APPENDIX TWO

Contract Compliance statement

for Third Party criminal conviction history check customers

Instructions for using this assessment

- You should complete this self-assessment if you have signed a Contract for Online Delivery of Criminal Conviction Histories (the Contract) with the Ministry of Justice.
- Assess your organisation against 16 compliance measures that have been identified as realistic measures you can take to help comply with the terms and conditions of the Contract. We acknowledge some may not be appropriate for the type or size of your organisation.
- Once completed, please hold the self-assessment form within your organisation for review 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 at CCHonline@justice.govt.nz

Name of your organisation:	
Name and role of person completing the self-assessment:	
Date:	

Section 1: Terms and requirements

I confirm that to the best of my knowledge and after making due enquiry with my reports:

Statement	Acknowledgement	Comments
1. My organisation is compliant with the requirements and obligations as per clause 3.1 of the Contract, including the CCH User Guide.	◯ Yes ◯ No ◯ N/A	
2. My organisation is compliant with the Ministry's privacy, confidentiality and security requirements, as per clause 10 of the Contact.	◯ Yes ◯ No ◯ N/A	
3. My organisation has such privacy training in place as may be reasonably required to ensure compliance with clause 10 of the Contract.	◯ Yes ◯ No ◯ N/A	
4. My organisation has procedures and system steps in place to ensure compliance with the Valid Identification requirements, Evidence of Identity requirements, and retention of Authorisation and Valid Identification requirements, as per clause 6.4 of the Contract.	◯ Yes ◯ No ◯ N/A	
5. My organisation has procedures or system steps in place to ensure compliance with the Contract and instances of non-compliance are reported to the Ministry.	◯ Yes ◯ No ◯ N/A	

6. Instances of significant non-compliance[1] of any term in clause 10 of the Contract have been notified immediately to the Ministry and are included on this form.	◯ All ◯ Some ◯ None ◯ N/A	
7. I have attached completed statements of all my organisation's administrators.	◯ All ◯ Some ◯ None ◯ N/A	
8. I have discussed Conflicts of Interest with my team this year. All Conflicts of Interest have been disclosed and are appropriately managed.	◯ Yes ◯ No ◯ N/A	

[1] This will depend on the specific legislation or obligations around non-compliance e.g. associated consequences, one-off systemic problem.

Section 2: Securities and data

Question	Please indicate which most applies to your organisation	Comments
9. Do all your devices have up-to- date antivirus[2] protection?	◯ All ◯ Some ◯ None ◯ N/A	
10. If you have a website(s) through which information is collected from a Named Individual in order to submit a CCH check to the Ministry– Do you regularly engage a security consultant to independently test your website for vulnerabilities? (i.e. penetration testing[3])	◯ Yes ◯ No ◯ N/A	
11. Are your staff 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	
12. Are your staff aware of how to report a cyber security incident? Have all cyber security incidents have been disclosed and are appropriately managed?	◯ Yes ◯ No ◯ N/A	

[2] 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.
[3] 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

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

Statement	Acknowledgement Please indicate which most applies to your organisation	Comments
13. Do you regularly review user and administrator accounts and disable accounts you no longer require?	◯ Yes ◯ No ◯ N/A	
14. Are individual user accounts (not shared) used for logging onto systems and web services?	◯ Yes ◯ No ◯ N/A	
15. 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	
16. Can you monitor and log any external attempts to gain unauthorised access to your services or devices? (i.e. monitor attempts to breach firewalls[4], network devices, database applications, file access on shared drives)	◯ All ◯ Some ◯ None ◯ N/A	

[4] Firewall is a 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

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
Contract	The Contract for Online Delivery of Criminal Conviction Histories.	
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
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
Ministry	The Ministry of Justice.	
Obligations	A third party's obligations as outlined in the Privacy Act 2020 and regulations, the contract (including practice standards), professional obligations and any relevant policies and procedures.	
Organisation	A third party registered by the Ministry, at its discretion, who fulfils the Ministry's requirements in accordance with clause 3 of the Contract.	
Penetration testing	Technical testing by security consultants to find vulnerabilities that could be exploited by malicious parties, using similar penetration-testing tools and techniques that hackers use.	https://www.ncsc.gov.uk/guidance/
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 publications/restricting-the purposes of managing, configuring or managing access to administrative-privileges systems under their control.	https://www.cyber.gov.au/

Users	Organisation staff members that has been set up as a user in the online Criminal Conviction History Check service.
Web services	Services that are provided by other parties via the public internet.