Cabinet Office

Commercial Continuous Improvement Assessment Framework (CCIAF) Security Operating Procedures (SyOPs)

Introduction:

1. This document constitutes the Security Operating Procedures (SyOPs) for the Continuous Improvement Assessment Framework (CCIAF). This document has been issued by the System Security Officer (SSO) in accordance with Cabinet Office policy, and has been approved by the Ministry of Defence's DART Team. All personnel using CCIAF are to read, understand and comply with these SyOPs and no departure from or amendment to them is permitted unless the SSO gains prior authorisation.

2. Disciplinary action will be taken against those personnel who breach or ignore these orders. Any incident that has, or is likely, to compromise the security of the CCIAF tool is to be reported immediately to the System Security Officer (SSO) in accordance with Cabinet Office policy.

Scope:

3. The CCIAF has been established to promote continuous improvement in commercial practices across the Government Commercial Function (GCF), and the wider public sector. The CCIAF does this by establishing a framework which sets out what best practice looks like, enabling organisations to benchmark their commercial operations against these standards. The goal of the CCIAF is to enable organisations to share insights about areas of strength and areas with scope for development, lessons learned, and common challenges.

Terms and Conditions:

1. PARTIES

1.1 The Provider: The representing organisation using the platform

1.2 The Governing Organisation: Cabinet Office

2. DEFINITIONS AND INTERPRETATION

2.1 In this agreement the following words and expressions have the meanings given to them in this clause;

Sector Oversight Teams: For the NHS, this is NHS England and NHS Improvement; for Local Authorities, this is the Department for Levelling Up, Housing and Communities.

Agent: a person who has been legally empowered to act on behalf of the Provider

Data: non-personal data shared as part of the CCIAF activity

3. GOVERNING ORGANISATION DUTIES AND OBLIGATIONS

3.1 The Provider agrees the Data shared as part of the CCIAF activity will be used by the Governing Organisation for the purpose of senior management reporting and ministerial briefing(s) at a summarised level across Government. Specifically, in relation to section 3 this will include:

Cabinet Office

i The creation of a leadership report, submitted to the Chief Commercial Officer.
ii The creation of playback reports, tailored to each organisation.
iii To validate pipelines for procurement activities.
iv To validate the third-party spend of each organisation.
v To benchmark the providers activity against other providers undertaking the same activity.

3.2 The Governing Organisation will not publish data externally that identifies individual departments, nor will they share data that identifies individual departments, without prior agreement from the Provider.

3.3 The Governing Organisation will not share data the Provider provides in raw format including the submitted self-assessment forms or documented evidence beyond the Purpose prior agreement of the Provider.

3.4 The Provider agrees the Data shared can be shared with the relevant Sector Oversight Teams and Regulators as stipulated in the definitions. For Local Authorities, additional authorisation to share Data must be granted to The Governing Organisation by an Agent of the Local Authority, using the share data tick-box within the CCIAF platform

3.5 Neither this Agreement nor the supply of any information grants the Governing Organisation any licence, interest or right in respect of any intellectual property rights of the disclosure except the right to copy the Confidential Information solely for the Purpose.

4. PROVIDER'S DUTIES AND OBLIGATIONS

4.1 The Provider will provide the requested Data required for the Purpose of CCIAF assessment.

4.2 Where the Provider is required to undertake Peer Review of another named Provider for the Purpose, it agrees:

i It will not use the disclosed Information for any other purpose.
ii To keep the Data secure and not to disclose it to any party beyond the agents assigned the duties of peer review or bodies involved with carrying out the CCIAF function.
iii Will not copy or retain any Data from other Providers without prior consent by the original Provider(s) of the Data.
iv Will not print any documents uploaded by other Providers without prior consent by the original Provider(s) of the Data.

4.3 The undertakings in section 4 apply to all of the information disclosed by the Provider as part of the Purpose regardless of the way or form in which it is disclosed or recorded but they do not apply to:

i any information which is or in future comes into the public domain (unless as a result of the breach of this Agreement); or ii any information which is already known to the Recipient, and which was not subject to any obligation of confidence before it was disclosed to the Recipient by the Provider.

Cabinet Office

4.4 Nothing in this Agreement will prevent the Governing Organisation from making any disclosure of the Confidential Information required by law or by any competent authority.

4.5 The Provider will itself keep confidential and will use all reasonable endeavours to ensure that its agents, consultants and subcontractors keep confidential all information to which the Agreement relates.

Security Operating Procedures:

5. ACCEPTABLE USE:

5.1 All Users of the platform are to comply with the Cabinet Office Acceptable Use Policy. In summary Users are not to:

i Attempt to access areas where they are not authorised to access ii Attempt to damage the system to prevent its use iii Attempt to introduce software or hardware of any type without consent from the System Security Officer
iv Attempt to share credentials with unauthorised users and/or attempt to logon as someone else (or with credentials which you are not authorised to use). Users must not allow unauthorised users to observe their screen.
v Users must not allow any person to observe them entering their system access credentials (e.g., password).
vi Passwords used on the system must be created in line with the platform's password standard.
vii Users must invoke the screensaver before leaving their workstation unattended viii A User account must only be created with permissions commensurate to that User's business role, and are only to be enabled once a signed copy of these SyOPs have been received from the user.

6. CLASSIFICATION:

6.1 CCIAF is a controlled area accessible only to authorised users and may be used to share OFFICIAL SENSITIVE information. Information of a higher classification must not be placed on the CCIAF Tool in any form. If such information is identified, users should notify the Systems Security Officer (SSO) and their unit security officers immediately.

7. EMAIL & UPLOADED ATTACHMENTS:

7.1 Users are responsible for ensuring that all emails they send comply with the following rules: JSP 740 Acceptable Use Policy & JSP 440 Part 4 Section 1

7.2 Users may send emails and upload attachments that are OFFICIAL SENSITIVE to recipients located on the CCIAF tool. Users should note that unmarked information may still be sensitive and must be given the protection they think it merits, respecting any handling instructions which have been added.

7.3 If there is a need to send emails and upload data over the internet at OFFICIAL SENSITIVE it must be in accordance with the organisation who owns the data's policy/guidance.

Cabinet Office

7.4 Document files may contain previously deleted, Protectively Marked classified information hidden within the file. All documents to be attached should first be cut and pasted from the original document into a new file and the new file uploaded.

8. PLATFORM ROLES AND RESPONSIBILITIES

8.1 The roles and responsibilities of the CCIAF platform are detailed below:

CCIAF System Administrator - commercialstandards@cabinetoffice.gov.uk
Maintain patch levels of supporting software.

- Act as Senior User Manager
- Provides advice around acceptable use.

CCIAF Systems Security Officer (SSO) - commercialstandards@cabinetoffice.gov.uk

- Handles reports of any suspicious activity and/or misuse
- Deals with any security concerns

9. PASSWORDS

9.1 Passwords are controlled by CCIAF. Passwords must be a minimum of 8 characters and must be alphanumeric with upper and lower case. Passwords are reset every 3 months

9.2 Password resets are initiated by the user and use a challenge response setup during registration.

9.3 Users are also required to maintain and update their security question and answers.

9.4 Passwords are not to be shared with anyone or written down anywhere under any circumstances.

10. MONITORING AND AUDITING

10.1 Use of the CCIAF platform is, and will continue to be, subject to monitoring. Users are advised that system logs are checked on a regular basis in order to detect unauthorised or suspicious system and security events.

10.2 CCIAF administrators have the right to gain access to user accounts in case of an emergency or a legitimate legal/business requirement. A detailed request is to be provided by the requester of exactly what they are requesting access to and for what purpose. This must be agreed with the user's line manager and recorded for audit purposes. Once the access is granted the extraction of information must be carried out within legal guidelines and a 2 man rule must be followed. Depending on the circumstances, all reasonable attempts will be made to inform the user of the request to access their account. Access to their account is to be conducted by the users Line Manager or the delegated authority given by the Systems Security Officer (SSO).

Cabinet Office

10.3 Anyone suspected of breaching the Acceptable Use Policy or detected misusing their privileges through monitoring may be subject to disciplinary or even legal action.

11. ACCOUNT DEACTIVATION

11.1 User accounts will be deactivated by the CCIAF System Administrator, after 90 days has elapsed without a CCIAF system login. Users will be warned of this, by email, at least 14 days before deactivation.

11.2 Accounts can be considered for reactivation by contacting the CCIAF System Administrator