Security considerations for remote working arrangements

From report 18: 2019/20 – Information Systems Audit Report 2020 – State Government Entities

Office of the Auditor General
Serving the Public Interest

In response to the spread of the Coronavirus (COVID-19), entities in all sectors across Australia are encouraging staff to work remotely from home. Rapid transition to these arrangements can introduce risks and challenges for entities who may not have previously implemented large-scale remote working arrangements. It is important that entities manage and address these risks, as well as staff security behaviour, to prevent people from exploiting the current situation to compromise systems and information.

The following table outlines some guiding principles entities should consider when rolling out remote working technology and procedures. This is not intended to be an exhaustive list. Entities can obtain further guidance from the Australian Cyber Security Centre[1] and the Office of Digital Government has recently issued some considerations for remote work.

Principle	Our expectation
Prioritise and simplify	Each entity needs to assess their unique risks associated with remote working arrangements and address critical risks as a priority. These risks will be different for each entity depending on the functions staff perform remotely and the types of information being accessed. Entities should ensure that procedures and technology for remote working are simple and easy to follow. Complex processes can introduce vulnerabilities that could result in undesired outcomes.
Engage with staff	Increase staff awareness by clearly communicating expectations including policies and any occupational health and safety requirements. The business continuity plan may come into effect and it is also important that staff understand how the plan impacts their day to day working procedures. Staff should have easy access to a forum or group where they can seek answers to their queries related to working from home and security.
Remote access technology	The technology used for remote access needs to be secure. The security controls that entities select will depend on the method of remote access, such as: • virtual private network (VPN) • web applications • remote desktop access Remote access servers should enforce technical controls in line with security policies.
Security of network	The majority of the remote workers will use internet to access entity resources. Entities should implement appropriate policies to secure remote access originating from untrusted networks. VPN is one of the better methods of securing remote access because it uses encryption to protect the confidentiality and integrity of communication over the network.

[1] https://www.cyber.gov.au/news/cyber-security-essential-when-preparing-covid-19

Principle	Our expectation
Physical security	Remote working locations may not be as secure as office environments. Entities need to understand the risks associated with this and define and implement appropriate controls to protect information. For example, implementing encryption on portable devices is a simple method to improve security. Entities also need to ensure the security of sensitive hard copy documents is maintained.
Multi-factor authentication	Remote access into entity systems and networks must be secured by strong authentication controls. Entities should implement multi-factor authentication for all remote access.
Bring your own device (BYOD) policies	A risk based policy should define the requirements for personal devices if they are allowed to access entity resources. Personal devices are generally not as secure as those provided by entities and attackers could exploit this weakness as more people work from home. Considerations should be given to: • encryption • access levels • segregated network zone for personal devices • security patch levels • malware controls.
Patch systems	All systems should be patched with latest updates. This applies to all the internet facing infrastructure and client applications.
Stay vigilant	Stay alert and educate staff on the risks especially phishing emails and text messages themed around COVID-19.

Source: OAG based on Australian Cyber Security Centre guidance