



# Information Security Manual

DECEMBER 2021

## Guidelines for Communications Systems

### Telephone systems

#### Telephone system usage policy

All non-secure telephone systems are subject to interception. Personnel accidentally or maliciously communicating sensitive or classified information over a public telephone network can lead to its compromise.

**Security Control: 1078; Revision: 3; Updated: Dec-21; Applicability: All**

*A telephone system 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 the sensitivity or classification of conversations that they can be used for. In addition, personnel should also be made aware of the security risks associated with the use of non-secure telephone systems in sensitive or classified areas.

When using cryptographic equipment to enable different levels of conversation for different kinds of connections, providing a visual indication to personnel as to the sensitivity or classification of information that can be discussed over the telephone system can assist in reducing the likelihood of unintended disclosure of information.

**Security Control: 0229; Revision: 3; Updated: Sep-18; Applicability: All**

*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: All**

*Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.*

**Security Control: 0231; Revision: 2; Updated: Dec-21; Applicability: All**

*When using cryptographic equipment to permit 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 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: All**

*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: All**

*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 personnel are able to reduce security risks through the use of an audio secure room that is secure during any conversations then they may be used.

**Security Control: 0235; Revision: 4; Updated: Dec-21; Applicability: O, P, S, TS**

*Speakerphones are not used on telephone systems in TOP SECRET areas unless the telephone system is located in an audio secure room, the room is audio secure during conversations and only personnel involved in conversations are present in the room.*

## **Off-hook audio protection**

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

**Security Control: 0236; Revision: 5; Updated: Dec-21; Applicability: All**

*Off-hook audio protection features are used on telephone systems in areas where background conversations may exceed the sensitivity or classification that the telephone system is authorised for communicating.*

**Security Control: 0931; Revision: 6; Updated: Dec-21; Applicability: O, P, S, TS**

*In SECRET and TOP SECRET areas, push-to-talk handsets or push-to-talk headsets are used to meet any off-hook audio protection requirements.*

## **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 Cryptography](#).

## **Video conferencing and Internet Protocol telephony**

### **Video conferencing and Internet Protocol telephony gateways**

Where a video conferencing or IP telephony network is connected to another video conferencing or IP telephony network from a different security domain, the gateways section of the [Guidelines for Gateways](#) 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 Gateways](#) does not apply.

## Video conferencing and Internet Protocol telephony infrastructure hardening

Video conferencing and IP telephony infrastructure can be hardened in order to reduce its attack surface. For example, by ensuring that a Session Initiation Protocol server has a fully patched operating system, uses fully patched software and runs only required services.

**Security Control: 1562; Revision: 0; Updated: Dec-19; Applicability: All**

*Video conferencing and IP telephony infrastructure is hardened.*

## Video-aware and voice-aware firewalls

The use of video-aware and voice-aware firewalls provides network security while supporting video and voice traffic. As such, when a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video-aware and/or voice-aware firewall will need to be used; however, this does not require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. In such cases, organisations are encouraged to implement one firewall that is video-aware and data-aware; voice-aware and data-aware; or video-aware, voice-aware and data-aware depending on their needs.

**Security Control: 0546; Revision: 7; Updated: Dec-21; Applicability: All**

*Where a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video-aware and/or voice-aware firewall is used.*

## Protecting video conferencing and Internet Protocol telephony traffic

Video conferencing and IP telephony traffic can be vulnerable to eavesdropping, denial of service, person-in-the-middle and call spoofing attacks. To mitigate this security risk, video conferencing and IP telephony signalling and audio/video data can be protected with the use of Transport Layer Security. This is achieved through the use of the Session Initiation Protocol Secure protocol and the Secure Real-time Transport Protocol.

**Security Control: 0548; Revision: 4; Updated: Dec-21; Applicability: All**

*Video conferencing and IP telephony calls are established using a secure session initiation protocol.*

**Security Control: 0547; Revision: 4; Updated: Dec-21; Applicability: All**

*Video conferencing and IP telephony calls are conducted using a secure real-time transport protocol.*

## 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: All**

*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: All**

*Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.*

**Security Control: 0555; Revision: 3; Updated: Dec-19; Applicability: All**

*Authentication and authorisation is used for all actions on an IP telephony network, including registering a new IP phone, changing phone users, changing settings and accessing voicemail.*

**Security Control: 0551; Revision: 7; Updated: Jan-20; Applicability: All**

*IP telephony is configured such that:*

- *IP phones authenticate themselves to the call controller upon registration*
- *auto-registration is disabled and only authorised devices are allowed to access the network*

- *unauthorised devices are blocked by default*
- *all unused and prohibited functionality is disabled.*

**Security Control: 1014; Revision: 6; Updated: Dec-21; Applicability: S, TS**

*Individual logins are implemented for IP phones used for SECRET or TOP SECRET conversations.*

## **Traffic separation**

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

**Security Control: 0549; Revision: 4; Updated: Oct-19; Applicability: All**

*Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.*

**Security Control: 0556; Revision: 5; Updated: Oct-19; Applicability: All**

*Workstations are not connected to video conferencing units or IP phones unless the workstation or the device uses Virtual Local Area Networks or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.*

## **Internet Protocol phones in public areas**

IP phones in public areas may give an adversary the opportunity to access data networks or poorly protected voicemail and directory services. As such, any services accessible to IP phones in public areas should be restricted.

**Security Control: 0558; Revision: 6; Updated: Dec-21; Applicability: All**

*IP phones used in public areas do not have the ability to access data networks, voicemail and directory services.*

## **Microphones and webcams**

Microphones (including headsets and Universal Serial Bus [USB] handsets) and webcams can pose a security risk in SECRET and TOP SECRET areas. Specifically, 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: 5; Updated: Dec-21; Applicability: O, P**

*Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.*

**Security Control: 1450; Revision: 2; Updated: Dec-21; Applicability: O, P, S**

*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**

Video conferencing and IP telephony services are considered a critical service for many organisations. A denial of service response plan will assist in responding to denial-of-service attacks against these services.

**Security Control: 1019; Revision: 8; Updated: Dec-21; Applicability: All**

*A denial of service response plan is developed and implemented for video conferencing and IP telephony services that includes:*

- *how to identify signs of a denial-of-service attack*
- *how to identify the source of a denial-of-service attack*
- *how capabilities can be maintained during a denial-of-service attack*

- *what actions can be taken to respond to a denial-of-service attack.*

## Further information

Further information on the use of 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 Cryptography](#).

Further information on firewalls and gateways can be found in the [Guidelines for Gateways](#).

Further information on the use of web conferencing solutions can be found in the Australian Cyber Security Centre's [Web Conferencing Security](#) publication.

## Fax machines and multifunction devices

### Using cryptographic equipment with fax machines and multifunction devices

Further information on processes 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: All**

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

**Security Control: 1092; Revision: 2; Updated: Sep-18; Applicability: All**

*Separate fax machines or MFDs are used for sending sensitive or classified fax messages and all other fax messages.*

**Security Control: 0241; Revision: 4; Updated: Dec-21; Applicability: All**

*When sending fax messages, the fax message is encrypted to an appropriate level to be communicated over unsecured telecommunications infrastructure.*

### 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: 2; Updated: Dec-21; Applicability: All**

*The sender of a fax message makes arrangements for the receiver to collect the fax message as soon as possible after it is sent and for the receiver to notify the sender if the fax message does not arrive in an agreed amount of time.*

## Connecting multifunction devices to networks

As networked MFDs are considered to be devices that reside on a network, they should have security controls (e.g. authentication and auditing measures) of a similar strength to other devices on the network.

**Security Control: 0590; Revision: 5; Updated: Dec-19; Applicability: All**

*Security controls for MFDs connected to a network are of a similar strength to those for other devices on the network.*

## Connecting multifunction devices to both networks and digital telephone systems

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

**Security Control: 0245; Revision: 5; Updated: Dec-19; Applicability: All**

*A direct connection from an MFD to a digital telephone system is not enabled unless the digital telephone system is authorised to operate at the same sensitivity or classification as the network to which the MFD is connected.*

## 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: 5; Updated: Dec-19; Applicability: All**

*MFDs connected to 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: All**

*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 Cryptography](#).

Further information on MFDs communicating via gateways can be found in the [Guidelines for Gateways](#).