National Cyber Security Centre

# Working Remotely: Getting Started on Cloud Security

New Zealand's National Cyber Security Centre is hosted within the Government Communications Security Bureau

**March 2020**

## Principles for Implementing Cloud Technologies at Pace

The threat of COVID-19 is forcing many organisations to find alternative ways to ensure their workforce remains operational. For some, this will require the creation and adoption of new processes and technology.

Cloud services are one of the few practical solutions available to meet the challenge of working remotely, however the movement to cloud services at pace creates risks. Managing these risks should be an organisation's objective throughout its COVID-19 response in order to ensure short-term fixes don't become long-term problems.

### Assess the risks

The need to maintain a productive and operational workforce needs to be weighed against information security risks. Organisations must continue to conduct risk assessments on products and services, especially when working at pace, to ensure they are making good decisions. An organisation's leaders and decision-makers are responsible for the security risks a new IT solution might introduce.

Make sure the business context for new tools and technologies is well-understood. A tool may be able to be set up quickly and easily, but it should still achieve all the required business objectives. For instance, not all cloud solutions can provide access to, or replicate the functions of, existing critical systems. Half solutions created out of expediency produce a great deal of 'technical debt' that must be resolved at a later date.

It is important you carry out some kind of risk assessment on any new services and processes you are looking to adopt. Risk assessments can be supported by reviewing other organisations' certification and accreditation (C&A) or assessments on the same product. No two organisations are identical, so consider any factors unique to your organisation – including risk appetite.

When operating at pace or in an agile way, security needs to be part of the whole development process, not tacked on at the end. The earlier security is considered, the more secure the final product will be.

It may not be possible to complete C&A before a remote access solution is implemented. However, you must have a plan and a timeline for the completion of a formal risk assessment and C&A, along with implementing any additional security controls required.

Cloud services often include online security tutorials, benchmarks and security scoring systems to guide good security decisions. Use them, and seek to implement robust security settings wherever possible.

## Supply chain risks

When deploying cloud solutions, it is important to know what data is going to be hosted outside of New Zealand. Data that is hosted in or transiting another jurisdiction is at higher risk of collection by foreign entities. This also exposes organisations to potential compliance risks.

Vendors are the key to finding and deploying cloud solutions in the current context. Make sure that vendors are trusted and have a track record of providing high-quality services. Where possible, public sector organisations should use trusted all-of-government services and common capabilities. Seek assurance from vendors that what they are supplying includes appropriate security considerations.

## VPNs, segmentation, and role-based access

When working remotely, all access to corporate systems should be via a Virtual Private Network (VPN). In addition to a VPN, access to resources should be based on roles. Segmentation and role-based access minimises the spread or impact of an incident, should one occur. For example, HR staff don't need access to your finance systems, and separating them ensures an incident on one system does not impact the other. It is even more important to ensure that administrator access, dashboards, or settings of any IT systems are strictly locked down to the necessary individuals.

## Multi-factor authentication

With staff working from home, strong multi-factor authentication (MFA) is a critical mitigation against unauthorised access. Activate, and consider mandating, MFA for all of your cloud services, across all users. The VPN is a critical IT asset and MFA for a VPN is more important than ever.

MFA can be implemented through one-time password (OTP) applications. Examples of these include Google Authenticator, Microsoft Authenticator, or Authy.

Hardware security tokens, such as YubiKeys, are also recommended. If you already have a supply of hardware security tokens and/or keys, prioritise the provision of these to privileged account holders such as system administrators and security teams.

It may be tempting to use TXT/SMS because this seems the simplest to roll out. While this authentication method is better than nothing, TXT/SMS is considered the least-secure MFA method. See the US National Institute for Standards and Technology (NIST) for further information regarding the security issues surrounding the use of TXT/SMS for MFA.

## Log everything

Monitoring and logging of systems and environments is key, even when it cannot be carried out in real time. Keeping comprehensive logs, and reviewing them at a later date, will be beneficial. At a minimum, when business returns to normal it will help you understand who did what, as well as when and how they did it. This will be useful for a number of reasons, including identifying any suspicious behaviour, especially if an incident is detected. If an

organisation has an existing SOC or SIEM, ensure the logs from any new cloud service are ingested into monitoring tools.

## BYOD use with your systems

If staff have been issued laptops for remote work, insist that they are used only for work purposes. Mixing work with play on a single device or account increases the risk to an organisation.

If staff have not already been issued with devices, procuring enough laptops may be a challenge. Some organisations already have policies regarding staff use of personal devices for work purposes. Where your organisation permits staff to use their own devices, the goal is to ensure that official information and organisational information systems are protected to a level equivalent to an environment provided and managed by the organisation.

For information regarding the use of personal devices for work purposes and Bring Your Own Device (BYOD) policies and controls, see the New Zealand Information Security Manual (NZISM).