurance Cryptographic Equipment can be requested from the Australian Cyber Security Centre.

Fax machine and multifunction device usage policy

As fax machines and multifunction devices (MFDs) are a potential source of cyber security incidents, it is important that organisations develop a policy governing their use.

Security Control: 0588; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS; Priority: Must
A fax machine and MFD usage policy is developed and implemented.

Sending fax messages

Once a fax machine or MFD has been connected to cryptographic equipment and used to send a fax message, it can no longer be trusted when connected directly to unsecured telecommunications infrastructure or the PSTN. For example, if a fax machine fails to send a classified fax message the device will continue attempting to send the fax message even if it has been disconnected from cryptographic equipment and connected directly to the PSTN. In such cases, the fax machine could send the classified fax message in the clear causing a data spill.

Security Control: 1092; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Separate fax machines or MFDs are used for sending sensitive or classified fax messages and all other fax messages.

Security Control: 0241; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When sending fax messages, the fax message is encrypted to an appropriate level to be communicated over unsecured telecommunications infrastructure or the PSTN.

Receiving fax messages

While the communications path between fax machines and MFDs may be appropriately protected, personnel should still be aware of who has a need to know of the information being communicated. It is therefore important that fax messages are collected from the receiving fax machine or MFD as soon as possible. Furthermore, if an expected fax message is not received it may indicate that there was a problem with the original transmission or the fax message has been taken by an unauthorised person.

Security Control: 1075; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The sender of a fax message makes arrangements for the receiver to collect the fax message as soon as possible after it is received and notify the sender if the fax message does not arrive in an agreed amount of time.

Connecting multifunction devices to telephone systems

When an MFD is connected to a computer network and a digital telephone system, the device can act as a bridge between the two. The telephone system therefore needs to be authorised to operate at the same sensitivity or classification as the computer network.

Security Control: 0245; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A direct connection from an MFD to a digital telephone system is not enabled unless the telephone system is authorised to operate at the same sensitivity or classification as the computer network to which the MFD is connected.

Connecting multifunction devices to computer networks

As networked MFDs are considered to be devices that reside on a computer network, they should have the same security controls as other devices on the computer network.

Security Control: 0590; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Where MFDs connected to computer networks have the ability to communicate via a gateway to another network:

- *each MFD applies user identification, authentication and audit functions for all information communicated by that device*
- *security controls are of similar strength to those specified for workstations on that network*
- *each gateway can identify and filter information in accordance with the security controls for the export of data via a gateway.*

Copying documents on multifunction devices

As networked MFDs are capable of sending scanned or copied documents across a connected network, personnel should be aware that if they scan or copy documents at a level higher than that of the network the device is connected to, it will cause a data spill.

Security Control: 0589; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
MFDs connected to computer networks are not used to copy documents above the sensitivity or classification of the connected network.

Observing fax machine and multifunction device use

Placing fax machines and MFDs in public areas can help reduce the likelihood of any suspicious use going unnoticed.

Security Control: 1036; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Fax machines and MFDs are located in areas where their use can be observed.

Further information

Further information on encryption can be found in the ***Guidelines for Using Cryptography***.

Further information on MFDs communicating via network gateways can be found in the ***Guidelines for Gateway Management***.