Forensic Science Regulator
Overseeing Quality

Report

Advice from the National Cyber Security Centre on potential new text for the Control of Data section of the Regulator's Codes of Practice and Conduct

FSR-R-648

Issue 1

This is a consultation and therefore should not be regarded or used as a standard. This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication or incorporation into the final document. The consultation will run from 14 August 2019 to 21 October 2019. Comments should be sent to FSRConsultation4@homeoffice.gov.uk and should be submitted by 21 October 2019. This mailbox is not for general correspondence and is not routinely monitored so no acknowledgement will normally be sent.

1. PURPOSE

1.1.1 The Regulator is considering incorporating advice on data security received from the National Cyber Security Centre (NCSC) into the Codes of Practice and Conduct[1] and asks for the forensic science community to comment on the proposal and/or identify any significant practical challenges to implementation.

2. BACKGROUND

2.1.1 The Forensic Science Regulator's (the Regulator's) Codes of Practice and Conduct (the Codes) mainly contains high-level standards requirements which providers are free to interpret how to achieve. The Codes are only prescriptive when this is required (e.g. where there are legal requirements or on topics were there has been criticism in the past) such as validation.

2.1.2 A recent cyber security issue that significantly affected a forensic science provider has raised the question of whether the community requires more specific requirements covering the range of possible types of IT security.

2.1.3 The NCSC was asked to consider what specific requirements could be considered for future versions of the Codes (issue 5 is scheduled for imminent publication, so any agreed changes will be incorporated in issue 6); Annex A contains the advice as received, in the form of a suggested insertion into the Codes.

2.1.4 Although the incident that prompted review in the issue of data security did not appear to result in irrecoverable loss of data, access to a data storage device and/or theft of data, the advice from the NCSC also covers how these risks can be avoided, managed and/or recovered from.

2.1.5 It is not possible to assess the impact of implementation without seeking views from the community.

3. RISKS

3.1.1 In assessing the potential impact of additional security provisions, the impact of a beach of IT security must be borne in mind.

[1] Available from: www.gov.uk/government/collections/forensic-science-providers-codes-of-practice-and-conduct

3.1.2 The probable impacts of a breach of IT security include but are not limited to the following.

a. Challenges to data/System Integrity.

b. Personal Data.

c. Operations.

d. Criminal Justice System Impact.

e. Recovery.

3.1.3 An affected system must be taken to include all computers, IT devices and analytical systems connected to the computer or network which was breached.

4. REQUEST

4.1.1 The Regulator asks that all forensic science providers of any size, review their IT security as informed by the text in Annex A, to:

a. Determine and address weaknesses; and

b. Identify and feedback on any significant practical challenges to implementation.

4.1.2 Comments should be sent to FSRConsultation4@homeoffice.gov.uk and should be submitted by 21 October 2019.

ANNEX A

Draft Additional Text For Section 21 “Control Of Data” of the Forensic Science Regulator Codes Of Practice and Conduct (Issue 4)

21. CONTROL OF DATA [1, 2, 3, 4 5, 6]

21.1. GENERAL

21.1.1 The forensic unit shall be compliant with applicable data protection legislation and any other obligations placed upon them through policy, standards or contract schedules. The forensic unit’s management system shall ensure that all information, (electronic and physical): (1) is accurate; (2) can only be accessed by those who are authorised to do so; and (3) is available when needed. When no longer needed, information shall be destroyed in accordance with the forensic unit’s retention and destruction policy.

…

21.3 ELECTRONIC INFORMATION SECURITY [7]

21.3.1 The forensic unit shall have an information security policy which explains how it meets its responsibilities outlined in section 21.1.1. The information security policy shall describe the processes, based on assessed business and security requirements, for the management of electronic information. These processes, and the corresponding procedures, shall be subject to regular audit and review.

21.3.2 The forensic unit’s information security policy shall have processes for:

a. access control to electronic information. The access control process shall include procedures for the identification, authentication and authorisation of users. Users shall be granted minimum privileges to allow them to access only the information needed, or the key operational services they require to perform their roles. Access shall be removed when users leave their role or the organisation. Periodic reviews should also take place to ensure appropriate access is maintained. Users with administrative rights and/or access to sensitive information shall be authenticated using a second factor where this is technically possible. Accounts with administrative rights and/or access to sensitive information shall not be used for accessing Email or browsing the Internet – separate accounts shall be provided for this.

Unauthorised access requests shall be throttled or locked out after 5 -10 attempts and logged. Access management procedures shall be protected to prevent unauthorised system-wide access [8, 9];

b. the selection, use and management of passwords. The process for the selection, use and management of passwords shall include procedures for helping users generate better passwords. Users should use machine-generated passwords and have appropriate facilities to store them. The use of password managers for secure storage where appropriate should be encouraged. Alternatively, users should adopt the 'three random words [10]' technique for generating suitably complex and memorable passphrases. Regular password expiry should not be enforced however, users shall change their passwords when it is known (or suspected) that they have been compromised. Passwords that are used for personal accounts shall not be used for work accounts. Passwords shall not be reused for accounts with administrative rights and/or access to sensitive information. A blacklist of commonly used passwords should be created to prevent the most common (and therefore easily guessed) passwords being used. Password should be protected in transit and at rest using appropriate encryption techniques. All default administrative passwords for applications, network equipment and computers shall be changed [9];

c. protection against malware. The process for the protection against malware shall include procedures for detecting and removing it using anti-malware software. Anti-malware software shall be updated when new definitions become available. Where technically possible, anti-malware software shall be installed on all computers. The forensic unit should implement additional anti-malware procedures such as application/executable whitelisting. The forensic unit shall have procedures in place to protect from website and Email-borne malware, caused by drive-by download and phishing attacks. The forensic unit should access the Internet via a proxy service which blocks malware. The forensic unit should have procedures for filtering or blocking phishing Emails or messages, before they reach users. The forensic unit shall have procedures to regularly update (patch) software and firmware to the latest versions. Where this is not possible, then other mitigations (such as physical or logical separation) shall be applied. Software and firmware that is no longer supported by vendors, should be replaced. All removable media shall be scanned using anti-malware software before and after use. The forensic unit should securely configure computers by following the End User Device security principles [11]. The forensic unit shall have access to backups of electronic information so that they can easily recover from ransomware [12, 13];

d. management of removable storage media. The management of removable storage media process shall include procedures for its issue and use. Removable storage media shall only be issued to users whose role requires it. Only the interfaces necessary for the use of removable storage media should be enabled on computers. Personal removable storage media shall not be used for the transfer of electronic information – only officially issued removeable storage media shall be used. All officially issued removable storage media shall be physically secured when not in use, they should be stored in a locked desk or cupboard. Officially issued removable storage media shall not be taken offsite unless its contents are secured using appropriate encryption techniques. All officially issued removable storage media shall be subject to accounting which includes record of ownership, location, muster and destruction. The forensic unit should use alternatives to removable storage media for transferring electronic information such as Email or cloud services [8, 14];

e. the segregation of forensic networks. The forensic unit shall have procedures for the segregation of systems used for the investigation of crime, from other networks. Systems and data that do not need to communicate or interact with each other should be separated into different network segments, and only allow users to access a segment where needed. Segregation can be achieved physically or logically so long as the systems used for the investigation of crime shall not be accessible from other networks. Logical separation can include access control lists, network and computer virtualisation, firewalling, and network encryption such as Internet Protocol Security (IPSec) [15, 16];

f. backups, recovery and business continuity. The backup, recovery and business continuity process shall have procedures to recover from incidents such as ransomware, theft or hardware failure, whilst ensuring the business can continue to function. The forensic unit shall identify what electronic information is essential to keeping operations running and make regular daily/weekly backup copies. The forensic unit shall identify its critical systems and have redundancy arrangements in place. The forensic unit shall regularly test that backups are working to ensure they can restore the electronic information from them in the event of an incident. Backups shall be kept separately from computers and stored offline for as long as necessary to meet the requirements of the Criminal Justice System. The forensic unit should use cloud services to back up electronic information, or backups should be securely stored away from business premises. The forensic unit shall have an incident management plan which helps staff identify, respond to and recover from incidents as well as continue to run the business. The incident management plan should include a communication strategy, roles and responsibilities of staff and third parties such as service providers and authorities, as well as contact details for those involved. The forensic unit shall periodically test the incident management plan to ensure that its electronic information and critical systems can be recovered in the event of an incident, whilst ensuring that the business can continue to operate. Revisions to the incident management plan should include lessons learnt to ensure the same event cannot occur in the same way again [8, 14];

g. network security and mobile working. The network security and mobile working process shall include procedures for managing the network perimeter by using firewalls to create a ‘buffer zone’ between the Internet (and other untrusted networks) and the networks used by the business. The forensic unit shall have procedures to protect their internal networks by ensuring there is no direct routing between internal and external networks (especially the Internet). The forensic unit shall have procedures for securing wireless access. All wireless access points shall be appropriately secured, only allowing known devices to connect to corporate Wi-Fi services. Where mobile working is required, the forensic unit shall have procedures for ensuring that connections are identified, authenticated (preferably using multiple factors) and authorised. All electronic information which transits the Internet (and other untrusted networks) shall be protected from eavesdropping and alteration using appropriate encryption such as IPSec and Transport Layer Security (TLS). All mobile devices shall only have the necessary applications and electronic information to fulfil the business activity that is being delivered outside the normal office environment. If the mobile device supports it, data shall be encrypted at rest. The forensic unit should have procedures for monitoring network traffic for unusual incoming and outgoing activity that could be indicative of an attack. The forensic unit should have procedures for testing the security of its networks [8];

h. the use of cloud-based software services. The process for the use and deployment of cloud-based software services shall include procedures to evaluate the security of the 'Software as a Service' (SaaS) offering. The forensic unit should use SaaS providers which: (1) can clearly explain the security characteristics of their products; (2) protect data-in-transit between clients and the service; (3) use correctly configured certificates; (4) protect data-in-transit between microservices; (5) implement Application Programming Interface (API) authentication; (6) enforce privilege separation; (7) support multi-factor authentication; (8) log events and make these available to customers; and (9) have a clearly defined policy for patching internal systems as well as dealing with security issues [17].

REFERENCES

1. International Organization for Standardization, 2005. ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories, ref 5.4.7. [pdf] International Organization for Standardization. Available at: <www.iso.org/standard/39883.html> [Accessed 16 July 2019].

2. International Organization for Standardization, 2017. ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories, ref 7.11. [pdf] International Organization for Standardization. Available at: <www.iso.org/standard/66912.html> [Accessed 16 July 2019].

3. The Chartered Institute for Archaeologists, 2014. Standard and guidance for forensic archaeologists refs 2.2, 2.5 & 7.2. [pdf] The Chartered Institute for Archaeologists. Available at: <www.archaeologists.net/sites/default/files/CIfAS&GForensics_2.pdf> [Accessed 16 July 2019].

4. The Royal Anthropological Institute, 2018. Code of Practice for Forensic Anthropology refs 7.16, 7.17, 7.19 & 7.1.10. [pdf] The Royal Anthropological Institute. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/710249/2018_Code_of_Practice_for_Forensic_Anthropology.pdf> [Accessed 16 July 2019].

5. Consultation Draft 0.4, 2019. Code of Practice for Forensic Gait Analysis refs 6.2.1, 10.1.3, 11.1.2, 11.1.8 & 11.2.3. [To be published].

6. International Organization for Standardization, 2012. ISO/IEC 15189:2012 Medical laboratories -- Requirements for quality and competence refs 4.1.3, 5.4.6 d & 5.10.3. [pdf] International Organization for Standardization. Available at: <www.iso.org/standard/56115.html> [Accessed 16 July 2019].

7. Cabinet Office, 2018. Minimum Cyber Security Standard. [pdf] Her Majesty’s Government. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf> [Accessed 16 July 2019].

8. The National Cyber Security Centre, 2018. 10 Steps to cyber security. [online] Available at: <www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps> [Accessed 16 July 2019].

9. The National Cyber Security Centre, 2018. Password administration for system owners. [online] Available at: <www.ncsc.gov.uk/collection/passwords/updating-your-approach> [Accessed 16 July 2019].

10. The National Cyber Security Centre, 2016. Three random words or #thinkrandom. [online] Available at: <www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0> [Accessed 16 July 2019].

11. The National Cyber Security Centre, 2018. End user device (EUD) security guidance. [online] Available at: <www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles> [Accessed 18 July 2019].

12. The National Cyber Security Centre, 2018. Mitigation malware. [online] Available at: <www.ncsc.gov.uk/guidance/mitigating-malware> [Accessed 16 July 2019].

13. The National Cyber Security Centre, 2018. Phishing attacks: defending your organisation. [online] Available at: <www.ncsc.gov.uk/guidance/phishing> [Accessed 16 July 2019].

14. The National Cyber Security Centre, 2019. Small Business Guide: Response and Recovery. [online] Available at: <www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery> [Accessed 16 July 2019].

15. The National Cyber Security Centre, 2018. Preventing lateral movement. [online] Available at: <www.ncsc.gov.uk/guidance/preventing-lateral-movement> [Accessed 16 July 2019].

16. The Australian Cyber Security Centre, 2019. Implementing Network Segmentation and Segregation. [pdf] Australian Government. Available at: <www.cyber.gov.au/sites/default/files/2019-05/PROTECT%20-%20Implementing%20Network%20Segmentation%20and%20Segregation%20%28April%202019%29.pdf> [Accessed 16 July 2019].

17. The National Cyber Security Centre, 2018. Software as a Service (SaaS) security guidance. [online] Available at: <www.ncsc.gov.uk/collection/saas-security> [Accessed 18 July 2019].

ABBREVIATIONS

Abbreviation	Meaning
API	Application Programming Interface
EUD	End user device
IPSec	Internet Protocol Security
IT	Information Technology
NCSC	National Cyber Security Centre
SaaS	Software as a Service
TLS	Transport Layer Security

Published by:

The Forensic Science Regulator

5 St Philip's Place

Colmore Row

Birmingham

B3 2PW

www.gov.uk/government/organisations/forensic-science-regulator

ISBN: 978-1-78655-874-9