ANNEX  Security Policy for users accessing SFC and Privacy Statement

1.1. Terms of Service
SFC is a software application accessible via the Internet, developed and hosted by the European Commission. The objective of SFC is to facilitate electronic exchange of information between the Member States of the Union and the European Commission in the context of shared management ("The Service").

By using the SFC system user agree to be bound by the following terms and conditions (“Terms of Service”).

The European Commission reserves the right to update and change the Terms of Service. In that event you will be asked for your acceptance of the new terms. Any new features that augment or enhance the current Service, including the release of new tools and resources, shall be subject to the Terms of Service. Continued use of the Service after any such changes shall constitute your consent to such changes. You can review the most current version of the Terms of Service at any time at SFC website.

1.2. Security Policy for access from National Authorities

Authentication
Users must accurately provide full legal name in ECAS to open an account in SFC.

Each login will correlate to only one user. Accounts created are available only with a username and password.

Authorisation
Users will create its own ECAS account (or via National Liaisons Officers) and later they will be given specific access rights to SFC according to their role. National Liaisons and DG Liaisons Officers must assign roles to users according to their expected role in SFC. SFC Security model ensures that users have access only to the specific data they need according to their role in the application.

National Liaison Officers and DG Liaison Officers together with user support agents in SFC are the only ones that can manage user accounts and roles.

National Liaison Officers and DG Liaison Officers are only ones authorised to request the creation or deletion of user accounts.

Users are responsible for all actions done under the username and passwords attributed to them, (even when including those actions have been carried out by others who are using your username and password).
**Integrity**

The Commission ensures that SFC complies with the requirements applicable to all IT systems at EU level set out in Commission Decision C(2006)3602 on Security of Information Systems and its implementing rules. This means that appropriate technical security measures are integrated in the SFC system. In particular, authentication (a username/password combination) and access control mechanisms ensure confidentiality and integrity of the SFC system and the information it contains.

Information during transmission is protected by using Secure Sockets Layer (SSL) software, which encrypts information you input when signing on, uploading and downloading content to and from SFC.

In addition, each SFC user must implement organizational security measures applicable to the processing of personal data in accordance with national legislation. In particular, appropriate security measures must be applied to personal data extracted from and further processed outside SFC (e.g. in a printed report or otherwise archived outside SFC or stored in national systems).

Also users must implement appropriate measures to protect their access credentials:

- Login and password credentials must not be shared with others. Users are responsible for keeping your account login and password private.
- Users must not misrepresent other people or take on the identity/role of someone else while using the Service.
- Users may not use the Service for any illegal or unauthorized purpose. The role provided in SFC should be appropriate to the role user have in the national authority.
- In the event that users change their in their national authorities and this affects the role in SFC they must inform immediately National Liaison officers to make the corresponding update.
- In the event that users notice a security incident or come to the knowledge that an SFC account is used inappropriately or shared among different people users agree to notify their corresponding National Liaison officer or DG Liaison Officer.

**1.3. Privacy Statement**

This privacy statement covers the part of SFC for which the Commission is responsible, i.e. the collection, registration, storage and deletion of personal data of SFC users (i.e. natural persons working on behalf of Member States in national authorities, European Commission desktop officers, National Liaisons officers, European Commission staff working in the operation and support of SFC, DG Liaisons officers). Thus it does not concern those data processing acts which fall under the responsibility of Member States.

All processing acts within the responsibility of the European Commission are governed by Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

The Commission collects the necessary contact details of the. These personal data are stored on a Commission database.
The following data is required:

- First name
- Last name
- E-mail address
- Preferred language
- Telephone, fax and additional information only when specified by the data subject (optional)
- Business details (name, address, country, type and code) in regards to users
- Authority details (name, address, country and code) in regards to Member State and Accession Country Administrators

The Commission needs to have access to contact details of SFC users in order to cooperate effectively with the Member States on shared management. Examples of such interactions are the notifications of failure of the system, reminders of actions that should be taken or notification of specific events to which users are subscribed.

These contact details may be processed for purposes compatible with the provision of the service, including monitoring of the use of the system by DG and National Liaisons Officers and the Commission, communication, training and awareness-raising initiatives, and gathering information required for the exchange of information.

The Commission supplies and manages the software and IT infrastructure for SFC, ensures the security of SFC, and is involved in the training of and technical assistance to SFC users. The Commission only has access to such personal data that are strictly necessary to carry out its tasks and provision the service.

Personal data of SFC users (staff working for the national authorities) will be stored as long as they continue to be users of SFC.

When natural persons cease to be SFC users, their personal data shall be blocked (i.e. made inaccessible via the normal interface of SFC by technical means). These data may only be processed for purposes of proof of an information exchange and will be deleted when it is no longer required for audit purposes.

Anonymous information might continue to be kept in SFC for statistical purposes.

Data kept in ECAS will be kept according to the specific privacy statement of ECAS.

Users can access their personal data directly via the ECAS and SFC applications. Further access to data stored for audit purposes can be done by contacting SFC support service. (See below)

In addition to these Privacy Statements the 'important legal notice' applies.

http://ec.europa.eu/geninfo/legal_notices_en.htm#personaldata

and concerning ECAS

https://webgate.ec.europa.eu/cas/privacyStatement.html
1.4. Web Services considerations:

Data Sending and Validation

According to Article 3(2) of Commission Implementing Regulation (EU) No 184/2014, “any transmission of information to the Commission shall be verified and submitted by a person other than the person who entered the data for that transmission. This separation of tasks shall be supported by SFC2014 or by Member State’s management and control information systems connected automatically with SFC2014.”

SFC2014 enforces the "four-eyes" principle, which means that the user who last validated an Operational Programme cannot submit it. Two different users are required; one to validate and another to send. In the case of the SFC2014 graphical user interface, this control is made by the SFC system itself. Given the impossibility to implement the four eyes principle in a machine to machine interface, when accessing SFC2014 via Web Services, each member state should take care of the implementation of the "four-eyes" principle internally in its own information system.

Sample Application

The SDK/Sample Application provided by the European Commission is a sample source code delivered "as is", it is provided as an example showing a possible integration with the SFC2014 web services based on a particular technology.

At any time without prior notice, the European Commission may make changes to the software.

Without limiting the foregoing, the European Commission makes no warranty that:

- The software will meet your requirements.
- The software will be uninterrupted, timely, secure or error-free.
- The results that may be obtained from the use of the software will be effective, accurate or reliable.
- The quality of the software will meet your expectations.
- Any errors in the software obtained from the sample application will be corrected.

The SDK and its documentation made available on the portal:

- Could include technical or other mistakes, inaccuracies or typographical errors.
- It will be only available on a specific technology
- Not all Webservices will have an associated SDK
- Errors will be corrected on a best effort basis.
- May be out of date and the European Commission makes no commitment to update such materials.
1.5. Cookies Directive
All the cookies are used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, and they are only used when is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”.

Cookies inventory

<table>
<thead>
<tr>
<th>Name</th>
<th>Service</th>
<th>Purpose</th>
<th>Cookie type and duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drupal.tableDrag.showWeight</td>
<td>Corporate content management platform, based on Drupal open source software</td>
<td>user interface preference</td>
<td>First-party persistent cookie, 1 year</td>
</tr>
<tr>
<td>_pk_id#</td>
<td>Corporate web analytics service, based on Matomo open source software</td>
<td>Recognises website visitors (anonymously – no personal information is collected on the user).</td>
<td>First-party persistent cookie, 13 months</td>
</tr>
<tr>
<td>_pk_ses#</td>
<td>Corporate web analytics service, based on Matomo open source software</td>
<td>Identifies the pages viewed by the same user during the same visit. (anonymously – no personal information is collected on the user).</td>
<td>First-party persistent cookie, 30 minutes</td>
</tr>
<tr>
<td>sfcsite_stick_to_https</td>
<td>ECAS</td>
<td>Determines whether user logs in via SSL secure connection.</td>
<td>First-party persistent cookie, deleted after you quit your browser</td>
</tr>
</tbody>
</table>
| SESS[Unique ID]             | Corporate content management platform, based on Drupal open source software | • his is used to distinguish users and has an expiration of 2-years.  
• This stores the Client ID.  
• lient ID: a unique, randomly generated string that gets stored in the browsers cookies, so subsequent visits to the same site can be associated with the same user.  
• his will not store any user information. | First-party persistent cookie, 10h |
| has_js                      | Corporate content management platform, based on Drupal open source software | Determines whether Javascript is enabled in your browser. This allows our websites to function properly. | First-party persistent cookie, deleted after you quit your browser |
| eu_cookie_consent           | Cookie consent kit                                                     | Stores your cookie preferences (so you won’t be asked again)                                | First-party persistent cookie, deleted after you quit your browser |

Source: https://ec.europa.eu/info/cookies_en

1.6. Contact Addresses:

Support
sfc2007-info@ec.europa.eu
ec-sfc2014-info@ec.europa.eu
Contacts for each DG involved in SFC:

DG AGRI
http://ec.europa.eu/agriculture/contact/index_en.htm

DG EMPL

DG HOME
http://ec.europa.eu/dgs/home-affairs/who-we-are/contact-us/index_en.htm

DG MARE
http://ec.europa.eu/fisheries/about_us/contacts/index_en.htm

DG REGIO

Contact for European Data Protection Supervisor and national data protection authorities
http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Contact/pid/156

http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm