Forensic Science Regulator
Overseeing Quality

**FSR Regulatory Notice 02/2020**

**Planned update for the “Control of Data” section of the Forensic Science Regulator Codes of Practice**

| | |
|---|---|
| **Issue date: 01/08/2020** | **Effective date: 01/08/2020** |

**Previous notice(s) which are amended/withdrawn by this notice being issued: None**

## Issue

1. The Forensic Science Regulator's (the Regulator's) Codes of Practice and Conduct (the Codes) mainly contains high-level standards requirements which forensic units 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 where there has been criticism in the past) such as validation.

2. Following a cyber security issue that significantly affected a forensic science provider and the Criminal Justice System, the National Cyber Security Centre (NCSC) advised that more specific requirements covering IT security were required.

3. The NCSC prepared draft text which was published for consultation in 2019. The comments received during the consultation have been considered by the Regulator and the Quality Standards Specialist Group, in collaboration with the NCSC, and by the Forensic Science Advisory Council. As a result, it is the intention of the Regulator that the provisions in Annex A of this Regulatory Notice [1] will be incorporated into the section on control of data in a future version of the Codes.

4. To assist easy read across, the section numbering in Annex A is based upon that of issue 5 of the Codes, although the Codes and therefore any text incorporated may be subject to revision and the final text will reflect the structure, numbering and style of the Codes at the time of incorporation.

5. The entire of section 23.3 Electronic information security is replacement text and is marked as such in grey in Annex A. There are no changes proposed at this time to the text in 23.1 General, but it is referred to by the new text so is included for ease of reference. The section titled 23.2 Electronic information capture, storage, transfer, retrieval and disposal is not referred to in the new text, there are no changes proposed and so only the heading is reproduced as a place marker.

6. This Regulatory Notice is issued so that all forensic units, of whatever size, can make amendments to their systems as required prior to the text being incorporated within the Codes.

[1] The intention is that the text as provided will be incorporated into the Codes; it is, however, as the Codes is a ‘living’ document it is possible that update(s) may be required.

# Annex A: Planned text for the “Control of Data” section of the Forensic Science Regulator Codes of Practice and Conduct (section 23 in Issue 5)

## 23. Control of Data

### 23.1 General

[Note: No fundamental changes to this sub-section from Issue 5 of the Codes, however the text is reproduced in this Regulatory Notice for ease of cross reference only.

23.1.1 The forensic unit shall have procedures within its management system to ensure that all necessary information is recorded accurately, maintained so that its authenticity and integrity is not compromised, and is retained and destroyed in accordance with the forensic unit’s retention and destruction policy. [1] [2] [3]

23.1.2 The unit shall identify key data and critical control points (i.e. places where data is entered, transferred, stored or processed in a manner where it may be vulnerable to corruption, errors, unauthorised manipulation etc.). [2]

23.1.3 The unit shall identify protection steps to:

a. minimise the risk of data loss;

b. minimise the risk of data corruption (deliberate, degraded, actual or suspected);

c. demonstrate that the results are reliable and analytically sound; and

d. maintain continuity and prevent unauthorised access to and/or amendment of all electronic records identified by assessment of the critical control points of key data.

23.1.4 Protection steps shall be tested by sampling of key data. [3]

### 23.2 Electronic Information Capture, Storage, Transfer, Retrieval and Disposal [4]

[Note: No fundamental changes to this sub-section proposed; new text does not cross reference to this sub-section, so it is not reproduced here.]

[2] This critical control point approach is advocated in guidance issued by the Regulator for assessing the risk of cognitive bias as a result of information flow as well as for assessing contamination and therefore the process mapping may be used for assessment of these and other risks in the process.

[3] Assessment of what is key data should be risk based, and process mapping to look at data flow through each process and identify critical control points would be an appropriate assessment of what stages in the process require specific protection steps to prevent loss, corruption and unauthorised access.

[4] Further information and guidance can be found in BS 10008:2014, Evidential weight and legal admissibility of electronic information – Specification.

## 23.3 Electronic Information Security [4]

23.3.1 The forensic unit shall have an information security policy which explains how it meets its responsibilities outlined in section 23.1.1. [5] , [6] The information security policy shall describe the procedures, based on assessed business and security requirements, for the management of electronic information. These procedures shall be subject to regular testing, audit and review by the forensic unit and/or their IT provider.

23.3.2 The forensic unit's information security policy shall have processes for the following.

### Access Control to Electronic Information

23.3.3 The access control procedures shall include the identification, authentication and authorisation of users. Users shall be granted minimum privileges to allow them to access only the information needed, and the key operational services they require to perform their roles.

23.3.4 Access shall be removed when users leave their role or the organisation. Reviews should take place at least every 6 months to ensure access rights are still needed - if access rights are no longer needed, they shall be removed. Users with administrative rights shall be authenticated using a second factor [7] where this is technically possible.

23.3.5 Accounts with administrative rights shall only be used to perform administrative duties and shall not be used to access e-mail or the Internet - separate accounts shall be provided for this.

23.3.6 Authentication failures should be throttled to 10 attempts in 5 minutes or locked out where this is practically possible. Access control mechanisms shall be protected to prevent unauthorised system-wide access. [5] [6]

### The Selection, Use and Management of Passwords

23.3.7 Procedures for the selection, use and management of passwords should be formulated to help users to generate better passwords. The procedures shall include the following.

a. Users should use machine-generated passwords and have appropriate facilities to store them.

b. Password managers [7] for the secure storage of passwords should be used where appropriate. Alternatively, users should adopt the 'three

[5] Should it be required, and relevant, more detailed good practice guidance can be obtained from BS ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements and BS ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management.

[6] Further guidance is available from the publication: Cabinet Office. Minimum Cyber Security Standard. Her Majesty's Government. Available at: www.gov.uk/government/publications/the-minimum-cyber-security-standard [Accessed 04/03/2020].

[7] Second factor authentication or two-factor authentication (often shortened to 2FA) is something that the user (and only the user) can access, such as a code that is sent by text message, or that is created by an application or dongle. Further information is available from: www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa [Accessed 01/04/2020].

random words [8]' technique for generating suitably complex and memorable passphrases.

c. Passwords shall be a minimum of 8 characters and have no maximum length. Regular password expiry should not be enforced. However, users shall change their password when it is known (or suspected) that it has been compromised.

d. Users should be educated to not use the same passwords for personal and work accounts.

e. Passwords shall not be reused for accounts with administrative rights.

f. Users should be prevented from selecting easily guessed or commonly used passwords [9].

g. Password should be protected in transit and at rest using appropriate encryption and hashing techniques. [6] [10] [11]

h. All default administrative passwords for applications, network equipment and computers shall be changed [6], and meet the requirements identified above.

**Protection Against Malware**

23.3.8 With the exception of evidence handling where the detection or removal of malware may have an impact or potential impact on the results of examinations or analysis, the procedures for the protection against malware shall include detection and removal of malware using anti-malware software.

23.3.9 Anti-malware software shall be updated when new definitions become available. Anti-malware updates should be overseen by the forensic unit's change procedures to manage any potential impact to the forensic examination process.

23.3.10 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 allow listing. [12]

23.3.11 The forensic unit shall have, or ensure that its IT provider has, procedures in place to protect from website and email-borne malware, caused by drive-by download and phishing attacks.

23.3.12 The forensic unit shall access the Internet via a proxy service which blocks malware. The forensic unit shall have procedures for filtering or blocking phishing Emails or messages, before they reach users. The forensic unit shall have procedures to update (patch) software and firmware in a timely manner overseen by the forensic unit's change procedures to manage any potential impact to the forensic examination process. Software and firmware that is no longer supported by vendors, should be replaced unless there is a technical or CJS justification for its continued use recorded in the procedure. [8] 'Critical' and 'High' severity patches for Internet-enabled systems shall be installed as soon

[8] For example, legacy software is sometimes required to access old media or for revisiting the analysis of old cases.

as is feasibly possible. Where this is not possible, then other mitigations (such as physical or logical separation) shall be applied.

23.3.13 All removable storage media shall be scanned using anti-malware software before use. The forensic unit should securely configure computers by following the End User Device security principles [13]. The forensic unit shall have access to offline backups of electronic information so that it can recover from a ransomware attack [14] [15].

**Management of Removable Storage Media**

23.3.14 The management of removable storage media procedures shall include its issue and use.

23.3.15 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.

23.3.16 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. Officially issued removable storage media should not be taken offsite unless its contents are secured using appropriate encryption techniques [16]. All officially issued removable storage media should be subject to accounting with the aim of tracking use and managing loss [5] [17].

**The Segregation of Forensic Networks**

23.3.17 The forensic unit shall have procedures for the segregation of systems used for forensic science work, 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.

23.3.18 Logical separation can include access control lists, network and computer virtualisation, firewalling, and network encryption such as Internet Protocol Security (IPSec) [18] [19].

**Backups, Recovery and Business Continuity**

23.3.19 The forensic unit shall have procedures for backup, recovery and business continuity to recover from incidents such as ransomware, theft or hardware failure, whilst ensuring the business can continue to function.

23.3.20 Where digital data is the evidence, the procedure should be risk-based, balancing consideration of the time between creation of the extracted material, retention of the evidential device and any identified off-site back-up requirement.

23.3.21 The forensic unit shall identify what electronic information is essential to keeping operations running and make regular backup copies, or where that infrastructure is provided by the larger organisation (e.g. police force) seek assurance the backup is adequate.

23.3.22 The forensic unit shall identify its critical systems and have redundancy arrangements in place. The forensic unit shall test that backups are working to ensure it can restore the electronic information from them in the event of an incident. Offline backups shall be created and stored for as long as necessary to meet the requirements of the Criminal Justice System.

23.3.23 Offline backups should be stored at a separate and secure location [9] [20] [21]. The forensic unit may use appropriate cloud services [22], for the online back-up of electronic information. [10]

23.3.24 The forensic unit shall have an incident management plan [11] 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.

23.3.25 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. [5] [17] [23]

**Network Security and Mobile Working**

23.3.26 The network security and mobile working procedures shall include the management of 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.

23.3.27 The forensic unit shall have procedures to protect its 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 to its networks. All wireless access points shall be secured using Wi-Fi Protected Access2 (WPA2) or WPA3, and only allow known devices to connect to corporate Wi-Fi services.

23.3.28 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). [10] [11]

23.3.29 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 ensure there are adequate

[9] Separate location means a separate building not merely a separate room. Exceptions to this requirement will be rare, but may include forensic units with specific high security requirements. Back-ups also need to be secured from potential malware or ransomware attacks so offline backup is expected. Sole traders may enter into reciprocal storage agreements if they choose to.

[10] There are situations where it may not be appropriate to use some cloud services for specific systems or data, partially if the data is evidential as there are legislative or jurisdictional requirements about where data is stored or where it travels through.

[11] This may be part of the overall business continuity and disaster recovery plan or a separate IT incident management plan.

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. [5]

**The Use of Cloud-Based Services**

23.3.30 The process for the use of cloud-based services shall include procedures to:

a. determine the business need and end-user requirements;

b. identify what data and information will be transported, stored and processed, and understand the associated risks;

c. evaluate the security of the offering; and

d. understand the residual risks and how these will be managed.

23.3.31 The forensic unit should use cloud providers which meet the NCSC's cloud security principles. [22] The storage and processing of evidential data and information using cloud-based services should only be performed from data centres physically located in the UK. The forensic unit should periodically review whether the cloud-based services still meet their business and security needs.

**Security Monitoring and Situational Awareness**

23.3.32 The security monitoring and situational awareness procedures shall include the generation, capture, retention, storage and analysis of logs from its computers and network equipment. The forensic unit's security monitoring procedures shall:

a. provide visibility of communication between their network and other networks (i.e. the Internet or 3rd party suppliers);

b. capture authentication and access attempts; and

c. provide asset and configuration information. All logs shall be stored securely so they are safe from tampering and unauthorised access. All logs should be stored for a minimum of 6 months so that they can be used to support incident management. [24] [25]

End of planned text for the “Control of Data” section of the Forensic Science Regulator Codes of Practice and Conduct issue 6.

As a result of the new text for issue 6, the following additions to the sections 29. Bibliography, 30. Acronyms and abbreviations and 31. Glossary will be considered when incorporated and/or are already in the Codes but are included here for clarity (based upon issue 5 numbering). The referencing convention in place in the Codes at the time of incorporating the text will be used.

# 29. Bibliography

[1] The National Cyber Security Centre, “Secure Sanitisation of Storage Media,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media. [Accessed 24 June 2020].

[2] The Centre for the Protection of National Infrastructure, “Secure Destruction,” 2019. [Online]. Available: www.cpni.gov.uk/secure-destruction. [Accessed 24 June 2020].

[3] The National Cyber Security Centre, “Acquiring, managing, and disposing of network devices,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/acquiring-managing-and-disposing-network-devices. [Accessed 24 June 2020].

[4] Cabinet Office, “Minimum Cyber Security Standard,” 2018. [Online]. Available: www.gov.uk/government/publications/the-minimum-cyber-security-standard. [Accessed 24 June 2020].

[5] The National Cyber Security Centre,, “10 Steps to cyber security,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps. [Accessed 24 June 2020].

[6] The National Cyber Security Centre,, “Password administration for system owners,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/passwords/updating-your-approach. [Accessed 24 June 2020].

[7] The National Cyber Security Centre, “Password manager buyers guide,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/passwords/password-manager-buyers-guide. [Accessed 24 June 2020].

[8] The National Cyber Security Centre, “Three random words or #thinkrandom,” 2016. [Online]. Available: www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0. [Accessed 24 June 2020].

[9] The National Cyber Security Centre, “Passwords, passwords everywhere,” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere. [Accessed 24 June 2020].

[10] The National Cyber Security Centre, “Using TLS to protect data 2017,” 2017. [Online]. Available: www.ncsc.gov.uk/guidance/tls-external-facing-services. [Accessed 24 June 2020].

[11] The National Cyber Security Centre, “Using IPSec protect data,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/using-ipsec-protect-data. [Accessed 24 June 2020].

[12] N. C. S. Centre, “National Cyber Security Centre,” 30 04 2020. [Online]. Available: www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white. [Accessed 30 06 2020].

[13] The National Cyber Security Centre, “End user device (EUD) security guidance,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/eud-security-principles. [Accessed 24 June 2020].

[14] The National Cyber Security Centre, “Mitigation malware,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/mitigating-malware. [Accessed 24 June 2020].

[15] The National Cyber Security Centre, “Phishing attacks: defending your organisation,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/phishing. [Accessed 24 June 2020].

[16] The National Cyber Security Centre, “Products & Services,” 2020. [Online]. Available: www.ncsc.gov.uk/section/products-services/all-products-services-categories?&start=0&rows=20. [Accessed 24 June 2020].

[17] The National Cyber Security Centre, “Small Business Guide: Response and Recovery,” 2019. [Online]. Available: www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery. [Accessed 24 June 2020].

[18] The National Cyber Security Centre, “Preventing lateral movement,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/preventing-lateral-movement. [Accessed 24 June 2020].

[19] The Australian Cyber Security Centre, “Implementing Network Segmentation and Segregation,” 2019. [Online]. Available: www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation. [Accessed 24 June 2020].

[20] The National Cyber Security Centre, “Offline backups in an online world,” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world. [Accessed 24 June 2020].

[21] The National Cyber Security Centre,, “Mitigation malware and ransomware attacks,” 2020. [Online]. Available: www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks. [Accessed 24 June 2020].

[22] The National Cyber Security Centre, “Cloud Security Guidance Implementing the Cloud Security Principles,” 2018. [Online]. Available: www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles. [Accessed 24 June 2020].

[23] The National Cyber Security Centre, “Incident Management,” 2019. [Online]. Available: www.ncsc.gov.uk/collection/incident-management. [Accessed 24 June 2020].

[24] The National Cyber Security Centre, “Introduction to logging for security purposes,” 2018. [Online]. Available: www.ncsc.gov.uk/guidance/introduction-logging-security-purposes. [Accessed 24 June 2020].

[25] The National Cyber Security Centre, “Logging made easy (LME),” 2019. [Online]. Available: www.ncsc.gov.uk/blog-post/logging-made-easy. [Accessed 24 June 2020].

[26] The National Cyber Security Centre, “Acquiring, managing, and disposing of network devices.,” 2016. [Online]. Available: www.ncsc.gov.uk/guidance/acquiring-managing-and-disposing-network-devices. [Accessed 24 June 2020].

## 30. Acronyms and Abbreviations

**API**

Application Programming Interface.

**IPSec**

Internet Protocol Security.

**SaaS**

Software as a Service.

**TLS**

Transport Layer Security.

**Wi-Fi**

A local area network that uses high frequency radio signals.

**WPA2**

Wi-Fi Protected Access 2.

**WPA3**

Wi-Fi Protected Access 3.

## 31. Glossary

**Encryption**

The process of converting data in such a way making it unintelligible to all but authorised parties.

**Hashing**

Using a mathematical function to generate a value or values from a string of data.

**Malware**

Malicious software.

**Ransomware**

A form of malware designed to block access to a computer system until a fee is paid.

**Second factor authentication**

Two-factor authentication (often shortened to 2FA) provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services or important accounts, the 'second factor', which is something that you (and only you) can access. This could be a code that is sent to you by text message, or that is created by an app.

**Shall**

Indicates a requirement set in the standard or Codes.

**Should**

Indicates generally accepted practice in the forensic science profession.

**Throttled**

A control set by a system administrator e.g. to reduce user available bandwidth, the number of access attempts etc.