Forum of Incident Response and Security Teams (FIRST)

Information Exchange Policy framework

Version 1.0

Introduction

1.   About this policy

1.1   This policy sets out the FIRST Information Exchange Policy (IEP) framework that Computer Security Incident Response Teams (CSIRT), security communities, organizations, and vendors may consider implementing to support their information sharing and information exchange initiatives.

1.2   This framework is intended to support both the existing approaches to defining information exchange policies used by CSIRTs, and information exchange policies that organizations will need as their information exchanges mature and evolve.

1.3   Example implementations are listed in **Appendix A: Machine Readable IEP Framework Examples**

2.   Background

2.1   Automating the exchange of security and threat information in a timely manner is crucial to the future and effectiveness of the security response community.

2.2   The timely distribution of sensitive information will only thrive in an environment where both producers and consumers have a clear understanding of how shared information can and cannot be used, with very few variations of interpretation.

2.3   The general lack of adequate policy that supports information exchange is increasingly becoming an impediment to timely sharing. This will only be exacerbated as more organizations start actively participating in information exchange communities and the volume of security and threat information being shared continues to grow.

2.4   The Traffic Light Protocol[1] (TLP) is the most commonly used method to mark and protect information that is shared. The original intent behind TLP was to speed up the time-to-action on shared information by pre-declaring the permitted redistribution of that information, reducing the need for everyone to ask the producer if it could be "shared with XYZ in my organization" and for that purpose TLP still works.

2.5   The challenge for producers of information is that they need to be able to convey more than just the permitted redistribution of the information. There can be a lack of clarity when defining and interpreting the permitted actions and uses of information shared between organizations. This is compounded by the sensitive nature and commercially competitive aspects of security and threat information.

2.6   FIRST, interested in enabling the global development and maturation of CSIRTs, recognized that the general lack of adequate policy supporting information exchange is increasingly becoming an impediment to information sharing amongst CSIRT teams.

2.7   Given the geographical and functional span of the membership of FIRST, it was determined that the community that it assembles would be an appropriate source for definitive capture and representation of CSIRTs IEP requirements.

---

[1] https://en.wikipedia.org/wiki/Traffic_Light_Protocol

2.8   Automating information exchange is not just a matter of technology; but also one of policy, language, and structured understanding.

Policy framework

3.   Framework Overview

3.1   The IEP framework is structured by Policy Types that act as high level categories under which the individual Policy Statements of similar type or intent are grouped and defined.

3.2   The Policy Types are intended to provide the smallest set of categories needed to encapsulate the majority of individual policy statements.

3.3   The Policy Types provide extensibility for exceptions and future requirements, as information exchange matures and evolves.

4.   Framework Policy Types

4.1   Four policy types are supported: **Handling, Action, Sharing, and Licensing (HASL)**.

    4.1.1 **HANDLING** policy statements define any obligations or controls on information received, to ensure the confidentiality of information that is shared

    4.1.2 **ACTION** policy statements define the permitted actions or uses of the information received that can be carried out by a recipient

    4.1.3 **SHARING** policy statements define any permitted redistribution of information that is received

    4.1.4 **LICENSING** policy statements define any applicable agreements, licenses, or terms of use that governs the information being shared

5.   Framework Definitions and Roles

5.1   **Provider** means the organization or individual who acts to provide, produce, publish, share or exchange information with third parties.

5.2   A provider stipulates the obligations and requirements for information they share through Policy Statements.

5.3   **Recipient** means the organization or individual who receives or consumes information from third party Providers.

5.4   Organizations can act as either a Provider or Recipient.

5.5   Although this document recognizes that relationships and sharing agreements exist between Providers and Recipients, it does not seek to define these inter-relationships.

6.   Framework Policy Statements

6.1   A Provider defines individual Policy Statements that articulate the specific requirements or obligations for Recipients on information the Provider shares.

6.2   Each policy statement includes the following properties, by definition:

    6.2.1   POLICY STATEMENT - states the common name for each policy statement.

    6.2.2   POLICY TYPE - states the Policy Type the Policy Statement is associated with.

    6.2.3   POLICY DESCRIPTION - provides context and defines the intended purpose of the policy statement.

6.2.4 POLICY ENUMERATIONS - Define the set of permitted enumerations for the policy statement and may include definitions for enumerations that are not described elsewhere in this policy.

6.2.5 REQUIRED STATEMENT - States if the Policy Statement is mandatory. Required statements must indicate the default enumeration. Default enumerations must be set to provide the most restrictive option for the Policy Statement.

6.3 Policy statement enumerations that indicate requirement levels use the key words "MUST", "MUST NOT", and "MAY" in this document are to be interpreted as described in RFC2119[2].

6.3.1 MUST - This word means that the policy statement is an absolute requirement.

6.3.2 MUST NOT - This phrase means that the policy statement is an absolute prohibition.

6.3.3 MAY - This word means that the policy statement is truly optional.

---

[2] https://tools.ietf.org/html/rfc2119

7. Handling Policy Statements

7.1 Handling policy statements define any obligations or controls on information received, to ensure the confidentiality of information that is shared.

7.1.1 ENCRYPT IN TRANSIT

Policy Statement	ENCRYPT IN TRANSIT
Policy Type	HANDLING
Policy Description	States whether the received information has to be encrypted when it is retransmitted by the recipient.
Policy Enumerations	**MUST** Recipients MUST encrypt the information received when it is retransmitted or redistributed. **MAY** Recipients MAY encrypt the information received when it is retransmitted or redistributed.
Required Statement	NO

7.1.2 ENCRYPT AT REST

Policy Statement	ENCRYPT AT REST
Policy Type	HANDLING
Policy Description	States whether the received information has to be encrypted by the Recipient when it is stored at rest.
Policy Enumerations	**MUST** Recipients MUST encrypt the information received when it is stored at rest. **MAY** Recipients MAY encrypt the information received when it is stored at rest.
Required Statement	NO

8. Action Policy Statements

8.1 Action policy statements define the permitted actions or uses of the information received that can be carried out by a recipient.

8.1.1 PERMITTED ACTIONS

Policy Statement	PERMITTED ACTIONS
Policy Type	ACTION
Policy Description	States the permitted actions that Recipients can take upon information received.
Policy Enumerations	**NONE** Recipients MUST contact the Providers before acting upon the information received. **CONTACT FOR INSTRUCTION** Recipients MUST contact the Providers before acting upon the information received. **INTERNALLY VISIBLE ACTIONS** Recipients MAY conduct actions on the information received that are only visible on the Recipients internal networks and systems, and MUST NOT conduct actions that are visible outside of the Recipients networks and systems, or visible to third parties. **EXTERNALLY VISIBLE INDIRECT ACTIONS** Recipients MAY conduct indirect, or passive, actions on the information received that are externally visible and MUST NOT conduct direct, or active, actions. **EXTERNALLY VISIBLE DIRECT ACTIONS** Recipients MAY conduct direct, or active, actions on the information received that are externally visible.
Required Statement	NO

8.1.2 VICTIM NOTIFICATIONS

Policy Statement	VICTIM NOTIFICATIONS
Policy Type	ACTION
Policy Description	Recipients are permitted notify affected third parties of a potential compromise or threat. Examples include permitting National CSIRTs to send notifications to affected constituents, or a service provider contacting affected customers. Scenarios include conducting active actions, on the information received, that are externally visible. Examples include pinging a host, takedown operations, deploying anti-virus signatures.

Policy Enumerations	**MAY**
	  Recipients MAY conduct active actions that are externally visible, on the information received.
	
	MUST NOT
	  Recipients MUST NOT conduct active actions that are externally visible, on the information received.

Required Statement	NO

9. Sharing Policy Statements

9.1 Sharing policy statements define any permitted redistribution of information that is received and any actions that need to be taken first.

9.1.1 TRAFFIC LIGHT PROTOCOL

Policy Statement	TRAFFIC LIGHT PROTOCOL
Policy Type	SHARING
Policy Description	Recipients are permitted to redistribute the information received within the redistribution scope as defined by the enumerations. The enumerations "RED", "AMBER", "GREEN", "WHITE" in this document are to be interpreted as described in the FIRST Traffic Light Protocol Policy[3]

Policy Enumerations	**RED**
	    Personal for identified recipients only.
	
	AMBER
	    Limited sharing on the basis of need-to-know.
	
	GREEN
	    Community wide sharing.
	
	WHITE
	    Unlimited sharing.

Required Statement	NO

---

[3] FIRST Traffic Light Protocol Policy <need url>

9.1.2 TRANSITIVE TRUST REQUIRED

Policy Statement	TRANSITIVE TRUST REQUIRED
Policy Type	SHARING
Policy Description	Recipients are permitted to redistribute the information received only with third parties the Recipient can ensure will protect the information to the same extent as the Provider requires of the Recipient. Examples include non-disclosure agreements, sharing agreements, or licenses the Recipient has with the third parties that ensure the equitable protection of information shared.

Policy Enumerations	**MAY**
	    Recipients MAY redistribute the information with third parties the Recipient does not have a formal agreement with.
	
	MUST
	    Recipients MUST only redistribute information with third parties that will protect the information to the same extent the Provider requires of the Recipient.

Required Statement	NO

9.1.3 PROVIDER ATTRIBUTION

Policy Statement	PROVIDER ATTRIBUTION
Policy Type	SHARING
Policy Description	Recipients could be required to attribute or anonymize the Provider when redistributing the information received.

Policy Enumerations	**MAY**
	    Recipients MAY attribute the Provider when redistributing the information received.
	
	MUST
	    Recipients MUST attribute the Provider when redistributing the information received.
	
	MUST NOT
	    Recipients MUST NOT attribute the Provider when redistributing the information received.

Required Statement	NO

9.1.4 OBFUSCATE VICTIMS

Policy Statement	OBFUSCATE VICTIMS
Policy Type	SHARING
Policy Description	Recipients could be required to obfuscate or anonymize information that could be used to identify the victims before redistributing the information received. Examples include removing victims IP addresses, or removing the victim names but leaving the victim industry vertical prior to sending a victim notification.
Policy Enumerations	**MAY** Recipients MAY obfuscate information about the specific victims. **MUST** Recipients MUST obfuscate information about the specific victims. **MUST NOT** Recipients MUST NOT obfuscate information about the specific victims.
Required Statement	NO

10. Licensing Policy Statements

10.1 Licensing policy statements define any applicable agreements, licenses, or terms of use that governs the information being shared. For example, a reference to an existing partner sharing agreement or commercial license.

10.1.1 COMMERCIAL USE

Policy Statement	COMMERCIAL USE
Policy Type	LICENSING
Policy Description	States whether Recipients are permitted to use information received in commercial products or services. An example is permitting the inclusion of the information in commercial feeds and services
Policy Enumerations	**MAY** Recipients MAY use this information in commercial products or services. **MUST NOT** Recipients MUST NOT use this information in commercial products or services.
Required Statement	NO

10.1.2 RESEARCH

Policy Statement	RESEARCH
Policy Type	LICENSING
Policy Description	Recipients could be permitted use of information received in research e.g. approved for use in malware research or data analytics
Policy Enumerations	**MAY** Recipients MAY use this information for Research. **MUST NOT** Recipients MUST NOT use this information for Research.
Required Statement	NO

10.1.3   TERMS OF USE

Policy Statement	TERMS OF USE
Policy Type	LICENSING
Policy Description	This statement can be used to convey a description or reference to any applicable licenses, agreements, or conditions between the producer and receiver. e.g. specific TERMS OF USE language, agreement name, or a URL.
Policy Enumerations	There are no TERMS OF USE enumerations and this is a free form text field.
Required Statement	NO

11. Metadata Policy Statements

Metadata policy statements define the metadata elements for an IEP that are needed to support implementation of the IEP framework and the machine readability of IEPs. Metadata policy statements have values but do not have enumerations.

11.1.1   POLICY ID

Policy Statement	POLICY ID
Policy Type	METADATA
Policy Description	Provides a unique ID to identify a specific IEP implementation.
Required Statement	YES

11.1.2   POLICY VERSION

Policy Statement	POLICY VERSION
Policy Type	METADATA
Policy Description	States the version of the IEP framework that has been used. e.g. 1.0
Required Statement	NO

11.1.3   POLICY NAME

Policy Statement	POLICY NAME
Policy Type	METADATA
Policy Description	This statement can be used to provide a name for an IEP implementation. e.g. FIRST Mailing List IEP
Required Statement	NO

11.1.4   POLICY START DATE

Policy Statement	POLICY START DATE
Policy Type	METADATA
Policy Description	States the UTC date that the IEP is effective from.
Required Statement	NO

11.1.5   POLICY END DATE

Policy Statement	POLICY END DATE
Policy Type	METADATA
Policy Description	States the UTC[4] date that the IEP is effective until.
Required Statement	NO

11.1.6   POLICY REFERENCE

Policy Statement	POLICY REFERENCE
Policy Type	METADATA
Policy Description	This statement can be used to provide a URL reference to the specific IEP implementation.
Required Statement	NO

---

[4] https://en.wikipedia.org/wiki/ISO_8601

Appendix A: Machine Readable IEP Examples

The following is an example JSON representation of an IEP implementation

```
"FIRST-mailing-list-iep": {
      "id": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
      "name": "FIRST.org Mailing List IEP",
      "version": 1,
      "reference": "https://www.first.org/mailing-list-iep",
      "start-date": "2016-01-01 10:09:00",
      "end-date": "2016-12-31 10:09:00",
      "encrypt-in-transit": "MAY",
      "encrypt-at-rest": "MAY",
      "permitted-actions": "EXTERNALLY VISIBLE DIRECT ACTIONS",
      "victim-notifications": "MAY",
      "tlp": "AMBER",
      "transitive-trust": "MUST",
      "attribution": "MUST NOT",
      "obfuscate-victim": "MUST",
      "commercial-use": "MAY",
      "research": "MAY",
      "terms-of-use": " https://www.first.org/about/policies/bylaws"
}
```

Appendix B: IEP Framework Glossary

This section is yet to be defined