SPG:Drafts:Security Policy

From EGIWiki

1 The *new draft* e-Infrastructure Security Policy

This is a DRAFT document being revised by EGI SPG. It is not final and has not been approved or adopted. The currently adopted top-level security policy document is available at https://documents.egi.eu/document/86.

This policy is one of a set of documents that together define the Security Policy (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)). This individual document must be considered in conjunction with all the policy documents in the set.

2 Introduction and Definitions

To fulfil its mission, it is necessary for the *e-Infrastructure* to protect its assets. This document presents the policy regulating those activities of *participants* related to the security of the *e-Infrastructure*.

2.1 Definitions

The phrase *e-Infrastructure* when italicised in this document, means all of the people and organisations, hardware, software, networks, facilities, etc. that are required to develop, test, deliver, monitor, control or support IT *services*.

The other italicised words used in this document are defined as follows:

- *Policy* is interpreted to include rules, responsibilities and procedures specified in this document together with all those in other documents which are required to exist by stipulations in this document.
- A *participant* is any entity providing, using, managing, operating, supporting or coordinating one or more IT *service(s)*.
- A *service* is any computing or software system, which provides access to, information about or controls *resources*.
- A *resource* is the *equipment* and *software* required to run a *service* on the *e-Infrastructure*, and any *data* held on the *service*.
- Included in the definition of *equipment* are processors and associated disks, tapes and other peripherals, storage systems and storage media, networking components and interconnecting media.
- Included in the definition of *software* are operating systems, utilities, compilers and other general purpose applications, any software required to operate any *equipment*, software and middleware released and/or distributed by the *e-Infrastructure* and any software required to support any application associated with *User Communities* or other authorised *users*.
- Included in the definition of *data* are data required to operate any equipment defined as a *resource*, data required to operate any *service*, data intended to be processed or produced by any software defined as a *resource*, and any application data.
- The *Management* is the collection of the various boards, committees, groups and individuals mandated to oversee and control the *e-Infrastructure*.
- A *User* is an individual who has been given authority to access and use *e-Infrastructure resources*.
- A *User Community* is a grouping of *Users* and optionally *resources*, usually not bound to a single institution, who, by reason of their common membership and in sharing a common goal, are given authority to use a set of *resources*.

- Included in the definition of a *User Community* are cases where *resources* are offered to individual *Users* who are not members of an explicitly organised *User Community*.
- *The User Community Management* is the collection of various individuals and groups mandated to oversee and control a *User Community*.
- A *Resource Centre* is an entity having administrative control of *resources* provided to the *e-Infrastructure*. This may be at one physical location or spread across multiple physical locations.
- *Resource Centre Management* is the collection of various individuals and groups mandated to oversee and control a *Resource Centre*.

Other terms are defined in the [Glossary (https://wiki.egi.eu/wiki/Glossary_V2)].

In this document the key words `must', `must not', `required', `shall', `shall not', `recommended', `may', and `optional' are to be interpreted as described in RFC 2119.

2.2 Objectives

This *policy* gives authority for actions which may be carried out by designated individuals and organisations and places responsibilities on all *participants*.

2.3 Scope

This *policy* applies to all *participants*. Every *Resource Centre* participating in the *e-Infrastructure* autonomously follows their local policies with respect to the *services* and *resources* they own, including those which are part of the *e-Infrastructure*. This *policy* augments local policies by setting out additional *e-Infrastructure*-specific requirements.

2.4 Additional Policy Documents

Additional policy documents required for a proper implementation of this *policy* may be found at a location specific to the *e-Infrastructure* (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

2.5 Approval and Maintenance

This *policy* is prepared and maintained by the Security Policy Group, approved by *Management* and thereby endorsed and adopted by the *e-Infrastructure* as a whole. This *policy* will be revised by the Security Policy Group as required and resubmitted for formal approval and adoption whenever significant changes are needed. The most recently approved version of this document is available at (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

3 Roles and Responsibilities

This section defines the roles and responsibilities of *participants*.

3.1 The Management

The *Management* provides, through the adoption of this *policy* and through its representations on the various management bodies of the *e-Infrastructure*, the overall authority for the decisions and actions resulting from this *policy* including procedures for the resolution of disputes.

The *Management* provides the capabilities for meeting its responsibilities with respect to this policy.

The *Management* is responsible for ensuring compliance of its participants and can represent them towards third parties with respect to this *policy*.

3.2 The e-Infrastructure Security Officer and the CSIRT

The *Management* must appoint a Security Officer who leads and coordinates the operational security capability (CSIRT). The Security Officer may, in consultation with the CSIRT, *Management* and other appropriate persons, require actions by *participants* as are deemed necessary to protect the *e-Infrastructure* from or contain the spread of IT security incidents. The Security Officer also handles requests for exceptions to this *policy* as described in section Exceptions to Compliance.

3.3 User Community Management

The *User Community Management* must designate a Security contact point (person or team) that is willing and able to collaborate with affected *participants* in the management of security incidents.

The *User Community Management* should abide by the *e-Infrastructure* policies in the areas of Acceptable Use, User Registration and Membership Management and all other applicable policies (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)). Exceptions to this must be handled as in section Exceptions to Compliance. They must ensure that only individuals who have agreed to abide by the *e-Infrastructure* AUP (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)) and the User Community AUP are registered as members of the *User Community*.

User Community Management and *Users* that provide and/or operate *resources* or *services* must abide by the Service Operations Security Policy , the Traceability and Logging Policy and all other applicable policies (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

For services requiring authentication of entities the *User Community Management* must abide by the policy on Acceptable Authentication Assurance (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

User Community Management is responsible for promptly investigating reports of *Users* failing to comply with the policies and for taking appropriate action to limit the risk to the *e-Infrastructure* and ensure compliance in the future, as defined in section Sanctions.

3.4 Users

Users must accept and agree to abide by the *e-Infrastructure* Acceptable Use Policy (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)) and the User Community AUP when they register or renew their registration with a *User Community*.

Users must use *services* and *resources* only in pursuit of the legitimate purposes of their *User Community*. They must respect the autonomy and privacy of the host *Resource Centres* on whose *resources* it may run. They must not attempt to circumvent any restrictions on access to *resources* and *services*. *Users* must show responsibility, consideration and respect towards other *participants* in the demands they place on the *e-Infrastructure*.

Users that provide and/or operate *resources* or *services* must abide by the Service Operations Security Policy and all other applicable policies (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

For services requiring authentication of entities the *Users* must abide by the policy on Acceptable Authentication Assurance (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

Users may be held responsible for all actions taken using their credentials, whether carried out personally or not.

No intentional sharing of user credentials is permitted.

3.5 Resource Centre Management

The *Resource Centre Management* must designate a Security contact point (person or team) that is willing and able to collaborate with affected *participants* in the management of security incidents and to take prompt action as necessary to safeguard *services* and *resources* during an incident.

Resource Centres must abide by the Service Operations Security Policy, the Traceability and Logging Policy and all other applicable policies (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

Resource Centres acknowledge that participating in the *e-Infrastructure* and allowing related inbound and outbound network traffic increases their IT security risk. *Resource Centres* are responsible for accepting or mitigating this risk.

Resource Centres must deploy effective security controls to protect the confidentiality, integrity and availability of their *services* and *resources*.

For services requiring authentication of entities the *Resource Centre* must abide by the policy on Acceptable Authentication Assurance (wiki.egi.eu/wiki/SPG:Documents (https://wiki.egi.eu/wiki/SPG:Documents)).

4 Physical Security

All the requirements for the physical security of *resources* are expected to be adequately covered by each *Resource Centre's* local security policies and practices. These should, as a minimum, reduce the risks from intruders, fire, flood, power failure, equipment failure and environmental hazards. Stronger physical security may be required for equipment used to provide certain critical *services* such as User Community membership services or credential repositories. The technical details of such additional requirements are contained in the procedures for operating and approving such *services*.

5 Network Security

All the requirements for the networking security of *resources* are expected to be adequately covered by each *Resource Centre's* local security policies and practices.

To support specific *User Community* workflows it may be necessary to permit inbound or outbound network traffic. It is the responsibility of the *Resource Centre* to accept or mitigate the risks associated with such traffic.

6 Exceptions to Compliance

Wherever possible, *e-Infrastructure* policies and procedures are designed to apply uniformly to all *participants*. If this is not possible, for example due to legal or contractual obligations, exceptions may be made. Such exceptions should be time-limited and must be documented and authorised by the *e-Infrastructure* Security Officer and, if required, approved at the appropriate level of management.

In exceptional circumstances it may be necessary for *participants* to take emergency action in response to some unforeseen situation which may violate some aspect of this *policy* for the greater good of pursuing or preserving legitimate *e-Infrastructure* objectives. If such a *policy* violation is necessary, the exception should be minimised, documented, time-limited and authorised at the highest level of the *management* commensurate with taking the emergency action promptly, and the details notified to the *e-Infrastructure* Security Officer at the earliest opportunity.

7 Sanctions

Resource Centres that fail to comply with this *policy* in respect of a *service* they are operating may lose the right to have their *services* recognised by the *e-Infrastructure* until compliance has been satisfactorily demonstrated again.

User Communities who fail to comply with this *policy* may lose their right of access to and collaboration with the *e-Infrastructure* and may lose the right to have their *services* recognised by the *e-Infrastructure* until compliance has been satisfactorily demonstrated again.

Users who fail to comply with this *policy* may lose their right of access to the *e-Infrastructure*, and may have their activities reported to their *User Community* or their home organisation.

Any activities thought to be illegal may be reported to appropriate law enforcement agencies.