Information Exchange Policy 2.0 Framework Definition

Copyright Notice

Abstract

The FIRST Information Exchange Policy (IEP) framework enables threat intelligence providers to inform recipients how they may use the threat intelligence they receive. IEP ensures that both parties are aware of any restrictions on the use of the shared threat intelligence, and reduces the likelihood of misunderstandings.

IEP 2.0 builds upon the work done in IEP 1.0 to enhance the re-usability of the IEP framework, reducing its impact on implementations, and enabling the sharing of common IEP Policies.

Co-chairs

The FIRST IEP-SIG Co-chairs at the time of release were:

- Terry MacDonald
- Paul McKitrick
- Merike Kaeo
- Steve Mancini

Editors

The FIRST IEP 2.0 Framework Definition was created and edited by the following people:

- Terry MacDonald
- Paul McKitrick
- Merike Kaeo

Contributors

The following people contributed to the FIRST IEP 2.0 Framework Definition:

- Terry MacDonald
- Paul McKitrick
- Merike Kaeo
- Steve Mancini
- Richard Struse
- John Wunder
- Thomas Millar
- Bret Jordan
- Allan Thomson

Introduction

1. About this policy

1.1 This policy sets out the FIRST Information Exchange Policy (IEP) 2.0 Framework Definition 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 An IEP 2.0 JSON Specification has been defined[1]. The IEP Framework is designed for implementation in a variety of formats and additional specifications may be added.

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[2] (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.

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

---

[1] IEP 2.0 JSON Specification (https://www.first.org/iep/2.0/first-iep-2.0-json-specification.pdf)
[2] FIRST Traffic Light Protocol (https://www.first.org/tlp)

Policy framework

3. Framework Roles

3.1 **Policy Authority** means the organization or individual who creates an IEP and defines the Policy Statements for that IEP implementation.

3.2 A Policy Authority typically creates an IEP and stores the Policy File in a location accessible by URL, to allow Providers and Recipients to reference it.

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

3.4 A provider stipulates the obligations and requirements for information they share by marking the exchanged information with an applicable IEP.

3.5 Providers typically mark the shared information with a reference to an existing IEP in a Policy File.

3.6 Providers may mark exchanged information directly by embedding an IEP within another protocol e.g. the Structured Threat Information eXpression (STIX)[3]

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

3.8 Organizations can act as a Policy Authority, Provider, and Recipient.

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

4. Framework Definitions

4.1 The **IEP Framework** specifies a series of structures that work together to form an IEP.

4.2 A valid IEP MUST have a unique **Policy ID** and MUST contain all the **Policy Statements** defined in sections 7, 8, 9, 0, 0, and 12 of this document. This mandatory requirement was introduced in IEP 2.0.

4.3 An IEP is immutable once it has been first used. Changes cannot be made to an existing IEP and a new IEP must be created instead.

4.4 An IEP can be created as a standalone **Policy File**, or can be embedded within another protocol structure such as STIX.

4.5 An IEP Policy File MUST contain at least one IEP and MAY contain more than one IEP.

4.6 A **Policy Reference** contains a Policy ID Reference and a URL for a specific IEP Policy File.

4.7 Policy References are designed for use within other information exchange standards and protocols, and enable reuse of common IEPs. Policy References are described in section 12 of this document.

[3] STIX (https://stixproject.github.io/)

5. Framework Policy Types

5.1 Policy Statements of a similar type or intent are grouped together into high level categories called **Policy Types**.

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

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

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

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

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

5.3 An additional **METADATA** policy type defines the group of policy statements that describe IEP metadata required to enable the effective use of the IEP Framework.

6. Framework Policy Statements

6.1 A Policy Authority 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.

6.3 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[4].

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.

[4] 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.

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.

7.2 The ENCRYPT IN TRANSIT Policy Statement does not define which encryption algorithms to use in transit, as it is expected that the information sharing protocols that utilize IEP will provide an adequate level of encryption functionality built into it.

7.3 The ENCRYPT AT REST Policy Statement does not define which encryption algorithms to use for data at rest, as it is expected that implementers will use a level of encryption commensurate with the type of data they are storing.

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 SHOULD NOT act upon the information received. *NOTE: In some cases the recipient is required to report the information to law enforcement or other officials due to laws in their local jurisdiction, and those laws will take precedence over this IEP Policy Statement.* **CONTACT FOR INSTRUCTION** Recipients MUST contact the Providers before acting upon the information received. An example is where information redacted by the Provider could be derived by the Recipient and identify the affected parties. **INTERNALLY VISIBLE ACTIONS** Recipients MAY conduct actions on the information received that are only visible on the Recipient's 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 internally visible actions, and MAY also conduct indirect, or passive, actions on the information received. Recipients MUST NOT conduct direct, or active, actions that will be visible by Threat Actors mentioned within the shared information. **EXTERNALLY VISIBLE DIRECT ACTIONS** Recipients MAY conduct direct, or active, actions on the information received that are externally visible. Recipients MAY also conduct externally visible indirect actions, and MAY conduct internally visible actions.

8.1.2 AFFECTED PARTY NOTIFICATIONS

Policy Statement	AFFECTED-PARTY-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. ***NOTE:*** *This setting may not be enforceable if the TLP setting is WHITE, GREEN or AMBER. Please see section 9.2 for more information.*
Policy Enumerations	**MAY** Recipients MAY notify affected parties of a potential compromise or threat. **MUST NOT** Recipients MUST NOT notify affected parties of potential compromise or threat. ***NOTE:*** *This setting may not be enforceable if the TLP setting is WHITE, GREEN or AMBER. Please see section 9.2 for more information.*

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	TLP
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 defined at https://www.first.org/tlp. ***NOTE:** This setting is impacted by the setting of AFFECTED PARTY NOTIFICATIONS. Please see section 9.2 for more information.*
Policy Enumerations	**RED** Not for disclosure, restricted to participants only. **AMBER** Limited disclosure, restricted to participants' organizations. **GREEN** Limited disclosure, restricted to the community. **WHITE** Disclosure is not limited.

9.1.2 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 directly attribute the Provider when redistributing the information received. **MUST** Recipients MUST directly attribute the Provider when redistributing the information received. **MUST NOT** Recipients MUST NOT directly attribute the Provider when redistributing the information received. *Warning: It still may be possible attribution will still be derived from the information itself.*

9.1.3 OBFUSCATE AFFECTED PARTIES

Policy Statement	OBFUSCATE-AFFECTED-PARTIES
Policy Type	SHARING
Policy Description	Recipients could be required to obfuscate or anonymize information that could be used to identify the affected parties before redistributing the information received. Examples include removing affected parties IP addresses, or removing the affected parties' names but leaving the affected parties industry vertical prior to sending a notification. *It is up to each information sharing protocol that makes use of IEP to determine what level of obfuscation is acceptable.*
Policy Enumerations	**MAY** Recipients MAY obfuscate information about the specific affected parties. **MUST** Recipients MUST obfuscate information about the specific affected parties. ***Warning:*** *It still may be possible affected parties will be identified from the derived information even after obfuscation.* **MUST NOT** Recipients MUST NOT obfuscate information about the specific affected parties.

9.2 The redistribution of information is controlled via a combination of the TRAFFIC LIGHT PROTOCOL (see section 9.1.1) and the AFFECTED PARTY NOTIFICATIONS (see section 8.1.2). The table below describes the sharing restrictions that arise from the combinations of those two Policy Statements.

TLP	AFFECTED PARTY NOTIFICATIONS	Resultant Re-sharing Restrictions
WHITE	MAY	**With anyone** The recipient may re-share the information they receive with anyone else. There are no restrictions on re-sharing with others.
GREEN	MAY	**Original community, and the affected party only** The recipient may re-share the information they receive with any other Organization or Person who belongs to the same community that this information was originally shared within by the Producer. The recipient may also re-share a subsection of the information they receive with the affected party mentioned in that subsection, even if that affected party is not within the community that the producer shared the information within. *You will need to check with the producer to re-share any information with anyone else, or to re-share the information, in full, with the affected parties.*
AMBER	MAY	**Within your Organization and the affected party's organization only** The recipient may only re-share the information they receive with

		other personnel within their own Organization, or a subsection of the information they receive with personnel within the affected party organization (but only the parts involving the affected party). *You will need to check with the producer to re-share any information with anyone else, or to re-share the information, in full, with the affected parties.*
RED	MAY	**Original recipient person and the affected party organization only** The recipient may only re-share the information they receive with other personnel within their own Organization, or a subsection of the information they receive with personnel within the affected party organization (but only the parts involving the affected party). *You will need to check with the producer to re-share any information with anyone else, or to re-share the information, in full, with the affected parties.*
WHITE	MUST NOT	**Anyone (which includes the affected party)** The recipient may re-share the information they receive with anyone else. There are no restrictions on re-sharing with others.
GREEN	MUST NOT	**Original community only (which may include the affected party)** The recipient may re-share the information they receive with any other Organization or Person who belongs to the same community that this information was originally shared within. The recipient is not allowed to re-share this information with the affected party, unless that affected party is part of the same community that this information was originally shared within by the Producer. *You will need to check with the producer to re-share this information with anyone else.*
AMBER	MUST NOT	**Organization only (which may be the affected party)** The recipient may only re-share the information they receive with other personnel within their own Organization. The recipient is not allowed to re-share this information with the affected party, unless the affected party is within their Organization, or is the Organization itself. *You will need to check with the producer to re-share this information with anyone else.*
RED	MUST NOT	**Recipient person only** The recipient may not re-share this information with anyone else. *You will need to check with the producer to re-share this information with anyone else.*

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 EXTERNAL REFERENCE

Policy Statement	EXTERNAL-REFERENCE
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, contractual language, agreement name, or a URL.
Policy Enumerations	There are no EXTERNAL REFERENCE enumerations and this is a free form text field.

10.1.2 UNMODIFIED RESALE

Policy Statement	UNMODIFIED-RESALE
Policy Type	LICENSING
Policy Description	States whether the recipient MAY or MUST NOT resell the information received unmodified or in a semantically equivalent format. As an example, transposing the information from a .csv file format to a .json file format would be considered semantically equivalent. *NOTE: Setting the unmodified_resale statement value to "must-not" does not restrict the consumer from deriving their own information from the information provided by the producer, and then selling their own derived information.*
Policy Enumerations	**MAY** Recipients MAY resell the information received. **MUST NOT** Recipients MUST NOT resell the information received unmodified or in a semantically equivalent format.

11. Metadata Policy Statements

11.1 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	ID
Policy Type	METADATA
Policy Description	Provides a unique ID to identify a specific IEP implementation.

11.1.2 POLICY IEP VERSION

Policy Statement	VERSION
Policy Type	METADATA
Policy Description	Defines which version of the IEP Framework this policy implements. This MUST be set to the number 2.0 to be valid IEP 2.0.

11.1.3 POLICY NAME

Policy Statement	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

11.1.4 POLICY START DATE

Policy Statement	START-DATE
Policy Type	METADATA
Policy Description	States the UTC[5] date that the IEP is effective from. If no START-DATE is specified the IEP is applicable up until the END-DATE. The representation of an empty START-DATE is defined in the respective protocol Specification document.

[5] https://en.wikipedia.org/wiki/Coordinated_Universal_Time

11.1.5 POLICY END DATE

Policy Statement	END-DATE
Policy Type	METADATA
Policy Description	States the UTC[6] date that the IEP is effective until. If no END-DATE is specified the IEP is applicable in perpetuity. The representation of an empty END-DATE is defined in the respective protocol Specification document.

12. Policy References

12.1 Policy References allow an IEP to be associated with shared information without including the Policy Statements themselves. This is particularly useful when sharing information within large communities as it reduces the overhead of constantly including the same IEP Policy.

12.2 A Policy Reference MUST point at a specific IEP within a Policy File.

12.3 A valid Policy Reference needs to include the following two Policy Reference Statements:

12.3.1 POLICY ID REFERENCE

Policy Statement	ID-REF
Policy Type	REFERENCE
Policy Description	Refers to the unique ID of a specific IEP Policy contained within the information returned from the Policy Reference URI.

12.3.2 POLICY REFERENCE URL

Policy Statement	URL
Policy Type	REFERENCE
Policy Description	This statement can be used to provide a URL at which the IEP Policy can be located and obtained. The IEP Policy reference to the specific IEP implementation.

12.3.3 POLICY REFERENCE IEP Version

Policy Statement	VERSION
Policy Type	REFERENCE
Policy Description	Defines which version of the IEP Framework this policy reference implements. This MUST be set to the number 2.0 to be an IEP 2.0 Policy Reference.

[6] https://en.wikipedia.org/wiki/Coordinated_Universal_Time

Appendix A: IEP Framework JSON examples

The IEP-SIG have defined an IEP 2.0 JSON Specification, outlining how JSON based information sharing protocols can use IEP within their sharing standards. This companion document can be found at the FIRST IEP-SIG homepage at https://www.first.org/iep.

IEP Policy object example

The following is an example JSON representation of an IEP 2.0 policy, using the implementation as defined by the IEP 2.0 JSON Specification.

```
{
	"id": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
	"name": "FIRST IEP-SIG TLP-AMBER",
	"version": 2.0,
	"start_date": "2017-01-01T00:00:00Z",
	"end_date": null,
	"encrypt_in_transit": "may",
	"encrypt_at_rest": "may",
	"permitted_actions": "externally-visible-direct-actions",
	"affected_party_notifications": "may",
	"tlp": "amber",
	"provider_attribution": "must-not",
	"obfuscate_affected_parties": "may",
	"unmodified_resale": "must-not",
	"external_reference": " https://www.first.org/about/policies/bylaws"
}
```

IEP Policy Reference example

The following is an example of how to refer to an IEP 2.0 policy using an IEP Reference as defined by the IEP 2.0 JSON Specification.

```
{
	"id_ref": "01bc4353-4829-4d55-8d52-0ab7e0790df9",
	"url": "https://www.first.org/iep/2.0/first-iep-sig-tlp-amber.iepj",
	"version": 2.0
}
```