Security FAQ

This page consists of common security related questions pertaining to the DSpaceDirect hosted service. If you have additional questions not answered below, please contact dspacedirect@lyrasis.org

Security Monitoring

DSpaceDirect provides the following security-focused monitoring:

- Scheduled and automated updates and patch deployment for the hosted operating system and system applications on DSpaceDirect servers
- Continual monitoring for DSpaceDirect service availability, with notifications sent to administrators in the event that the service is experiencing an outage. Outages, whether due to system or application failure or external attack are resolved as quickly as possible by administrative staff.
- Use of SSH intrusion prevention software on all DSpaceDirect servers
- On-going review of known exploits which may affect DSpaceDirect services followed, as needed, by manual patching and updates to limit exposure
- Monitoring for notifications from customers of DSpaceDirect failures, outages, or issues via the ZenDesk support system. Issue tickets are resolved by administrative staff.
- Monitoring of the DSpace technical community discussions for discovered security vulnerabilities. Discoveries of a security vulnerability are followed by coordination of development effort to fix the vulnerability for DSpace and integration of the fix into the deployed DSpaceDirect service.
- Community-based updates to DSpace software testing suites, which run automatically as part of the software build and release cycle, along with community-based manual system testing, coordinated by the release manager, as part of every major software release.

Data Centers and Security Compliance

Amazon Web Services (AWS) is the data center for DSpaceDirect. AWS provides very detailed documentation on their security compliance:

- AWS Security documentation: https://aws.amazon.com/security/
- AWS Compliance documentation: https://aws.amazon.com/compliance/
- AWS Whitepapers (some of which are security related): https://aws.amazon.com/whitepapers/

SOC Certification

The data center we use for DSpaceDirect is AWS (Amazon Web Services). It is SOC certified. See: https://aws.amazon.com/compliance/soc-faqs/

ISO Certifications (e.g. ISO 27001)

DuraSpace / DSpaceDirect does not have any independent ISO certifications. However, AWS (Amazon Web Services), which provides our data center, is ISO 27001 certified. See: https://aws.amazon.com/compliance/iso-27001-faqs/

Authorization / authentication Support

We support:

- IP address / range authorization (e.g. for restricting access to specific collections to "on campus")
- Default DSpace authentication (where DSpace manages all accounts, passwords and permissions)

Please be aware that configuring/managing authorization plugins often requires extra support and/or coordination with local staff at your institution.

Is data encrypted at rest in DSpaceDirect?

No. DSpaceDirect is intentional about not putting any barriers in place for access, preservation or reuse of data. You are welcome to encrypt data yourselves before putting it into storage, however DSpaceDirect will then only share the encrypted data with users. Simply put, whatever you upload into DSpaceDirect is what is then shared (there is no built in facility to encrypt or decrypt data dynamically).

Is data encrypted in transit (upload/download) in DSpaceDirect?

Yes, all calls to DSpaceDirect are encrypted using Transport Layer Security protocols (HTTPS). We require HTTPS for all sites, and do not allow site data to be sent via plain HTTP. All sites also enable HSTS (HTTP Strict Transfer Security) to tell all web browsers to only use HTTPS.

Note, however, there is one exception to this rule. As OAI-PMH requires HTTP, we do allow HTTP access via the OAI-PMH interface only. That said, OAI-PMH only allows access to publicly available metadata, and does not provide any means for file access, authentication, etc.