**Survey-DATA**

*1) Which core service or asset are you reporting for?*

The OSGEDU VO. Please realize that the underlying service is not run by Tim Cartwright (owner of the VO) but by the GOC, so many of the answers are “The VO is run by the GOC”.

*2) Have you read the OSG Security Plan, Data Integrity section 2.3.3 within the past 12 months and understand your responsibilities for the proper handling of Sensitive Personal Data, Restricted Data, Limited Distribution Data and Public Data. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389*

No, not within the last 12 months.

*3) If your service does not store, process, transmit any data, you may indicate it here and conclude the survey.*

We store, process, and transmit data.

*4) Are you the owner of the data? The data owner is responsible for collection, storage, and treatment of the data. Although you own the core service/process, there may be another person who owns the data. If so, please provide his/her name below, and answer the following questions with that person.*

Yes, Tim Cartwright is the owner.

*5) Please enter data name you own along with a very brief description and the data type. The data types are explained in Section 2.4.3* *https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389.*

*5-A) Name*

*5-B) Description*

*5-C) Type*

Section 2.4.3 is about scanning: you mean Section 2.3.3.

Name: VO membership information

Description: Names, DNs and email addresses of members of the OSGEDU VO

Type: Public

*6) What is your data backup policy (e.g., weekly full, daily differential, etc.) ?*

This is determined by the GOC, which runs the underlying VOMS Admin server.

*7-A) How long do you retain the back-ups?*

No idea, we leave this to the GOC.

*7-B) How do you ensure that your data back-ups are stored correctly, protected and restorable?*

We don’t. However, membership in the OSGEDU VO is not critical data.

*8) Please list your on-call support email address and/or phone number in case of emergencies, such as unexpected power loss, security attacks or natural disasters.*

There is no support for the osgedu VO.

*9) Are you aware of any attacks against the data? What do you think is the biggest threat against the data?*

We are aware of no attacks. The biggest threat is losing all the data and quite frankly, it does not scare us, because this is a VO meant for temporary usage by students.

*10) If you own Restricted Data please answer the following questions.*

There is no restricted data.

11) If you do not own any limited data, skip to Question 12.

There is no limited data.

12) If you have any public data, please answer the following questions

12-A) What are the, if there are any, access control mechanisms applied to your Public data to maintain its integrity? (An example would be a list of the authorized people who can modify the data.)

We use the controls provided by VOMS Admin: only a VO administrator can maintain the membership in the VO.

**ConfigMgmt**

*1) Which core service or asset are you reporting for?*

The OSGEDU VO

*2) Please indicate if you have read the OSG Security Plan, Configuration Management section 2.4.4 within the past 12 months and understand your responsibilities for Monitoring, Version Control and Security Review of the OSG Core resources under your control. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389 \**

No, not within the last 12 months.

*3) How do you ensure that your service's configuration variables are not modified by unauthorized parties? How can you detect if unauthorized changes are made?*

We rely on the GOC for access to the software installation.

*4) Please indicate the version control system you employ for tracking changes to your service configuration. For e.g. do you maintain a change log that could be used to track and rollback any changes to configuration?*

We rely on the GOC.

*5)Please indicate the process of approving configuration changes for your core OSG service. Specifically what steps are taken to review the security implication of the proposed changes*

We rely on the GOC.

**VulnMgnt**

*1) Which core service or asset are you reporting for?*

The OSGEDU VO

*2) What system do you use to report and track vulnerabilities of your core service. E.g. Do you maintain vulnerability logs?*

We rely on the GOC. We don’t know what they do.

*3) What steps do you employ to mitigate vulnerability to your core services. For e.g. What types of vulnerability scanning are being done? Do you have regular scheduled updates/maintenance schedule to fix known vulnerabilities?*

We rely on the GOC. We don’t know what they do.

**Phys**

1) Which core service or asset are you reporting for?

The OSGEDU VO

*2) Please indicate if you have read the OSG Security Plan, Physical Access Control and Site Management section 2.4.6 within the past 12 months and understand your responsibilities for the OSG Core resources under your control. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389 \**

No not in the last 12 months

*3) Physical access to all production core OSG systems must be controlled -- with a lock, key, etc.  Verify that your core OSG resources comply with this requirement and are indeed in an access controlled area, as defined above.*

We don’t know, but it’s run by the GOC and we assume they do this.

*4) Who among your team currently has root and sudo access on the OSG systems providing core services and what is the policy of granting such access?*

The GOC

*5) According to the OSG Security Plan, network login or command line access to a production core OSG system shall be permitted only from a client via secure authorization and authentication mechanisms. Describe which authorization and authentication mechanisms you are using for secure network login or command line access by privileged staff versus unprivileged users.*

We rely on the GOC for this.

*6) All production core OSG systems shall run the absolute minimum set of network services required for their functions. Have you verified in the past year that your core OSG resource systems are running only those network services necessary for system operation? Also list the network services running that are deemed NOT necessary.*

We rely on the GOC for this.

*7) All production core OSG service providers must have a plan describing redundancy or other mechanisms used to maintain service availability in case of operational disruption or emergencies. Please describe the redundancy plans that would be deployed for your core service to ensure availability in case of unplanned disruption or emergency.*

We rely on the GOC for this. As far as we know, there is no redundancy, but there is no SLA for the OSGEDU VO so it really doesn’t matter.

*8) On each production core OSG system, a copy of the system and service logs shall be saved on line for at least 30 days. Have you verified within the past year that this requirement is being met?*

We rely on the GOC for this.

**Auth**

*1) Which core service or asset are you reporting for?*

The OSGEDU VO

*2) Indicate that you have read the OSG Security Plan, Access Control section 2.5.2 Scanning section 2.5.3 within the past 12 months and understand your corresponding responsibilities for the OSG Core resources under your control. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389 \**

No, not in the last 12 months.

*3) What authentication mechanism is employed for privileged access to core resources*

X.509 certificate access.

*4) How is privileged access to core resource granted and what authorization technique is used?*

We use VOMS Admin to control access. It uses X.509 certificates and limits access to VO Admins.

*5) What are the authentication and authorization techniques used for non-privileged user access?*

None — there is no authentication or authorization for non-privileged users. Everyone in the world is allowed to see the membership of the VO (which is the only non-privileged operation.)

*6) At what frequency are you scanning web services for vulnerabilities and what types of vulnerability scanning are being done?*

We leave this to the GOC.

*7) What remedial procedures are followed when vulnerabilities are detected?*

We leave this to the GOC.

*8) What steps are being taken to scan for local vulnerabilities/intrusion detection and how often?*

We leave this to the GOC.