**Instructions for Using the Template**

1. Please complete this UKAS FSR Codes of Practice and Conduct (Issue 7) Gap Analysis form and submit to Kimberley Brumpton (kimberley.brumpton@ukas.com) by the **22nd June 2021**.
2. Please make an entry below confirming your state of compliance with each clause. If you are currently compliant please indicate where in your management system the clause is addressed and reference any relevant supporting documentation. If your management system is non-compliant, or is currently working towards compliance, please choose the appropriate answer from the drop-down list but detail what actions you plan to take to address the gap and the **associated timescale** for completion.
3. The information detailed below should be more than just a reference to the documented procedure and should explain what is in place to confirm compliance, what has been changed and any related actions taken by the laboratory.
4. The greyed-out boxes are for UKAS use only. Please do not enter any information in these boxes.
5. The provision of documents will not be evidence of our assessment of your compliance, but they may be reviewed if required.
6. Management approval confirming that the information provided is accurate and that any timescales for completion of actions to address any gaps are achievable is required on the completed Gap Analysis; this should be evidenced by a signature below.
7. Please continue to update your UKAS FSR Codes of Practice and Conduct (Issue 7) Gap Analysis form with any updates / progress and re-submit this one month before your annual routine assessment.

As a result of the assessment of your completed Gap Analysis further actions may be instigated by UKAS e.g. a more detailed desktop review.

All information provided in your Gap Analysis will be reviewed at your next assessment.

**Please note**: should it be identified that any of the information provided on this Gap Analysis is false then this may prompt UKAS to review the accreditation status of your organisation and could result in the application of sanctions, which may include the suspension of accreditation.

|  |
| --- |
| **Declaration to be completed by management.** |
| I confirm to that the information provided below is an accurate reflection of the current status of this organisation.  |
| **Signed:**  |
| **Name and position within the organisation (printed):**  |

|  |  |  |
| --- | --- | --- |
| **TO BE COMPLETED BY LABORATORY** |  | **TO BE COMPLETED BY UKAS ASSESSORS** |
| **Organisation Name** |  |  | **Assessment Manager** |  |
| **UKAS Accreditation Number** |  |  | **Assessment Team Members & Roles** |  |
| **Completed by** |  |  | **Date(s) of review** |  |
| **Date of Completion** |  |  | **Issue Date** |  |

| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| --- | --- | --- | --- |
| **CLAUSE** |
| 23.3.1The forensic unit shall have an information security policy which explains how the unit meets its responsibilities outlined in section 23.1.1 (see note, below). The information security policy shall describe the procedures, based on assessed business and security requirements, for the management of electronic information. The forensic unit shall ensure procedures are subject to regular testing, audit and review.NOTE: Clause 23.1.1 requires that 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. | Choose an item. | ***Example:*** ***Actions taken:*** *A risk assessment has been undertaken of all information security processes. A number of changes have been identified and these will be detailed under the relevant clauses below* *Current Info Sec Policy IS1234 has been updated to include a requirement for annual penetration testing of the forensic network and a need to monitor results of internal Force monitoring exercises.* *Internal audit schedule has been updated and all required audits have been completed****Actions to be taken:*** *1. Schedule for annual testing of information security procedures to be planned. To include pen testing; process review; and internally developed vulnerability testing.**Timescale 1 month.* *2. Identify and assess external suppliers of penetration testing.* *Timescale: 1 month.* *Etc….*  | *Example:**InfoSec SOP IS1234 documents current info audit schedule covers required aspects: , including access control, password management, malware, removable storage media, network segregation, backups, network security and security monitoring.* *The organisation does not use any cloud-based services.**Audits #15 completed in Jan 21 covers access control, password management and removable storage media,* *Audit #19 completed in April 2021 covers malware, network segregation, backups, network security and security monitoring.* *Etc.*  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.1:**  |

|  |  |
| --- | --- |
| **23.3.2** | **The forensic unit’s information security policy shall have processes for the following.** |
| **Access Control to Electronic Information** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |
| 23.3.3 | The access control procedures shall include the identification, authentication, and authorisation of users. Users shall have defined privileges which limit, as far as practical, access to only the information needed and the key operational services they require to perform their roles. | Choose an item. |  |  |
| 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. | Choose an item. |  |  |
| 23.3.5 | Users with administrative rights shall be authenticated using a second factor 87 where this is technically possible. | Choose an item. |  |  |
| 23.3.6 | 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. | Choose an item. |  |  |
| 23.3.7 | Authentication failures should be throttled to 10 attempts in 5 minutes or locked out where this is practically possible as per industry norms. Access control mechanisms shall be protected to prevent unauthorised system-wide access. | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.3 – 2.3.7:** |

|  |
| --- |
| **The Selection, Use and Management of Passwords** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |
| 23.3.8 | 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: | Choose an item. |  |  |
| 23.3.8a | Users should use machine-generated passwords and have appropriate facilities to store them. |  |  |  |
| 23.3.8b | Password managers for the secure storage of passwords should be used where appropriate. Alternatively, users should adopt the 'three random words' technique for generating suitably complex and memorable passphrases. | Choose an item. |  |  |
| 23.3.8c | Passwords shall be a minimum of 8 characters and have no maximum length. Regular password expiry should not be enforced, users shall change their password when it is known (or suspected) that it has been compromised. | Choose an item. |  |  |
| 23.3.8d | Users should be educated to not use the same passwords for personal and work accounts. | Choose an item. |  |  |
| 23.3.8e | Passwords shall not be reused for accounts with administrative rights. | Choose an item. |  |  |
| 23.3.8f | Users should be prevented from selecting easily guessed or commonly used passwords. | Choose an item. |  |  |
| 23.3.8g | Password should be protected in transit and at rest using appropriate encryption and hashing techniques. | Choose an item. |  |  |
| 23.3.8h | All default administrative passwords for applications, network equipment and computers shall be changed, and meet the requirements identified above. | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.8** |

|  |
| --- |
| **Protection Against Malware** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.3.9 | With the exception of evidence handling where the detection or removal of malware may have an actual 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. | Choose an item. |  |  |
| 23.3.10 | Anti-malware software shall be updated when new definitions become available. Anti-malware updates should be included in the forensic unit's change procedures to manage any potential impact to the forensic examination process. | Choose an item. |  |  |
| 23.3.11 | Anti-malware software shall be installed on all compatible computers and hardware, unless specified operational requirements dictate otherwise. The forensic unit should implement additional anti-malware procedures such as application/executable allow listing. | Choose an item. |  |  |
| 23.3.12 | 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. | Choose an item. |  |  |
| 23.3.13 | 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. | Choose an item. |  |  |
| 23.3.14 | The forensic unit shall have procedures to update (patch) software and firmware in a timely manner and included in the forensic unit's change procedures to manage any potential impact to the forensic examination process. | Choose an item. |  |  |
| 23.3.15 | 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. 'Critical' and 'High' severity patches for Internet-enabled systems shall be installed promptly. Where this is not possible, then other mitigations (such as physical or logical separation) shall be applied. | Choose an item. |  |  |
| 23.3.16 | All removable storage media shall be scanned using anti-malware software before use. | Choose an item. |  |  |
| 23.3.17 | The forensic unit should securely configure computers by following the End User Device security principles. | Choose an item. |  |  |
| 23.3.18 | The forensic unit shall have access to offline backups of electronic information so that it can recover from a ransomware attack. | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.9 – 23.3.18:** |

|  |
| --- |
| **Management of Removable Storage Media** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.3.19 | Procedures for management of removable storage media shall include controls related to issue and use. | Choose an item. |  |  |
| 23.3.20 | Removable storage media shall only be issued to users whose role requires it. Only the minimum interfaces necessary for the use of removable storage media should be enabled on computers. | Choose an item. |  |  |
| 23.3.21 | Personal removable storage media shall not be used for the transfer of electronic information - only officially issued removeable storage media shall be used which: | Choose an item. |  |  |
| 23.3.21a | Shall be physically secured when not in use | Choose an item. |  |  |
| 23.3.21b | Should not be used to take data offsite unless its contents are secured using appropriate encryption techniques | Choose an item. |  |  |
| 23.3.21c | Should be subject to accounting with the aim of tracking use and managing loss | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.19- 23.2.21:**  |

|  |
| --- |
| **The Segregation of Forensic Networks** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.3.22 | 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.92 Segregation can be achieved physically or ‘logically’. Logical separation can include access control lists, network and computer virtualisation, firewalling, and network encryption such as Internet Protocol Security (IPSec) | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.22:**  |

|  |
| --- |
| **Backups, Recovery and Business Continuity** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.3.23 | The forensic unit shall have procedures for business continuity with an incident management plan including backup and retrieval of data, to recover from incidents such as ransomware, theft or hardware failure, whilst ensuring the business can continue to function. | Choose an item. |  |  |
| 23.3.24 | 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. | Choose an item. |  |  |
| 23.3.25 | 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. | Choose an item. |  |  |
| 23.3.26 | 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. | Choose an item. |  |  |
| 23.3.27 | Offline backups should be stored at a separate and secure location. The forensic unit may use appropriate cloud services for this back-up of electronic information; ‘offline’ here means digitally disconnected when not in use and designed to remain unaffected should any incident impact the live environment. | Choose an item. |  |  |
| 23.3.28 | 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. | Choose an item. |  |  |
| 23.3.29 | 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. | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.3.23 – 23.3.29:**  |

|  |
| --- |
| **Network Security and Mobile Working** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.3.30 | 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. | Choose an item. |  |  |
| 23.3.31 | 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. | Choose an item. |  |  |
| 23.3.32 | 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). | Choose an item. |  |  |
| 23.3.33 | 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 procedures for monitoring network traffic for unusual incoming and outgoing activity that could be indicative of an attack. The forensic unit shall have procedures for testing the security of its networks. | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.30 – 23.3.33:**  |

|  |
| --- |
| **The Use of Cloud-Based Services** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.3.34a | The process for the use of cloud-based services shall include procedures to determine the business need and end-user requirements. | Choose an item. |  |  |
| 23.3.34b | The process for the use of cloud-based services shall include procedures to identify what data and information will be transported, stored and processed, and understand the associated risks. | Choose an item. |  |  |
| 23.3.34c | The process for the use of cloud-based services shall include procedures to evaluate the security of the offering. | Choose an item. |  |  |
| 23.3.34d | The process for the use of cloud-based services shall include procedures to understand the residual risks and how these will be managed. | Choose an item. |  |  |
| 23.3.35 | The forensic unit should use cloud providers which meet the NCSC’s cloud security principles. 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. | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.34 – 23.3.35:**  |

|  |
| --- |
| **Security Monitoring and Situational Awareness** |
| **FSR Codes of Practice and Conduct (FSR-C-100, Issue 7)** | **Compliant?** | **What action have you taken or planned to take and the associated time scale?** | **Evidence of Compliance** **(e.g. reference to policy / procedure number)** |
| **CLAUSE** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23.3.36 | The forensic unit's security monitoring and situational awareness procedures shall include the generation, capture, retention, storage and analysis of logs from its computers and network equipment. | Choose an item. |  |  |
| 23.3.36a | The forensic unit's security monitoring procedures shall provide visibility of communication between their network and other networks (i.e. the Internet or 3rd party suppliers). | Choose an item. |  |  |
| 23.3.36b | The forensic unit's security monitoring procedures shall capture authentication and access attempts. | Choose an item. |  |  |
| 23.3.36c | The forensic unit's security monitoring procedures shall 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. | Choose an item. |  |  |
| **UKAS COMMENTS ON COMPLIANCE & REF TO FINDINGS 2.3.36:**  |

**Executive Summary:**

**Recommendation:**