Cyber Security Primer

Prepared By:

Datanova Compliance Team

INDEX

Disclaimer

This document is not meant to be a definitive guide on Cyber Security and the author is not a cyber security specialist. This guide was put together at the request of Datanova clients and is only meant as an introduction to some of the things that can be implemented to increase protection against cyber attacks.

Datanova recommends that you contract a Cyber Security Specialist to review your systems and processes and follow their advice on increasing security. Obtaining ISO27001:2022 certification will provide you with a complete Information Security framework to not only protect against cyber-attacks, but also ensure that your information security policies and procedures meet international standards.

1. Introduction

Cyber-crime has now surpassed all other forms of crime in value. Cyber criminals are targeting systems that contain valuable information of individuals. NDIS participants are a prime target, so NDIS Providers have an obligation to protect the Personal Identifiable Information (PII) of participants.

Rather be safe than sorry. Do not trust anybody. You never know who might find themselves in a compromising position which open them up for exploitation. The cyber-criminals are clever and ruthless – they want your data and don't care what they do to get it.

2. Hardware

- Ensure that every computer has a dedicated Admin User login. This is different from the standard user login which should never allow a user to install software on a computer or alter system settings.
- Only properly licenced software should be installed by a trusted IT Technician.
- All magnetic and solid-state drives must have encryption turned ON. This will prevent access to the data in the event of the computer being lost or stolen.
- If you are using Apple computers, enable "Find My Mac" to help locate stolen or misplaces computers.
- Install software or apply machine policies to prevent saving data to USB drives.
- Create a checklist of software to be installed on each computer, or even better, a standard image for every user type which eliminates human error.

3. End Point Protection

- Every computer MUST have End Point Protection software installed that continuously scan for malware. Sophos is one of the best.
- Consider installing End Point Protection software that enables remote wiping of data.

4. Access to Software and Data

- Limit who can access data and software programs. Put rules in place to limit access to data and only install the software required to perform the duties of the user. The reasoning here is that one can't copy or corrupt data that one does not have access to.
- Disallow access to social media sites on company owned computers, including access to private e-mail accounts.

5. Passwords

- Ensure the use of strong passwords
  - Some agencies just advise a long pass phrase without the need for special characters
  - The longer and more complex a password is, the more secure it is – e.g. 14 characters that include capitals, lower case, numbers and special characters.

- It is virtually impossible to remember all the different passwords required by the different programs and applications we use, so use password managers to help keep you sane.
- Most password managers have built-in functions that create complex passwords. If you use a password manager, ensure that you have a very strong master password and link it to a fingerprint scanner , face id or multi-factor authentication for added security.
- Never write down passwords in a place where others can find it, especially not on a sticky note stuck to the computer screen. This sounds logical, but I see it all the time.
- Enable multi-factor authentication wherever possible. It can be cumbersome, but it provides an extra layer of protection to keep you safe.

6. Networks

- Install a hardware firewall to control incoming and outgoing network traffic.
- Use strong passwords to gain access to wireless networks.
- If practical, restrict device access using a RADIUS server or MAC address whitelisting.
- Never allow non-employees access to your networks – if required you might need to install a second network with limited access.
- Do not allow employees to access the company network or internet with privately-owned computers and smart phones.

7. Internet

- Disallow access to the internet with exception to reliable cloud services like FlowLogic.
- If your employees need internet access, restrict the sites they can visit by creating whitelists.

8. Email

- Company e-mail is for business purposes only – enforce this. Do not allow access to private e-mail accounts on company-owned computers.
- Be very careful when opening e-mail from an unknown sender, and NEVER click on an attachment without first scanning it with your anti-virus software.
- Consider installing mail-scanners to stop malicious mail from getting to end users.
- Limit what attachments employees can send via e-mail. All data containing PII must be encrypted before sending it.
- Ensure company email has correctly configured SPD, DKIM and DMARC records.

9. Data Security

- Keeping you information safe includes backing up locally stored data, be that on your own server (if you have one) or on users' magnetic or solid-state drives. Making regular backups is important, but verifying the backups are even more important. A backup is only useful if it can be restored successfully.
- All company data and documents should be stored on a local server or in the cloud. This allows for the easy sharing of information. Create a logical directory structure on all your shared drives and restrict who can create additional folders. If you give your employees free reign you will spend your life searching for data.
- Implement and enforce a standard file naming convention. This makes finding a stored file so much easier.
- Cloud storage is safe and secure, and the service provider typically ensures that your data is backed up as part of the service agreement. However, do your research to determine where the data is stored physically – there is legislation in place that prohibits data containing Australian PII being store outside of Australia.
- This legislation also covers the use of smartphone apps – no PII may be stored or transmitted via apps if there is any risk that the data may leave Australian soil.

10. Education

- The most important thing you can do to protect against cyber-attacks is to train your staff in cyber security. Knowledge is power!
- Create and enforce Policies and Procedures to ensure cyber security is maintained. Ensure that your staff are trained in these policies and procedures and implement measures to ensure that the Policies and Procedures are being adhered to.

End of Document

Revision History				
Version	**Details of Changes**	**Updated by**	**Approved by**	**Date Approved**
0	Creation of document	Johan Steyl	Christian Krauter	