



Information Security Manual

Published: 22 June 2023

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.

Control: ISM-1078; Revision: 4; Updated: Dec-22; Applicability: All; Essential Eight: N/A

A telephone system usage policy is developed, implemented and maintained.

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.

Control: ISM-0229; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Personnel are advised of the permitted sensitivity or classification of information that can be discussed over both internal and external telephone systems.

Control: ISM-0230; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

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

Control: ISM-0231; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A

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.

Control: ISM-0232; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.

Cordless telephone systems

Cordless telephone handsets and headsets typically have minimal transmission security and are susceptible to interception. As such, using cordless telephone handsets and headsets may result in the disclosure of communications to an adversary unless appropriate encryption is used.

Control: ISM-0233; **Revision:** 4; **Updated:** Mar-23; **Applicability:** All; **Essential Eight:** N/A

Cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are encrypted.

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 and they should not be used. 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.

Control: ISM-0235; **Revision:** 4; **Updated:** Dec-21; **Applicability:** O, P, S, TS; **Essential Eight:** N/A

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.

Control: ISM-0236; **Revision:** 5; **Updated:** Dec-21; **Applicability:** All; **Essential Eight:** N/A

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.

Control: ISM-0931; **Revision:** 6; **Updated:** Dec-21; **Applicability:** O, P, S, TS; **Essential Eight:** N/A

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 encrypting communications can be found in the cryptographic fundamentals section of the [Guidelines for Cryptography](#).

Video conferencing and Internet Protocol telephony

Internet Protocol telephony

This section describes the controls applicable to Internet Protocol (IP) telephony and extends upon the prior telephone systems section.

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.

Control: ISM-1562; **Revision:** 0; **Updated:** Dec-19; **Applicability:** All; **Essential Eight:** N/A

Video conferencing and IP telephony infrastructure is hardened.

Video-aware and voice-aware firewalls and proxies

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

Control: ISM-0546; **Revision:** 9; **Updated:** Jun-22; **Applicability:** All; **Essential Eight:** N/A

When video conferencing or IP telephony traffic passes through a gateway containing a firewall or proxy, a video-aware or voice-aware firewall or proxy 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.

Control: ISM-0548; **Revision:** 4; **Updated:** Dec-21; **Applicability:** All; **Essential Eight:** N/A

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

Control: ISM-0547; **Revision:** 4; **Updated:** Dec-21; **Applicability:** All; **Essential Eight:** N/A

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.

Control: ISM-0554; **Revision:** 1; **Updated:** Sep-18; **Applicability:** All; **Essential Eight:** N/A

An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.

Control: ISM-0553; **Revision:** 3; **Updated:** Sep-18; **Applicability:** All; **Essential Eight:** N/A

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

Control: ISM-0555; **Revision:** 3; **Updated:** Dec-19; **Applicability:** All; **Essential Eight:** N/A

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.

Control: ISM-0551; **Revision:** 7; **Updated:** Jan-20; **Applicability:** All; **Essential Eight:** N/A

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.*

Control: *ISM-1014; Revision: 6; Updated: Dec-21; Applicability: S, TS; Essential Eight: N/A*

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.

Control: *ISM-0549; Revision: 4; Updated: Oct-19; Applicability: All; Essential Eight: N/A*

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

Control: *ISM-0556; Revision: 5; Updated: Oct-19; Applicability: All; Essential Eight: N/A*

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.

Control: *ISM-0558; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A*

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.

Control: *ISM-0559; Revision: 5; Updated: Dec-21; Applicability: O, P; Essential Eight: N/A*

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

Control: *ISM-1450; Revision: 2; Updated: Dec-21; Applicability: O, P, S; Essential Eight: N/A*

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

Denial of service response plan

Video conferencing and IP telephony services may be a critical service for an organisation. In such cases, a denial of service response plan will assist in responding to denial-of-service attacks against these services.

Control: *ISM-1019; Revision: 9; Updated: Dec-22; Applicability: All; Essential Eight: N/A*

A denial of service response plan for video conferencing and IP telephony services is developed, implemented and maintained.

Control: *ISM-1805; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: N/A*

A denial of service response plan for video conferencing and IP telephony services contains the following:

- *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 gateways can be found in the gateways section of the [Guidelines for Gateways](#).

Further information on firewalls can be found in the firewalls section of 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 Australian Signals Directorate-approved 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 an organisation develops, implements and maintains a policy governing their use.

Control: ISM-0588; Revision: 4; Updated: Dec-22; Applicability: All; Essential Eight: N/A

A fax machine and MFD usage policy is developed, implemented and maintained.

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.

Control: ISM-1092; Revision: 2; Updated: Sep-18; Applicability: All; Essential Eight: N/A

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

Control: ISM-0241; Revision: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A

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.

Control: ISM-1075; Revision: 2; Updated: Dec-21; Applicability: All; Essential Eight: N/A

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 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.

Control: ISM-0245; Revision: 5; Updated: Dec-19; Applicability: All; Essential Eight: N/A

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.

Authenticating to multifunction devices

To prevent users from printing sensitive or classified documents and forgetting to collect them, as well as assisting with the collection of sufficiently detailed event logs, MFDs should implement authentication measures that are of the same strength as used for other devices on the same network they are connected to, such as user workstations. For example, if user access to workstations on a network requires multi-factor authentication, so should user access to MFDs before users can print, scan or copy documents.

Control: ISM-1854; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Users authenticate to MFDs before they can print, scan or copy documents.

Control: ISM-0590; Revision: 8; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Authentication measures for MFDs are the same strength as those used for workstations on networks they are connected to.

Scanning and copying documents on multifunction devices

As MFDs residing on networks are often capable of sending scanned documents across networks they are connected to, personnel should be aware that if they scan documents at a level higher sensitivity or classification than that of the network it will cause a data spill. In addition, MFDs used to copy documents above the sensitivity or classification of the network may cause a localised data spill if copies are retained on non-volatile memory within the devices.

Control: ISM-0589; Revision: 7; Updated: Jun-23; Applicability: All; Essential Eight: N/A

MFDs are not used to scan or copy documents above the sensitivity or classification of networks they are connected to.

Auditing multifunction device use

MFD event logs, including metadata and shadow copies of documents printed, scanned or copied by users, can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents. To facilitate such activities, MFD event logs should be captured and stored centrally.

Control: ISM-1855; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: N/A

Use of MFDs for printing, scanning and copying purposes, including the capture of shadow copies of documents, are logged.

Control: ISM-1856; Revision: 0; Updated: Jun-23; Applicability: All; Essential Eight: N/A

MFD event logs are stored centrally.

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.

Control: ISM-1036; Revision: 3; Updated: Sep-18; Applicability: All; Essential Eight: N/A

Fax machines and MFDs are located in areas where their use can be observed.

Further information

Further information on encrypting communications can be found in the cryptographic fundamentals section of the [Guidelines for Cryptography](#).

Further information on event logging can be found in the event logging and monitoring section of the [Guidelines for System Monitoring](#).