APPENDIX TWO

Data security self-assessment for providers of Justice services

Instructions for using this assessment

- You should complete this self-assessment if you deliver justice services for our Ministry, for example if you are a family violence, restorative justice or community law service provider etc.
- It is a useful but optional resource for legal aid lawyers and one-off providers of court services (such as court report writers).
- Assess your organisation against 28 data security measures that have been identified as realistic measures you can take to help keep information safe. We acknowledge some may not be appropriate for the type or size of your organisation.
- There are two levels of recommended data security controls, priority 1 (orange) and priority 2 (yellow). If implementing changes in your organisation, it is recommended you put in place priority 1 controls first.
- Once completed, please hold the self-assessment form within your organisation for monitoring and audit purposes. We may discuss your assessment with you.
- You should review and update your self-assessment annually, or more frequently if your systems and processes change.
- Footnotes explain IT terms in more detail. Please get in touch if you need any help to complete this form.

Name of your organisation:

Name and role of person completing the self-assessment:

Date of self-assessment:

Section 1: Educating your personnel about data security

Question	Please indicate which most applies to your organisation	*When were people last reminded of their responsibilities?* 6mth	12mth	24mth	24mth+	Comments (including any reasons the recommended control is not applicable to your organisation)
1. Are people aware of common cyber-attacks? This includes hacker tactics such as fraudulent emails (phishing), infecting systems with rogue USBs (baiting), fake IT support calls seeking passwords (quid pro quo), tricking people into thinking they have been hacked so they download infected software (scareware) etc.	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

Question	Please indicate which most applies to your organisation	*When were people last reminded of their responsibilities?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
2. Are people aware of the importance of using strong passwords[1]?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
3. Do people know how to report a cyber security incident?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

Section 2: Protecting your devices and files from unauthorised access or loss

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
4. Is encryption[2] applied to all your portable devices? (i.e. passwords on all laptops, phones, tablets and USB drives)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
5. Are your operating systems and applications, including patch management[3] up to date for all devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
6. Do all your devices have up-to-date antivirus[4] protection?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
7. Are Microsoft Office macro settings configured to allow only trusted macros[5] on all your devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

1 **Strong passwords** are passwords that are difficult for others to guess, typically involve unpredictable phrases, or the use of multiple character types such as capitalisation, numbers and special characters such as #,?, <, % etc). CERT NZ provides guidance at **https://www.cert.govt.nz/business/guides/policies-and-processes/password-policy-for-business/**

2 **Encryption** is the encoding or 'scrambling' of information so that it cannot be accessed by people who don't have the right key (password) to decrypt it. Encryption can be applied to network traffic, files, folders, portable drives, or entire devices. Microsoft provides guidance on encrypting files at **https://support.microsoft.com/en-us/help/4026312/windows-10-how-to-encrypt-a-file**.

3 **Patch management** is the process of ensuring that vulnerabilities that have been identified in software or devices you use are corrected promptly, by regularly installing security updates released by vendors. CERT NZ provides guidance at **https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/keep-up-with-your-updates/**

4 **Antivirus** products can detect and block many forms of viruses and other malware hidden in files. Ensuring that all devices (computers, phones, laptops) have antivirus products installed and constantly kept up to date will help to ensure they are adequately protected from malicious files.

5 **Macros** are small applications that can run inside larger applications – usually within Microsoft Office documents such as Word, Excel and PowerPoint. When used maliciously in a document, macros have the potential to delete files, upload data, or download further malicious applications.

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
8. Is data on all your devices regularly backed-up? (e.g. to cloud-based service or external hard drive)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
9. Are all sensitive documents encrypted before you send them over the internet? (e.g. email, file sharing service)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
10. Do you have up-to-date firewall[6] protection for any systems or devices connected to the internet?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
11. Do you use a proxy / web filtering[7] service to automatically scan and allow or block access to certain websites on all your devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
12. Do you restrict application usage[8] to prevent untrusted applications from running on your devices?	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
13. Are unused services and ports on all your devices disabled[9]?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
14. Is autorun[10] disabled on all your USB drives?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
15. Do you have a guest network[11] available on your Wi-Fi for customers/clients?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

6 **Firewall** is hardware or software that monitors incoming and outgoing network traffic (for example to or from the internet) and permit or blocks traffic based on a set of security rules. Firewalls can block suspicious traffic and prevent attacks.

7 **Proxy/web filtering service** is a service that sits between you and the internet. It runs every website request through a filter, looks up each address in its database of allowed or disallowed sites, and allows or blocks each request accordingly. This can be used to ensure websites with bad reputations are automatically denied if requested by users.

8 **Restricting application usage** is restricting the ability of software programmes and processes able to run on a device to a list of known and trusted applications. Usually carried out by policies and rules on the device's operating system or by software installed on the device. Further guidance on **https://www.cyber.gov.au/publications/implementing-application-whitelisting**

9 **Disabled ports** are services or protocols not required for systems to function made inoperable.

10 **AutoRun** is the ability of programmes or services to be automatically launched from a USB drive as soon as it is plugged into a device. You can search the USB manufacturer's support pages for guidance on disabling autorun.

11 **Guest network** is a network (usually Wi-Fi) provided for external parties (e.g. clients) that is segregated from networks used by the business, preventing third-party access to information held by the business.

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
16. If you have a website(s) – Do you regularly engage a security consultant to independently test your website for vulnerabilities? (i.e. penetration testing[12])	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

Section 3: Ensuring information is only being accessed on a need to know basis, and regularly reviewing who can access what information.

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	**Comments** (including any reasons the recommended control is not applicable to your organisation)
17. Do you use multifactor authentication[13] for any online service containing personal information? (e.g. your email accounts, case management system)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
18. Have you ensured default credentials[14] (factory setting passwords) on any off the shelf product you use have been replaced with strong passwords? (e.g. new software, network devices and web services)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
19. Do you regularly review user and administrator accounts and disable accounts you no longer require?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
20. Are individual user accounts (not shared) used for logging onto systems and web services?	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
21. Is all information stored and accessed through services and devices under your control? (i.e. not on personal devices of your staff/ volunteers)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

12 **Penetration testing** is technical testing by security consultants to find vulnerabilities that could be exploited by malicious parties, using similar tools and techniques as hackers use. Further guidance on **https://www.ncsc.gov.uk/guidance/penetration-testing**

13 Multifactor authentication is a requirement for more than one control factor to be provided in order to gain access to a system. Examples include using an ATM which requires possession of a bank card and knowledge of a PIN number, or one-time code numbers sent to a user's mobile phone once a valid user name and password combination has been provided. CERT NZ has resources on **https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/two-factor-authentication/**

14 Default credentials are any generic username and passwords provided with a system by the manufacturer to allow a new owner initial access to a system. CERT has resources on **https://www.cert.govt.nz/it-specialists/guides/default-credentials/**

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	Comments (including any reasons the recommended control is not applicable to your organisation)
22. **Do your systems require users set strong and difficult to guess passwords?** (For example email passwords have minimum character requirements).	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
23. **Can you monitor and log what information your users have accessed/used?**	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
24. **Do you use a single service to manage the sign-in process (passwords) for multiple applications within your organisation?** (i.e. centralised authentication[15]).	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	
25. **Are email accounts within your organisation used for business purposes only?** (i.e. not used to log into Facebook, Twitter, etc)	◯ All ◯ Some ◯ None ◯ N/A	◯	◯	◯	◯	

Section 4: Responding appropriately to a privacy or cyber security incident

Question	Please indicate which most applies to your organisation	*If you have a plan for putting this control in place, when?* 6mth	12mth	24mth	24mth+	Comments (including any reasons the recommended control is not applicable to your organisation)
26. **Can you wipe[16] your portable devices remotely if necessary?** (e.g. if a device is lost or stolen)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
27. **Can you monitor and log any external attempts to gain unauthorised access to your services or devices?** (i.e. monitor attempts to breach firewalls, network devices, database applications, file access on shared drives)	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	
28. **Do you have and periodically test processes to restore your IT services following disruption by a significant event?** such as earthquake, fire, flood or other event that prevents your normal operations. (i.e. disaster recovery).	◯ Yes ◯ No ◯ N/A	◯	◯	◯	◯	

15 Centralised certification is a single service to manage the sign-in process for multiple applications used within an organisation.

16 Remote wiping is the ability to delete all user data and information from a device without being in physical possession of the device. Remote wiping is typically provided on modern smartphones.

Definitions

Table 1: Terms used in these guidelines

Term	Description	More information
Antivirus protection	Antivirus products can detect and block many forms of viruses and other malware hidden in files. Ensuring that all devices (computers, phones, laptops) have antivirus products installed and constantly kept up to date will help to ensure they are adequately protected from malicious files.	**https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product**
Autorun on USB	AutoRun is the ability of programmes or services to be automatically launched from a USB drive as soon as it is plugged into a device.	Search the manufacturer's support pages for your operating system for guidance on disabling autorun.
Centralised authentication	A single service to manage the sign-in process for multiple business applications within a business.	
Cloud-based services	Services delivered by other parties via the public internet to which anyone can sign up or subscribe to use.	**https://www.cert.govt.nz/individuals/guides/stepping-up-your-cyber-security/how-the-cloud-works/**
Court and judicial information	Information that is in the possession of the court and is listed in the District Court Act and that does not fall within the protection of the Privacy Act 2020	*"The Senior Courts Act 2016 Schedule 2 and the District Court Act 2016 Schedule 1 defines categories of court information".*
Default credentials	Any generic username and password provided with a system by the manufacturer to allow a new owner initial access to a system.	**https://www.cert.govt.nz/it-specialists/guides/default-credentials/**
Disabled ports	Computers connect with each other over a combination of services and protocols. Disabled ports refers to the process of making inoperable any service or protocol not required for the system to function.	**https://www.cert.govt.nz/it-specialists/critical-controls/unused-services-and-protocols/**
Disaster recovery	Processes and resources to restore business services following disruption by a significant event such as earthquake, fire, flood or other event that prevents normal business operation.	
Encryption	Encryption is the encoding or 'scrambling' of information so that it cannot be accessed by people who don't have the right key (password) to decrypt it. Encryption can be applied to network traffic, files, folders, portable drives, or entire devices.	Microsoft provides guidance on encrypting files at **https://support.microsoft.com/en-us/help/4026312/windows-10-how-to-encrypt-a-file**.
Firewall protection	A firewall is hardware or software that monitors incoming and outgoing network traffic (for example to or from the internet) and permit or block traffic based on a set of security rules. Firewalls can block suspicious traffic and prevent attacks.	**https://www.staysmartonline.gov.au/protect-your-business/doing-things-safely/firewalls**
Guest networks	A network (usually Wi-Fi) provided for external parties (e.g. clients) that is logically segregated from networks used by the business, preventing third-party access to information held by the business.	
Macros	Macros are small applications that can run inside larger applications – usually within Microsoft Office documents such as Word, Excel and PowerPoint. When used maliciously in a document, macros have the potential to delete files, upload data, or download further malicious applications.	**https://www.cyber.gov.au/publications/microsoft-office-macro-security**

Term	Description	More information
Malware	A kind of malicious software designed to damage or harm a computer system and often aims to go unnoticed.	https://www.cert.govt.nz/individuals/explore/malware/?topic=malware
Multifactor authentication	A requirement for more than one control factor to be provided in order to gain access to a system. Examples include using an ATM which requires possession of a bank card and knowledge of a PIN number, or one-time code numbers sent to a user's mobile phone once a valid user name and password combination has been provided.	https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/two-factor-authentication/
Patch management	The process of ensuring vulnerabilities that have been identified in software or devices are corrected promptly, by installation of security updates released regularly by vendors.	https://www.cert.govt.nz/individuals/guides/getting-started-with-cyber-security/keep-up-with-your-updates/
Penetration testing	Technical testing by security consultants to find vulnerabilities that could be exploited by malicious parties, using similar tools and techniques that hackers use.	https://www.ncsc.gov.uk/guidance/penetration-testing
Personal information	Personal information is any information that could identify a living person. A person doesn't have to be named in the information if they can be identified from it in other ways (for example, by a combination of characteristics, or by association with other information such as the context). Personal information includes contact details, a person's image or a recording of their voice, and their bank account, fines, and financial information.	s7 of the Act, Interpretation and related matters, and s69 Interference with privacy of individual.
Privileged accounts	System accounts that have rights in excess of those required by normal users. Typically used by system administrators for the purposes of managing, configuring or managing access to systems under their control.	https://www.cyber.gov.au/publications/restricting-administrative-privileges
Proxy/web filtering services	A service that sits between you and the internet. It runs every website request through a filter, looks up each address in its database of allowed or disallowed sites, and allows or blocks each request accordingly. This can be used to ensure websites with bad reputations are automatically denied if requested by users.	
Remote wiping	The ability to delete all user data and information from a device without being in physical possession of the device. Remote wiping is typically provided on modern smartphones.	
Restricting application usage	Restricting the ability of software programmes and processes able to run on a device to a list of known and trusted applications. Usually carried out by policies and rules on the device's operating system or by software installed on the device.	https://www.cyber.gov.au/publications/implementing-application-whitelisting
Strong passwords	Techniques to design passwords that are difficult for others to guess, typically involving unpredictable phrases, or the use of multiple character types such as capitalisation, numbers and special characters such as #, ?, <, % etc).	https://www.cert.govt.nz/business/guides/policies-and-processes/password-policy-for-business/
Web services	Services that are provided by other parties via the public internet.	