May 2019

EISF Information Sharing Policy & Protocol

All EISF Full and Associate Members and EISF Affiliates agree to the terms of this Information Sharing Policy as a condition of their membership and/or engagement with EISF.

EISF Information Sharing Policy

1. Confidential Information Sharing

1.1 EISF Members, including all registered HQ and regional SFPs, and EISF Affiliates agree to share information on security related issues with the EISF membership directly through the EISF_Chat and/or to the EISF Executive Director (or delegated Secretariat staff), for dissemination to the wider EISF Membership. If required, EISF will take agreed measures to anonymise information shared via the Secretariat to the extent necessary.

This may entail, among other things, a) removing all names and identifiers such as location from the information; b) removing all email addresses; and c) in certain cases collating this information with other similar information to make it anonymous.

The Criteria for deciding whether the information is to be anonymised are as follows:

- has the person who passed on the information requested that the information be made confidential?
- does it contain incriminating information (e.g. causes reputational risk)?
- does it contain information that could put people's lives at risk?

Areas for information sharing include, but are not limited to:

- policy, standard operating procedures (SOP) and contingency planning documents
- context analysis
- incident reports and details
- training and other support activities

1.2 All EISF Members and Affiliates agree that they will disseminate any information they receive, through EISF emails, EISF website, EISF_Chat or EISF events, respectfully and discreetly.

1.3 All information shared by members and registered guests on the EISF_Chat facility is shared under Chatham House rule, meaning that participants are free to use the information received, but neither the identity nor the affiliation of the writer(s), nor that of any other participant, may be revealed.

1.4 If a member realises that information has been shared inadvertently, they must notify the EISF Secretariat immediately for corrective action.

1.5 If a breach of confidentiality of information is identified (rather than self-reported) the EISF Secretariat will investigate it. The Steering Group will then decide on the appropriate action to be taken, for example, a warning letter for an accidental breach or removal of information privileges from the Member or Affiliate in cases of deliberate misuse.

2. Confidential Information Recipient Status

2.1 Information disseminated by the EISF Secretariat is intended for designated recipients only; this includes information from the member only component of the EISF website and the EISF_Chat.

2.2 HQ and regional SFPs and/or their organisations will inform the EISF Membership and Projects Officer (eisf-info@eisf.eu) or EISF Administrator (eisf-admin@eisf.eu) if they leave their current position, and communicate to the EISF Membership and Projects Officer or EISF Administrator the contact details of their replacement.

2.3 Recipient Groups:

A. Full EISF Members
B. Associate Members
C. Potential EISF Members
D. EISF Affiliates (e.g. Security consultants and providers, academic institutions, research bodies and coordination networks)
E. Friends of EISF and other interested parties
F. Registered Website Users (which may include individuals of groups C, D & F)

	A+B	C	D	E	F
	EISF Full & Associate Members	Potential EISF Members	EISF Affiliates	Friends of EISF & Other Interested Parties	Registered website users
Questions & answers	Yes	If added value	If added value	If added value	No
EISF up-dates and alerts	Yes	Yes	Yes, but excluding forum business & confidential members information	Yes, but excluding forum business & confidential members information	No
EISF blogs and articles	Yes	Yes, if registered	Yes	Yes, if registered	Yes
EISF_Chat	Yes	If added value, but excluding access to the Members only channels	Public Channels and any Affiliate Specific Channels	If added value, but excluding access to the Members only channels	No
Member only website	Yes	No	No	No	No

3. SAFEGUARDS AGAINST MISUSE

3.1 EISF recommends that all Members and Affiliates take the following steps to safeguard against misuse:

1. Emails:
   a) access emails on a secure server only;
   b) delete emails after reading them and, where appropriate, store the information on a secure server;
   c) do not forward these emails. If it is necessary to circulate the information, copy and paste the necessary details into a new email and ensure they are sent only to individual email addresses and not group addresses according to a pre-arranged procedure.

2. Member only area of EISF website (www.eisf.eu)
   a) access the member only area of the website on a secure server/wifi network only;
   b) use an appropriate password;
   c) do not share your log-on details with anybody else;
   d) if downloading "member only" information from the website store the information on a secure server;
   e) if disseminating "member only" information further ensure they are sent only to individual email addresses and not group addresses according to a pre-arranged procedure;
   f) if you think your computer or smart device may have been compromised advise EISF secretariat immediately so they can take appropriate action to secure the website.

3. EISF_Chat
   a) access the application on a secure server/wifi network only;
   b) use an appropriate password;
   c) do not share your login details with anyone else;
   d) do not take photographs or screenshots of conversations;
   e) if disseminating information ensure that Chatham House Rule is observed and the identity or affiliation of the information provider is not revealed;
   f) if you think your Mattermost account has been compromised advise the EISF Secretariat so it can take appropriate action.

INFORMATION SHARING PROTOCOLS

1. ***Member's Questions and Answers:*** are sent out to Groups A & B and groups C, D & E or individuals therein, if it is felt that they may have useful input into the answers. Questions and answers will be anonymised as required.

2. ***EISF Updates:*** are sent to groups A & B. Information will be anonymised as required.
   Parts of these updates will be sent to groups D & E. However, information to be excluded includes, but not be limited to, information on EISF Forums issues affecting individual members and/or any information which is deemed to be restricted to members only.

3. ***EISF Blogs & Articles:*** - will be uploaded to the public area of the EISF website and sent to groups A, B & D through the website mailing system.

4. ***EISF_Chat*****:** EISF Member only channels will be accessible by groups A & B. Additional staff members from Full and Associate Members may be invited to participate in context-specific private channels, but these requests must be submitted to EISF Secretariat by the respective HQ SFP and access is only provided on a temporary basis. EISF Affiliates, group D, are given access to the Public channels and Affiliate specific channels. Individuals of groups C, D & E may be invited to join the Public Channel or specific private channels to share expertise on a particular issue or context on a temporary basis.

   Access is limited to work e-mail addresses only.

5. ***EISF Website Member Only Component***: Accessible only to groups A & B

   Security Safeguards built into Member Only Component of website include:
   - Invitation only access (access will be revoked by the EISF Secretariat when SFP leaves their post)
   - Appropriate password identification
   - Lock-down after 3 failed attempts to access area
   - Automatic log-out after 10 minutes inactivity
   - Links sent in emails will require password access to documents
   - Background protection to prevent automated log-in attempts
   - Background searches and warnings for unusual usage patterns (e.g. number of downloads in a certain time)
   - A second level of protected area will be provided for more sensitive documents if required
   - The contact details stored within the system will only be permitted to be a work email address