Master Information Security Policy & Procedures
Open Science Grid

v1.0
Last updated on 12/1/2019

Authors: Zalak Shah, Mike Stanfield
Information Security Officer: Mike Stanfield

1 Introduction

This document represents the core information security policies and procedures for Open Science Grid (OSG), including information security-related roles and responsibilities; references to other, special purpose policies; and the core procedures for developing, implementing, and maintaining an information security program.

Our information security program is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security and levels of information-related risk. This program entails ongoing activities to address relevant policies and procedures; technology and mitigations; and training and awareness.

This document is intended for the OSG Security team and OSG stakeholders.

2 Roles & Responsibilities

2.1 Management / Leadership

The OSG Executive Director accepts risk on behalf of the organization, with advice from the Information Security Officer. The Executive Director will work directly with the ISO to ensure that s/he stays abreast of major security issues facing OSG, as well as the organization's security posture. Any new or changed security policies must be accepted by the Executive Director before they are put into effect.

The OSG Executive Director at the time of this policy's execution is Frank Wuerthwein. The current Executive Director and Executive Team can always be found at https://opensciencegrid.org/management/#executive-team.

2.2 Information Security Officer (ISO)

OSG maintains a position of Information Security Officer (ISO), who reports to the OSG Technical Director, Miron Livny, and the OSG Executive Director. The ISO has responsibility for overseeing and coordinating the information security program. The ISO maintains all security policy and procedure documents for OSG, including this document. All reviews of OSG-wide security policies and procedures are coordinated and archived through this office. The ISO's office also documents any exceptions made to security policies.

The ISO is the first point of contact for any request for clarification of OSG information security policy and procedures. The ISO will coordinate information security incident response, including correspondence between the affected staff and users.

As of the date of publication of this document, the Information Security Officer is Mike Stanfield.

Contact information for the ISO follows:

ISO:	Mike Stanfield
Email address:	stanfiem@iu.edu
Office phone:	812-856-1385
OSG Security team:	security@opensciencegrid.org

2.3 Project Personnel and Staff

It is the responsibility of each individual working for OSG to review and respect these policies and procedures. It is also the staff member's responsibility to understand the underlying policies that drive those detailed procedures, so that the individual is able to make rational decisions in situations not specifically covered by the detailed procedures.

Each staff member is expected to immediately report any known or suspected violations of security procedures, or known or suspected information security incidents to the security team. In all cases, the staff member and the time of the incident will be documented in order to support a timely analysis of and coordinated response to the situation.

2.4 External Users

External users are responsible for reviewing and respecting the following policies while using OSG resources:

- Open Science Grid Acceptable Use Policy
- Open Science Grid Privacy Policy
- Policy on OSG use by Commercial Entities

3 Developing, Implementing, and Maintaining Our Cybersecurity Program

The goal of the OSG is to advance open science through distributed high throughput computing. Our Cybersecurity program is an essential component in support of this goal. Both the information security risk management processes, and possible exceptions to these processes are evaluated by the management, ISO, staff, and external stakeholders with an eye towards this overarching goal.

3.1 Information Security Risk Management Processes

The Security team is responsible for identifying, assessing and managing risks to the Open Science Grid project, as well as providing guidance and training to other teams within OSG in order to enable OSG's continued security.

Goals

The first goal of OSG Security is always the integrity and trustworthiness of OSG-run services and OSG-distributed software. Second to that is the confidentiality of information entrusted to OSG. Third is our availability: we will explicitly sacrifice uptime in an incident by taking down an affected system temporarily, if doing so mitigates risk to the integrity of software and services, or confidentiality of data.

Software vulnerabilities handled by the OSG security team will be handled with the following priorities:

1. Top priority: OSG-developed or OSG-maintained software
2. Second priority: OSG-distributed software which is not developed or maintained at OSG
3. Best effort only: We may issue advisories about other software on a best-effort basis only, when it is obvious that the community would benefit from such action.

Process

The OSG Security Team will endeavor to raise the maturity of OSG's security program over time, through acquiring appropriate resources, helping teams get baseline best practices in place, providing security expertise to other OSG teams, and managing security incidents. The security team will also reach out to VO and resource provider security contacts to enable them to learn best practices for security with regard to their relationship with OSG.

The security policies of OSG will be reviewed by the security team at least once every two years and updated as necessary.

3.2 Exception Management

In order to request an exception to a particular policy, send an email to security@opensciencegrid.org with the following details.

1. Name, version, and URL of the policy to which you want to make an exception
2. Name of the requester
3. Scope of the request, i.e. what would be done differently than specified in policy, for how long, and in which code or system(s). Please be as specific as possible about the implications of the request: the more research we must do, the slower our response time will be.
4. Justification for the request, i.e. why it is a necessary exception

The Security team is responsible for evaluating exceptions and the ISO (or delegate) will approve (or disapprove) most exceptions. Exceptions which may present new risks to OSG will be passed up to the Executive Director along with Security Team recommendations regarding approval, approval with mitigations, alternatives, or disapproval. The Security team will review

the exceptions at least annually or after the approval period is over, whichever comes first.

The Security team will own the risk for the exceptions that are approved by the ISO (or delegate). The OSG Executive Director will own the risk for the exceptions that are signed off by them.

The Security team will maintain a spreadsheet of approved/disapproved exceptions: OSG Security Policy Exceptions Catalog.

3.3 Enforcement

Violations of OSG information security policies can result in loss of access to resources and services, and/or disciplinary action. Activities in violation of any laws may be reported to the proper authorities for investigation and prosecution. Anyone who believes that there is a violation of any information security policy or has a related question should contact security@opensciencegrid.org.

3.4 Modifications to Information Security Policies and Procedures

The Information Security Officer (ISO) is responsible for coordinating changes to established policies and procedures. Requests for changes to established procedures should be presented to the ISO who will analyze the feasibility and cost of changing the procedure. The ISO will also collaborate with the staff responsible for implementing the recommended change before making a decision. The ISO recommends all internal changes to policies and procedures to the Executive Director, who has final approval. The final version of the policies and procedures (PDF format) are uploaded on Google Drive and the URLs to those are shared with the appropriate OSG personnel via email.

4 Resources & Key Contacts

- Resources
  - Open Science Grid Security Documentation
  - OSG Security Announcements
  - OSG Service Catalog
- Key Contacts
  - The OSG areas and their coordinators
  - OSG Security Team: security@opensciencegrid.org

5 Other Policy and Procedure Documents

In addition to this Master document, OSG has adopted the following additional policies and procedures.

- Incident Response Policies and Procedures- A pre-defined organized approach to addressing and managing a security incident.
- Policy and Procedure to approve OSG Connect accounts - users requesting OSG Connect account needs to satisfy the requirements mentioned in this document in order to be approved.
- OSG Service Container Security Policy
- Procedure for Vulnerability Management
- Open Science Grid Privacy Policy
- Open Science Grid Acceptable Use Policy

6 Terms and Acronyms

- OSG (Open Science Grid): A consortium dedicated to the advancement of all of open science via the practice of Distributed High Throughput Computing, and the advancement of its state of the art.
- ISO (Information Security Officer): The person who is designated as the responsible party for information security within OSG. This person is lead for the OSG Security Team.

***

This document is based in part on
Trusted CI's Master Information Security Policies & Procedures Template, v2.
For template updates, visit trustedci.org/guide.