Secure communications principles

Guidance to help you assess the security of voice, video and messaging communication services.

Modern technology provides a wealth of options for communicating in the workplace, which now includes voice, email, group messaging, and video conferencing.

This guidance contains a set of principles that can help all organisations make sound security decisions when selecting products and services that provide secure communications.

The guidance is aimed at risk owners and security professionals who wish to assess communication technologies for use in their organisations, to help them achieve the right balance of **functionality**, **security** and **privacy**. It is of particular relevance for those working in government (with OFFICIAL systems) and the public sector.

How to use this guidance

To choose a communications product or service, you should create a shortlist of candidates that provide the functionality you require, and assess them against these principles. You can then make informed decisions regarding the risk involved, to ensure your security needs are appropriately met.

The NCSC's secure communication principles

1. Protect data in transit
2. Protect network nodes with access to sensitive data
3. Protect against unauthorised user access to the service
4. Provision for secure audit of the service

/

5. Allow administrators to securely manage users and systems
6. Use metadata only for its necessary purpose
7. Assess supply chain for trust and resilience

---

1. Protect data in transit

Is data protected against eavesdropping and tampering?

Communications will typically transit an untrusted network, such as the internet. An untrusted network is outside of your control, which means someone may be able to access (or modify) data transiting that network.

You can protect against eavesdropping and tampering by using a service that encrypts and provides integrity of the data as it travels between participants.

Can participants confirm who they are communicating with?

Communications can inadvertently be sent to the wrong recipient. This could be as simple as mistyping the recipient's details, which on some open services could result in sending information outside your organisation. Alternatively, if someone can 'spoof' their identity (i.e. pretend to be somebody they are not), then they can trick users into communicating with them. By appearing as a trusted user, it's then simple to share links to malicious websites, or spread misinformation.

You should use a service that offers authentication of other users, which allows a recipient to confirm a sender's identity. Where unauthenticated users may be allowed to join communications, such as with video conferencing, the service should offer a way for trusted users to permit or block unauthenticated individuals' access to the communications.

---

2. Protect network nodes with access to sensitive data

Are network nodes with access to un-encrypted data protected appropriately?

Communications will typically transit a network, and in doing so they will pass through various servers and routers. Any of these network nodes with access to un-encrypted data may be able to access **all** communications between **all** users. Alternatively, a service may offer the ability to back up user data to a cloud solution, which could include a wealth of historical message data.

Network nodes that have access to un-encrypted data should be appropriately protected, at a level commensurate with the impact of any compromise of communications. If the appropriate level of protection required for network nodes cannot be met, you should consider using a service that encrypts data as it passes through (or resides at) network nodes.

Are network nodes that manage cryptographic key material protected appropriately?

Communications normally rely on cryptography for security, with trust in the security relying on cryptographic keys. If someone gained access to the key management functionality in a service, then they could abuse this trust (for example to spoof any user, or potentially access their communications data).

As cryptographic key material often acts as the root of trust in a secure communications service, any part of the service involved in key management should be appropriately protected at a level commensurate with the impact of compromise.

---

3. Protect against unauthorised user access to the service

Is user access to the service protected?

When a user sends content to another user, they will assume that only the true owner of the user's account will be able to access it. If someone else gains access to a user's account, they can impersonate them, see their communications, and send misinformation to other users.

User access to the service should be authenticated to ensure that only the intended users can access communications.

Is the user's device appropriately protected?

The device used to access a communications service will process un-encrypted data and may store user account credentials or key material, along with historic communications content. If someone were able to gain a privileged status on the device, then they may be able to access the application (or its data store), which could allow them to impersonate the user (or access communications content).

Devices should be appropriately configured to protect against unauthorised access to the user account, and ensure that communications are kept private. Using a compatible mobile device management (MDM) or mobile application management (MAM) solution may offer extra control over app data.

---

4. Provision for secure audit of the service

Does the service log security events?

The accidental or intentional misuse of the communications service could have a detrimental impact on an organisation. Certain events could indicate such misuse, for example:

- multiple failed login attempts
- access to the service at unusual times or from unusual locations
- excessive communications being sent

Using a service that logs security-related events allows authorised administrators to identify issues early, in order to limit any damage.

Do you require access to communications content for audit purposes?

Communications services have scope to be misused, for example by spreading malware, or launching phishing attacks. Alternatively, insiders could leak

privileged information, or commit financial fraud.

It is the responsibility of an organisation to decide if they require the ability to audit their communications; this could be to provide improved defensive monitoring or to fulfil regulatory/legal requirements (such as investigating fraud or unlawful activities). The ability to audit communications content could be impacted by certain solutions used to meet principle 1 (protect data in transit).

Where audit is required, the communications service should provide appropriate audit functionality.

Is access to audit functionality and communications content restricted?

Misuse of a service's audit functionality could allow unauthorised access to communications content. Only an authorised administrator (with appropriate permission and remit when access conditions are met) should be able to access communications content and associated metadata. Access to the audit functionality should be logged with a record of the activity performed, and the corresponding justification. The audit functionality provides access to sensitive data and so should meet principle 2 (protect network nodes with access to sensitive data).

---

5. Allow administrators to securely manage users and systems

Can administrators suitably manage their users' accounts?

If users are allowed to manage their own accounts, then an organisation will **not** have full control over how those accounts are accessed. Many organisations will need to manage how this is done, which could be as simple as a 'joiners, movers and leavers' policy to ensure that users' accounts are revoked when they leave the organisation. Another example may be managing user access to different groups within the service, or granting permission to certain users so that they can set up groups.

The communications service should allow administrators to securely manage their organisation's users. Administrators should be able to manage user accounts throughout their life cycle, giving them the required control to authorise or deny certain actions using the concept of least privilege.

Is administration and management protected and restricted?

Access to the administration interface of the communications service could allow new accounts to be created and user access permissions to be changed. If someone gained control of this, they could create unauthorised accounts on the system, which could then be used nefariously. They could also disable legitimate accounts, or elevate the permission levels of users to subvert security controls.

Administration and management of the system should be restricted to authorised individuals, whose privileged access should be authenticated, using two-factor authentication if supported, and logged. In addition, the enrolment of users onto the service should require identification of the user to ensure they are authorised, before provisioning security credentials for the user account. Administration should also be practical for the scale of the organisation, to ensure that administrators do not take shortcuts in performing authorisation checks before carrying out administrator functions.

---

6. Use metadata only for its necessary purpose

Is the use of metadata well-understood and used only when necessary?

When a communication is sent, the communications service needs certain metadata in order to operate. This includes user identifiers and timings (in other words, the 'who', 'where', 'when' and 'how' of the communication). This imparts information about users of the system, especially in aggregate, and if misused it could reveal the individual connections of users of the system.

You should ensure that the service only collects metadata that is necessary for the operation of the service, and that such metadata is only used for its necessary purpose. In particular, that it is not harvested, sold or exploited by the communications service. The communications service should provide clear and

transparent terms and conditions that set out what **content** and what **metadata** is collected and processed, and for what purpose. Moreover, you should have confidence that these conditions will be followed, and are appropriate for your corporate need (as opposed to a consumer need).

---

7. Assess supply chain for trust and resilience

Do you trust all components of the service?

If you do not have confidence in the security and operation of any component within the service, whether it be a mobile application or a cloud provider, then any assessment of the service could be undermined. You should build trust with the service provider to ensure that you are content with their supply chain security, including that of any third party products and services they rely on.

You should also consider how much control you require over your data, for example to be able to comply with relevant laws (such as GDPR). Choose a service that allows you to retain appropriate ownership of (and control over) your data, for example if you want to choose where data is geographically hosted. Using a service with open APIs can offer you greater access to your data or, alternatively, you may prefer to use a service that can be hosted and run on your own infrastructure.

How resilient is the service?

Communications services that are only supported by a single vendor carry certain risks with them. For example, there is a risk to the availability of the service if that vendor were to suffer a temporary outage (either accidental or malicious), or go out of business entirely. If the service is not reliable, then legitimate users may revert to using insecure communication methods. Alternatively, the service may change and no longer meet these principles, if (for example) the vendor is taken over by another company.

You may prefer to use a standards-based communications service, which is supported by multiple vendors in an interoperable way. The existence of

alternative providers reduces the dependence on a single vendor. You should also make sure measures are in place to ensure the availability of the service.

Are users able to communicate with contacts using different services?

Many organisations will wish to communicate securely with contacts outside of their own organisation. If a communications service does not allow this, then their members may revert to using an insecure service that does not meet these principles.

Where an organisation has requirements to securely communicate with people external to their organisation, they should choose a service that is interoperable with secure services used by partners.

PUBLISHED

16 January 2020

REVIEWED

30 September 2021

VERSION

2.0

WRITTEN FOR

Public sector

Cyber security professionals

Large organisations