## DOspace Mentor/Member Database Security Policies

### Acceptable Use Policy

The daily use of this database is to be restricted to DOspace staff only. Maintenance should only be performed by IT support staff and data entry/queries should be limited to staff working in the DOspace Mentor/Member Mentorship program.

This database is to be used to match mentor’s and member’s and to create reports for management purposes. This database is not for other purposes not approved by upper level management. Information is confidential and DOspace property that should not be openly shared unless to serve the needs of a management request or to create a mentorship meeting.

### Acceptable Maintenance, Troubleshooting, and Modifications Policy

As stated in the Acceptable Use Policy this Database should only be modified and maintained by DOspace IT support staff. Maintenance and Modifications to the system must be discussed in advance and planned changes documented. Before modifications are made to the system a solution must be in place to repair the production system in the event a modification damages the production system.

After any changes have been made they must be logged in the DOspace Change Management log. This Policy will ensure that a clear trail of modifications to the system exist and that downtime is minimized.

### New User Access Policy

It is important that all new users are fully aware of policies before beginning their work. When a New User is assigned to perform Administrative or Maintenance tasks to the system they must have a functioning Office365 account. This account will be restricted to the Mentor/Member Database as well as other relevant resources. When a New User applies for an account they will need to sign an agreement stating they have read and understand the DOspace policies for this and other relevant systems.

### Email Use Policy

The Mentor/Member Mentorship Database is based on Access 2016 for Office365. While it does not directly use email in it’s processes email is none the less important to the functioning of the System. Office365 requires a user account which has an associated email address. This email address does not have to be the primary work email of the user however it must still meet all DOspace Work Email Policies

Email addresses are stored in this database. Email is increasingly a crucial part of communication in today’s world. This said not all users have or wish to share an email address, as a result the email field in the database is not used as a key and is not a required field. The email address like all information in this database is privileged and should only be used per Acceptable use policy. When copying emails do not leave them open in printed form and do not convey a mentor/member’s email for reasons falling outside the Acceptable use policy or DOspace management approval.

### Password Policy

To maintain the security of this system sufficiently strong passwords are required. As a cloud resource a Office365 account is a larger target then a local LAN account. For this reason passwords must meet or exceed DOspace complexity requirements. Currently complexity requirements are set at the Office365 admin console which is maintained and documented by the management team in charge of the DOspace Office365 Business account.

### Anti-Malware Policy

Malware is a security concern that is removed by using Office365. While Desktop Anti-Malware can assist in preventing some attacks the majority of threats are to the cloud infrastructure through other internet connected devices. Microsoft maintains the Office365 system and is responsible for the Anti-malware policy on it. Users at all levels do not have access to scan the infrastructure of Office365 for vulnerabilities

As a result of this there are no special policies in place for the database. However all Client Devices under DOspace control which access the Office365 system must meet DOspace Anti-Malware Policy.

### Remote Access Use Policy

The Office365 system should only be accessed by a computer that is in compliance with DOspace Policies. This is because a vulnerable Desktop not on the DOspace campus can in some rare cases be used to damage the Mentor/Member Mentorship Database on Office365.

Due to the nature of the Office365 Cloud Resource the only Remote Access policy is that a user meets the Acceptable use and Password policies. Microsoft provides limited remote access policy features but what is available falls under the Remote Access policies of the DOspace Office365 admin policies

### Data Backup Policy

There is no Backup policy for this project. Office365 as a platform keeps the design of it’s infrastructure as a trade secret. It is only revealed that a large network of servers with virtualized instances and Redundant Disk Arrays is in place to maintain 99% uptime with 100% data retention from multiple layers of fault tolerance.