Information Exchange Policy 2.0 Framework Definition

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.

Release Date

6 November 2019

Co-chairs

The FIRST IEP Special Interest Group Co-chairs at the time of release were:

- Terry MacDonald
- Paul McKitrick
- Merike Kaeo

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
- Emily Anderson
- Sarah Kelley
- Jason Keirkstead
- Trey Daley
- Mark Davidson

Copyright Notice and License

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 CSIRT's existing policies to define information exchange and new policies to define matured and evolved CSIRT information exchange.

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 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. A clear understanding of how shared information can and cannot be used by producers and consumers will foster timely distribution of sensitive information amongst producers and consumers.

2.3 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. This will be exacerbated as more organizations start actively participating in information exchange communities and the volume of shared security and threat information grows.

2.4 The Traffic Light Protocol[2] (TLP) is the most commonly used method to indicate how sensitive information can be redistributed. 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".

2.5 The challenge for information producers is that they need 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 producers and consumers. This is compounded by the sensitive nature and commercially competitive aspects of security and threat information.

2.6 FIRST membership includes diverse geographic and functional breadth. As such, it was determined that the FIRST membership community is an appropriate source for reasonable capture and representation of global CSIRTs IEP requirements.

2.7 Automating information exchange is not just a matter of technology, but also one of policy, language, and common 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. 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 inter-relationships.

3.10 **Protocol Author** means the standards body, organization or individual who decides to use IEP within another Protocol that they author or control (e.g. OASIS Cyber Threat Intelligence Technical Committee).

3.11 **Protocol** means the Protocol created by the Protocol Author that leverages IEP to describe information sharing restrictions.

3.12 A Protocol Author can choose to enforce consequences for violation of IEP within their Protocol, or it can choose to make IEP informational only and not enforce restrictions for violation of the IEP.

3.13 If IEP violation results in consequences when used within a Protocol, we recommend that Protocol Authors document those consequences within their Protocol documentation.

4. Definitions

4.1 The **IEP 2.0 Framework** specifies a series of structures that work together to form an IEP.

4.2 An IEP is not a legal agreement and SHOULD NOT be considered as one.

4.3 A valid IEP MUST have a unique **Policy ID** and MUST contain all the **Policy Statements** defined in sections 7, 8, 9, 10, and 11 of this document. This mandatory requirement is introduced in IEP 2.0.

4.4 An IEP is immutable once it has been first defined. Changes cannot be made to an existing IEP. A new IEP must be created instead.

4.5 An IEP may be created as a standalone **Policy File**, or may be embedded within another protocol structure such as STIX 2.1.

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

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

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

4.8 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.

5. Policy Statements

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

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

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

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

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

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

5.3 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]

5.3.1 MUST - the policy statement is an absolute requirement.

5.3.2 MUST NOT - the policy statement is an absolute prohibition.

5.3.3 MAY - the policy statement is truly optional.

5.4 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC2119.[5]

6. Policy Types

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

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

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

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

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

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

6.3 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.

---

[4] Key words for use in RFCs to Indicate Requirement Levels: https://tools.ietf.org/html/rfc2119

[5] Id.

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. Software implementations MUST ensure that any information retransmitted is encrypted during transit to an adequate level of encryption, as defined in the protocol that uses IEP. **MAY** Recipients MAY encrypt the information received when it is retransmitted or redistributed. Software implementations MAY ensure that any information retransmitted is encrypted during transit to an adequate level of encryption, as defined in the protocol that uses IEP.

7.2 The ENCRYPT IN TRANSIT Policy Statement does not define which encryption algorithms to use in transit, as it is expected that each information sharing protocol that utilizes IEP will define which encryption algorithms, standards and technologies will be considered an adequate level of encryption functionality for that protocol.

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. The information SHOULD only be used for internal informational purposes, and internally visible actions, externally visible indirect actions and externally visible direct actions SHOULD NOT be performed. **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 any actions on the information received.

8.1.2 AFFECTED PARTY NOTIFICATIONS

Policy Statement	AFFECTED-PARTY-NOTIFICATIONS
Policy Type	ACTION
Policy Description	Recipients are permitted to notify affected third parties of a 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 applicable 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.

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, and with clients or customers who need to know the information to protect themselves from further harm. **GREEN** Limited disclosure, restricted to peers and partners in 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.*

9.2 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 Sharing Restrictions**
WHITE	MAY	**With anyone** The recipient may redistribute the information they receive with anyone else. There are no restrictions on redistributing with others.
GREEN	MAY	**Original community, and the affected party only** The recipient may redistribute 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 redistribute 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 redistribute any information with anyone else, or to redistribute the information, in full, with the affected parties.*
AMBER	MAY	**Within your Organization and the affected party's organization only** The recipient may only redistribute 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 redistribute any information with anyone else, or to redistribute the information, in full, with the affected parties.*
RED	MAY	**Original recipient person and the affected party organization only** The recipient may only redistribute 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 redistribute any information with anyone else, or to redistribute the information, in full, with the affected parties.*
WHITE	MUST NOT	**Anyone (which includes the affected party)** The recipient may redistribute the information they receive with anyone else. There are no restrictions on redistributing with others.
GREEN	MUST NOT	**Original community only (which may include the affected party)** The recipient may redistribute 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 redistribute 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 redistribute this information with anyone else.*
AMBER	MUST NOT	**Organization only (which may be the affected party)** The recipient may only redistribute the information they receive with other personnel within their own Organization. The recipient is not allowed to redistribute 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 redistribute this information with anyone else.*
RED	MUST NOT	**Recipient person only** The recipient may not redistribute this information with anyone else. *You will need to check with the producer to redistribute this information with anyone else.*

10. Licensing Policy Statements

10.1 Licensing policy statements define any applicable permissions or restrictions from agreements, licenses, or terms of use that govern the information being shared. For example, restrictions on redistributing the information in commercial feeds.

10.1.1 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. The Policy ID MUST be either UUIDv4 or UUIDv5 as specified in RFC4122[6]

11.1.2 POLICY IEP VERSION

Policy Statement	IEP-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 TLP-AMBER IEP”

11.1.4 POLICY DESCRIPTION

Policy Statement	DESCRIPTION
Policy Type	METADATA
Policy Description	This statement can be used to provide some background information about the IEP implementation. This field MUST NOT be used to add any additional conditions to the IEP. e.g. "This is the FIRST TLP-AMBER Information Exchange Policy." The DESCRIPTION policy statement is intended to be used to provide additional detail about the IEP Policy, and MUST NOT be used to describe additional restrictions.

[6] A Universally Unique IDentifier (UUID) URN Namespace: https://tools.ietf.org/html/rfc4122

11.1.5 POLICY START DATE

Policy Statement	START-DATE
Policy Type	METADATA
Policy Description	States the UTC[7] 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.

11.1.6 POLICY END DATE

Policy Statement	END-DATE
Policy Type	METADATA
Policy Description	States the UTC[8] 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.

11.1.7 EXTERNAL REFERENCES

Policy Statement	EXTERNAL-REFERENCES
Policy Type	METADATA
Policy Description	This statement can be used to convey a list of URL references that resolve to network accessible locations containing any applicable licenses, agreements, or conditions between the producer and receiver. e.g. a list of URLs, where each URL's contents contain specific terms of use, contractual language, agreement name, or other additional information.
Policy Enumerations	There are no EXTERNAL REFERENCES enumerations, but this field MUST contain a list of valid URLs as per RFC3986[9].

11.2 Information can be marked with more than one IEP Policy at a time to facilitate the ability for information to be embargoed until a certain date using one IEP Policy, and then re-sharing being allowed after a certain date using a second IEP Policy.

11.3 Each IEP Policy applies to the information it is associated with from the START DATE until the END DATE.

11.4 If there is any overlap of time such that information is marked with more than one IEP Policy, then during that time the Default Unknown IEP Policy MUST be applied to that information, as shown below:

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

[8] Id.

[9] Uniform Resource Identifier (URI): Generic Syntax: https://tools.ietf.org/html/rfc3986

ID	e4eb1db1-e0fb-4200-9f4c-4c713bb197aa
NAME	FIRST IEP-SIG Unknown IEP
DESCRIPTION	This is the FIRST IEP-SIG Unknown Information Exchange Policy, and is applied whenever an implementation cannot access a previously assigned IEP.
IEP-VERSION	2.0
START-DATE	2017-01-01T00:00:00Z
END-DATE	EMPTY/NULL
ENCRYPT-IN-TRANSIT	MUST
PERMITTED-ACTIONS	INTERNALLY VISIBLE ACTIONS
AFFECTED-PARTY-NOTIFICATIONS	MUST NOT
TLP	RED
ATTRIBUTION	MUST NOT
UNMODIFIED-RESALE	MUST NOT
EXTERNAL-REFERENCES	https://www.first.org/iep https://www.first.org/tlp

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 three 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	IEP-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.

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",
            "description": "This is the FIRST IEP-SIG TLP-AMBER Information
Exchange Policy.",
            "iep_version": 2.0,
            "start_date": "2017-01-01T00:00:00Z",
            "end_date": null,
            "encrypt_in_transit": "may",
            "permitted_actions": "externally-visible-direct-actions",
            "affected_party_notifications": "may",
            "tlp": "amber",
            "attribution": "must-not",
            "unmodified_resale": "must-not",
            "external_references": [
                  "https://www.first.org/tlp",
                  "https://www.first.org/iep"
            ]
      }
```

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-tlp-iep.iepj",
      "iep_version": 2.0
}
```