Data Integrity

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

DocDB. Osg-docdb.opensciencegrid.org

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? See [OSG Security Plan](https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389)

Yes.

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

DocDB is a file storage and management system.

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.

Any user of DocDB assumes responsibility for the data they upload.

5. Please enter data name you own along with a very brief description and the data type. The data types are explained in Section 2.3.3 of the [OSG Security Plan](https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389)

5A. Name

Document data.

5B. Description

Conference proceedings, talks, posters, outreach docs et cetera. OSG Member and OSG Staff groups, OSG Finance, Plans, and Security Groups.

5C. Type

Public data, Limited access data, Restricted access data.

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

Incremental data is backed up daily. Full backups are done monthly. Backup data is kept by the Fermilab Core Computing Division Storage Network Services group for a period of one year via the “tibs” backup system.

7. Backups

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

Backup data is kept by the Fermilab Core Computing Division Storage Network Services group for a period of one year via the “tibs” backup system.

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

Fermilab CCD Storage Network Services group provides backup services.

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.

Contact the Fermilab Service Desk at 630-840-2345 or [servicedesk@fnal.gov](mailto:servicedesk@fnal.gov). The DocDB application administrator staff can also be e-mailed at docdb-adm@fnal.gov.

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

We are not aware of any attacks. If username and password access are used, a third party could determine the password and view, modify, and delete documents or put code in meta-data that would be executed in users’ browsers. A new version of DocDB that enables single sign-on is in progress.

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

10A. Who are the authorized people who can access this data? How do you determine this list of people?

Each individual DocDB user chooses the appropriate access level for the document they are posting or updating.

10B. Do you inform the authorized people about how they should treat restricted data?

The OSG DocDB home page, <http://osg-docdb.opensciencegrid.org> contains this information.

10C. Which access control mechanisms applies to this data?

Certificate authentication is used to allow persons to view and modify the data. When a user accesses DocDB with their current certificate for the first time, they must apply for access to particular security groups. Membership in these groups determines what documents they are able to view and modify. If a user’s role within the organization is unknown or if the user applies to a group to which their membership is questionable, their application is submitted for approval to an “owner” of the particular security group data.

It is also possible to use unencrypted username and password access if the username and password are given to users.

10D. Do you keep a log of accesses to the data?

Yes.

10 E. And if so, how long do you keep the log files?

4 weeks locally, but Apache logs are also sent to Fermilab security.

10F. What information is recorded in the log files?

IP address, URL accessed and time of access are retained.

10G. How do you terminate rights of authorized recipients? Which mechanisms are used to achieve this?

Their access to DocDB is manually removed. There is no automated process in place to ensure that people leaving the project are removed from DocDB. Periodically, the DocDB administrator sends email to the “owners” of the various DocDB security groups with a list of members and asks if any of those members should be removed.

11. If you do not own any limited data, skip to Question 12. If you have multiple data under restricted category and each one has different answers for the following questions, please answer the questions for each data separately

11A. Who is authorized to access the data? How do you determine this list of people?

When a user arrives at DocDB with an approved certificate type for the first time, they must apply for access. They are manually added to one or more of the various security groups. If their requested membership in one of these groups is questionable, their application is forwarded to the “owners” of those particular security groups for approval before they are granted access.

11B. How do you communicate the security requirements to the data to authorized recipients? Do the recipients agree to the requirements? Do you keep record of such communications in a way that can be audited?

The OSG DocDB home page, <http://osg-docdb.opensciencegrid.org> contains this information. I don’t think that recipients formally agree to the requirements of that we have any record of such agreement that can be shown or audited.

11C. Which access control mechanisms applies to this data?

Certificate authentication is used to allow persons to view and modify the data. When a user accesses DocDB with an acceptable certificate for the first time, they must apply for access to particular security groups. Membership in these groups determines what documents they are able to view and modify. If a user’s role within the organization is unknown or if the user applies to a group to which their membership is questionable, their application is submitted for approval to an “owner” of the particular security group data. It is also possible to use unencrypted username and password access if the username and password are given to users.

11D. Do you keep logs of access to the data?

Yes.

11E. And if so, how long do you keep the log files?

4 weeks locally, but Apache logs are also sent to Fermilab security.

11F. What information is recorded in the log files?

IP address, URL accessed and time of access are kept.

11G. How do you terminate rights of authorized recipients? Which mechanisms are used to achieve this?

Their access to DocDB is manually removed. There is no automated process in place to ensure that people leaving the project are removed from DocDB. Periodically, the DocDB administrator sends email to the “owners” of the various DocDB security groups with a list of members and asks if any of those members should be removed.

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

12A. 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.)

Certificate authentication is used to allow persons to view and modify the data. When a user navigates to DocDB with an acceptable certificate for the first time, they must apply for access to particular security groups. Membership in these groups determines what documents they are able to view and modify. If a user’s role within the organization is unknown or if the user applies to a group to which their membership is questionable, their application is submitted for approval to an “owner” of the particular security group data. It is also possible to user unencrypted username and password access if the username and password are given to users.

Configuration Management

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

DocDB.

2. Please indicate if you have read the OSG Security Plan, Configuration Management section 2.3.4 within the past 12 months and understand your responsibilities for Monitoring, Version Control and Security Review of the OSG Core resources under your control. See [OSG Security Plan](https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389)

Yes.

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?

The only people who can log into the machine hosting the software are members of Fermilab Unix Server Support, Web Service Administration and DocDB administration groups. The only people who can access the BlueArc file area where the DocDB application and data are stored are the people whom they exported it to, when they made the volume. We do not have a system to check if unauthorized changes are made.

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?

The DocDB software is served from the SourceForge hosting site and uses git for version control. Git has a change log that can be used to track changes and we can roll back to a previous branch if needed. The server’s operating system upgrades and patches are taken care of by the Fermilab Unix Server Support Group. Changes to each individual DocDB instance’s customization file are not tracked, monitored or in version control. However, they are rarely changed and a prior version could be retrieved from backups.

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

DocDB service administration and the machine administration are under ITIL change management. So changes are classified as standard, minor or major and security is reviewed for each type of change appropriately.

Vulnerability Management

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

DocDB.

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

Service Now is used to track bugs, enhancement requests or security changes needed. Incident and Change tickets are retained according to Fermilab policy.

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?

The Fermilab Security group and/or Web Services Administration group does periodic scanning of Fermilab services, including DocDB. We believe they use Nessus for this scanning. Operating system patches are implemented by the Unix Server Support Group on a quarterly basis. If there were an urgent vulnerability, they would patch the system as soon as possible. When we determine there is a critical software vulnerability, development of a fix and software upgrade are planned and implemented using ITIL change management procedures.

Physical/Console Access Control

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

DocDB.

2. Please indicate if you have read the OSG Security Plan, Physical Access Control and Site Management section 2.3.6 within the past 12 months and understand your responsibilities for the OSG Core resources under your control. See [OSG Security Plan](https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389)

Yes.

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.

The DocDB machine is in a Fermilab computer room which requires a card key with authorization for access by the individual with the card key.

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?

Root or sudo privileges are provided to only members of the Fermilab Unix Server Support Group and selected members of the Web Services Administration Group and DocDB Administrators group.

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.

Login to the system is provided only via Kerberos authentication for individual users and k5login access for a docdb and mysql group.

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.

The Unix Server Support Group monitors this aspect of the systems they support and minimize unnecessary network services.

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.

DocDB does not have a redundancy plan. Support is provided on an 8x5 basis. However, DocDB is now on a VM platform with image backup allowing for machine restoration from a range of previous dates.

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 have verified that the Apache logs are kept for 4 weeks. We believe that the system logs are also kept for 4 weeks by the Unix Server Support Group.

Authentication Control

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

DocDB.

2. Indicate that you have read the OSG Security Plan, Access Control section 2.4.2 Scanning section 2.4.3 within the past 12 months and understand your corresponding responsibilities for the OSG Core resources under your control. See [OSG Security Plan](https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389)

Yes.

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

Certificate authentication is used to allow persons to view and modify the data. When a user accesses DocDB with an acceptable certificate for the first time, they must apply for access to particular security groups including a group for privileged access. Membership in these groups determines what documents they are able to view and modify. If a user’s role within the organization is unknown or if the user applies to a group to which their membership is questionable, their application is submitted for approval to an “owner” of the particular security group data. It is also possible to use unencrypted username and password access if the username and password are given out for use with the privileged group. Usually membership in the privileged group is limited to a small number of people. In OSG’s DocDB instance, there are 7 members of the privileged group that have access to administer the OSG DocDB instance.

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

Privileged access would need to be granted by one of the existing members of the privileged group.

5. What is the authentication and authorization techniques used for non-privileged user access?

Privileged access would need to be granted by one of the existing members of the privileged group.

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

The Fermilab Security Group and/or Web Systems Administration Group scan the DocDB web service and contact us if vulnerabilities are found. Nessus scanning (including CGI scanning) has been used. We don’t know how frequently this is done.

7. What remedial procedures are followed when vulnerabilities are detected?

When a vulnerability is detected, it is reported to the DocDB administration staff and management decides whether remediation is needed. When remediation is needed, a development change is planned and implemented using ITIL change management procedures.

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

The Fermilab Security Group and/or Web Systems Administration Group scan the DocDB web service and contact us if vulnerabilities are found. Nessus scanning (including CGI scanning) has been used. We don’t know how frequently this is done.