March 2018

EISF INFORMATION SHARING POLICY & PROTOCOLS

All EISF members (full and associate) agree to the terms of this Information Sharing Policy as a condition of their membership.

EISF INFORMATION SHARING POLICY

1. CONFIDENTIAL INFORMATION SHARING

1.1 Security Focal Points (SFPs) agree to share information on security related issues with the EISF Executive Director (or delegated Secretariat staff), and thus with the EISF Members, on the understanding that the EISF Executive Director will take agreed measures to 'sanitise' this information 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 sanitised 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
- incidents
- training and other support activities

1.2 SFPs agree that they will disseminate information they receive, through email, EISF website, EISF_Chat or 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 take appropriate action, be it a warning letter for an accidental breach or removal of information privileges from the member for 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 area of the EISF website and the EISF_Chat.

2.2 These recipients are included on the member contact list on the understanding that they are the decision makers regarding security risk management for their organisation.

2.3 SFPs and/or their agency 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 Project Officer or EISF Administrator the contact details of the replacement.

2.4 Recipient Groups:

A. Full EISF Members
B. Associate EISF Members (e.g. Red Cross organisations)
C. Potential EISF Members
D. Registered Website Users (which may include individuals of groups C,E and F)
E. EISF Associates (e.g. Security Consultants, Other SFPs)
F. Other interested parties (e.g. academics)

Table I: Information provided to Recipient Groups

	A+B	C	D	E	F
	EISF Members Associate Members	Potential EISF Members	Registered Website Users	EISF Associates	Other interested parties
Questions & answers	Yes	If added value		If added value	If added value
EISF updates and alerts	Yes	Yes		Yes, but excluding Forum business & confidential members information	Yes, but excluding Forum business & confidential members information
EISF blogs and articles	Yes		Yes		
EISF_Chat	Yes	If added value, but excluding access to the Members Only Channel		If added value, but excluding access to the Members Only Channel	If added value, but excluding access to the Members Only Channel
Member only websites	Yes				
Associated lists (e.g. SLT)	Yes				

3. SAFEGUARDS AGAINST MISUSE

3.1 EISF recommends that members take the following steps to safeguard against misuse of information:

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 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 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 login details with anyone else;
   d) if downloading 'ember only' information from the website store the information on a secure server;
   e) if disseminating 'member only' information further ensure that it is 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 has been compromised advise the 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.

3.2 A Steering Group member will be 'on-call' at all times to advise the EISF Executive Director about confidentiality issues or questions.

INFORMATION SHARING PROTOCOLS

Questions and Answers: will be sent out to groups A & B and groups C, E & F or individuals therein, if it is felt by the EISF Secretariat that they may have useful input into the answers. Questions and answers will be sanitised as required.

EISF Updates & Alerts: will be sent to groups A, B & C. Information will be sanitised as required.

Parts of these updates will be sent to groups E & F. The types of exclusions include, but are not be limited to, information on Forum business (e.g. initial evaluation results), issues affecting individual members and/or any information which is deemed to be confidential.

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.

EISF_Chat: EISF Member Only Channel will be accessible by groups A & B. Individuals of groups C,E & F may be invited to join the 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.

EISF Website Member Only Area: Accessible only to groups A & B

Security safeguards built into the Member Only area of website include:

- Invitation only access (access will be revoked by the EISF Secretariat when SFPs leave their post)
- Appropriate password identification
- Lock-down after three failed attempts to access area
- Automatic log-out after 10 minutes inactivity
- Links sent in emails will require a password to access 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

Associated Lists: includes groups A & B. All information sharing policies apply equally to information disseminated through associated lists accessible through membership of EISF, e.g. the United Nations Department of Safety & Security Saving Lives Together initiative.