GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

May 2020

Principles for Secure Video, Voice, and Messaging Communications

There are a number of technology options for communicating that now include voice, group messaging, and video. While many of these technologies require specific measures to ensure they are used securely, some enduring principles can be used to help organisations make sound security decisions. This includes considerations when selecting and managing these communication products and services and achieving the right balance of functionality, security and privacy. These include:

- Understanding your context
- Selecting a provider
- Understanding your provider's security stance
- Reviewing the provider's security settings
    - Protecting data in transit
    - Protecting access to sensitive data across networks
    - Protecting user access to the service
    - Ensure secure audit of communications is provided
    - Allow administrators to securely manage users and systems
    - Use metadata only for its necessary purpose
    - Assess supply chains for trust and resilience

Understanding your context

Develop a good understanding of the context within which you plan to use the communication service:

- Who will be using the service, and for what purpose?
- What is the sensitivity of the communications?
- What are the security requirements of the communications?
- Where, and from what device, will the service be used?
- What is the expected level of use, and how long is the service intended to be used for?
- What particular services are actually needed, and would unnecessary ancillary services add risk?
- What are the foreseeable consequences if something goes wrong? Who would be affected by those consequences?

Once you understand your context for using a service, you should be able to make a decision on how much information is required to support your risk assessment. If you have determined that there are no significant consequences to your organisation, it may not be necessary to ascertain as much assurance around the provider or their service.

You may find it helpful to complete the first 27 questions of the *GCDO Cloud Computing — Information Security and Privacy Considerations* to help you consider your risks. See: https://www.digital.govt.nz/dmsdocument/1-cloud-computing-information-security-and-privacy-considerations/html

Selecting the provider

It is important to understand details about the provider including:

- What is their profit model?
- Do they generate revenue mainly by charging for the service, or from advertising and analysis of the product's use?
- In which countries do they reside?
- What does their own supply chain of providers look like?
- Whose data centres do they operate out of? It is important to understand where the service is housed and managed.

Select a provider that supports you in exercising appropriate corporate governance. This means they should:

- Provide adequate corporate contracts (reflecting their own corporate capability);
- Allow easy access to terms of service and privacy statements; and
- Take a considered approach to your rights, your intellectual property, and indemnity.

Understanding your provider's security stance

It is important to have a good understanding of the security culture within the provider:

- Does the provider have any compliance or security certifications, and do they provide information on how to secure or manage their services?
- Does the provider allow security testing or provide proof that security is independently reviewed and tested?
- Do the provider's security statements contain information of substance, or is it more a generic marketing exercise?
- Is there any reporting around a security breach or disclosed vulnerabilities? If so, how did they deal with the problem and learn from their mistakes?

Government agencies should consider whether other agencies use the service and if they can provide material to assist you in making your assessment. Is the product or service on the All-of-Government approved panel agreement, or do they have a Government Chief Digital Officer (GCDO) Service Security Certificate? Has the provider completed the answers to the GCDO Cloud Risk Assessment tool, or are they open to doing so? Agencies should consult the GCDO for assistance in regard to these elements.

Review the provider's security settings

It is essential that you review the security features and settings offered by the product. Many services have an opt-in security approach, where their usage or sessions are essentially open-to-all by default and must be changed by whoever in your organisation is managing the service. The default security settings should be reviewed and amended to suit your organisation. Where possible and appropriate, the security settings established by the provider should be integrated with your existing security measures.

The following seven principles will help you to assess the provider's security settings:

1. Protecting data in transit

Using untrusted networks such as the internet for communications means someone may be able to access and possibly alter your data as it travels between participants. Encryption of the communications channel is an important mitigation against this threat. It is recommended that organisations follow the encryption standards as set out in Chapter 17 of the NZISM.

2. Protecting access to sensitive data across networks

Your communications will usually need to transit a network and pass through servers and routers. These critical network nodes may be able to access the unencrypted communications of users and therefore they need to be protected. If the appropriate level of protection required for the network nodes is not available, then you should consider alternative services that do not require unencrypted communications to pass through the network.

Where a network is purporting to protect communications with the use of cryptographic keys, it is crucial these keys are appropriately managed. If a malicious actor was to gain access to the key management in a service, they could gain access to communications, change them, or pretend to be a particular user. Cryptographic keys should be protected at the level commensurate to the potential impact of its compromise.

3. Protecting user access to the service

It is important to confirm that the right participants are part of the communication. This means ensuring the recipient's details to prevent sending information outside your organisation. Malicious actors could also 'spoof' users' identities and pretend to be legitimate users. To prevent this you should use services that require the authentication of users and confirmation of participants' identities.

Where cloud services are being used they should integrate with your organisation's cloud identity and access management (IAM) or other identity tools with multi-factor authentication (MFA). This reduces the risks of credentials being compromised within the service.

Control access to sessions with a password or PIN, and make sure notifications are enabled for when users join or leave a meeting. Some services have a waiting room or landing zone before you enter a session – if so, this should be utilised.

The devices of users must also be protected. This means ensuring that unencrypted data, user account credentials, and historical communications content is not easily available. User devices should be configured to protect against unauthorised access so that all communications on the device are kept private.

4. Ensure secure audit of communications is provided

All communications services are likely to be subject to malicious attempts to access the data they hold. It is consequently important to have the ability to audit the service and undertake incident response and investigation activities. Make sure you have clear policies for, and control over, things such as session recording and logging.

Given how critical the audit functionality for the service is, the control of access to communications content needs to be via a strict authorisation process. Only administrators with permissions should be able to access communications content and metadata. All access to the audit function needs to be logged, and any activity recorded and justified.

5. Allow administrators to securely manage users and systems

Your administrators need to be able to manage all users' accounts to ensure that there is control around how those accounts are accessed and used. This could be outlined in an organisational policy for how your users join and leave service accounts. These policies could also specify which groups a user will have access to, and what permissions they have for setting up new groups. The service you adopt should allow your administrators to manage users during service use and terminate access when necessary.

Access to administrator roles should be restricted and only permitted by individuals who are authorised. Administrators should only be enrolled with their privileges following an appropriate identification process and gain accesses after they have been authenticated with a form of two-factor authentication. All of their activities should be logged and audited as required.

6. Use metadata only for its necessary purpose

Many communications services require metadata contained within the communications to be able to deliver the service. Metadata may include the identification of users and key characteristics of the communication itself. It is important that any metadata being utilised has been agreed in the terms and conditions of use. These terms need to transparently outline what metadata and other content is collected, and the purposes this may be used for. It is critical to understand where there is risk of data being harvested, sold or exploited by the communications service. The considerations around these issues may be different for an organisation and its information assets than for an individual.

7. Assess supply chains for trust and resilience

It is important that you can trust all aspects of the service and that you are comfortable with their supply chain security and the third-party products and services they depend upon. You also need to consider the interoperability of the service with your current technology solutions, and whether it introduces new risks to legacy infrastructure.

Your reliance upon one service could be an issue from an availability and security perspective and it may be prudent to use multiple vendors and avoid vendor lock-in. These measures will also help to reduce the risks around services that do not permit communication outside their network and raise the likelihood of personnel using alternative, insecure 'shadow IT'. Proactive planning will help to reduce the risk of unsuitable communications services being adopted during a crisis.

For further information and advice please contact the National Cyber Security Centre (NCSC): info@ncsc.govt.nz

Helpful links:

- For the all-of-government list of current suppliers, see: https://www.digital.govt.nz/products-and-services/current-suppliers/
- Government Chief Digital Officer (GCDO) – Privacy, Security and Risk: https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/security/
- For the GCDO cloud risk questionnaire within the *Cloud Computing — Information Security and Privacy Considerations,* see: https://www.digital.govt.nz/dmsdocument/1-cloud-computing-information-security-and-privacy-considerations/html
- Chapter 17 of the New Zealand Information Security Manual: https://www.nzism.gcsb.govt.nz