Open Science Grid | Security Policies

Team: Mike Stanfield[1], Adrian Crenshaw[1], Josh Drake[1], Zalak Shah[1], Jeny Teheran[2]
Institutions: [1]Indiana University (partially funded by IRIS-HEP), [2]Fermi National Accelerator Laboratory

Master Information Security Policy & Procedures

Adopted 1 Dec 2019

The Master Information Security Policies and Procedures (MISPP) is the core information security document for OSG. It defines the roles and responsibilities within the organization as they relate to security, and the guidelines and procedure for designing and implementing all other security policies.

The MISPP lays out the goals of the security program within the context of supporting the larger mission of OSG, and defines how to prioritize them in relation to one another (see below). This policy also establishes procedures for handling exceptional cases and for changing and enforcing security policies.

Goals:

1. Uphold the integrity and trustworthiness of OSG services and software
2. Maintain the confidentiality of information entrusted to OSG
3. Maintain a high level of availability without compromising points 1 & 2

http://go.iu.edu/2i6d

Service Container Security Policy

Adopted 1 Dec 2019

This policy describes how service containers deployed by the OSG software and operations teams should be configured. Since service containers are usually deployed at the edge of the network and are Internet accessible, it is important that there is a standardized process for building and updating them.

This policy defines the requirements for upstream sources to be used for building containers and sets limits on the life of a given container before it is rebuilt to ensure that critical software updates are being applied in a timely manner. Additionally, containers should offload their logs to separate volumes for **persistence beyond a container's short lifespan.**

Goals:

1. Standardizes upstream sources to latest software builds
2. Recommends persistent logging for better analysis and incident response
3. Establishes container build review processes
4. Ensures frequent updating by limiting container lifespan

http://go.iu.edu/2i6f

Incident Response Plan

Adopted 1 Dec 2019

The Incident Response Plan covers policies and procedures for handling incidents that affect infrastructure owned or operated by the OSG, or software developed, maintained, or distributed by OSG.

An information security incident is an occurrence that potentially jeopardizes the confidentiality, integrity, or availability of information or an information system.

This policy is regularly tested by performing table top exercises designed to simulate a real incident.

Goals:

1. Minimize negative impacts
2. Protect confidentiality of non-public information entrusted to OSG systems and services
3. Keep OSG stakeholders informed
4. Collect information needed to understand specific impact
5. Maintain operational availability of OSG services
6. Collect evidence needed for identifying or prosecuting perpetrators

http://go.iu.edu/2i6g

This project is supported by National Science Foundation under Cooperative Agreement OAC-1836650. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.