

ED Usage Requirements

1. All services using the Enterprise Directory's person credentials, currently known as the UUPID and password, must collect and transmit these credentials over a secured communication that ensure end-to-end information integrity and confidentiality such as SSL or TLS.
2. Services will connect to the ED-Auth and ED-ID systems using only LDAPS (SSL version 3) or LDAP over TLS (TLS version 1).
3. Any service wishing to connect to the Enterprise Directory system will have at least one active full-time salaried employee designated as the responsible party and one current technical contact person for the service.
4. Service administrators will not share or proxy their service's credentials in any manner except with the Enterprise Directory system.
5. Services will use a person's UID, not their UUPID, as the principal identifier for that person, though the UUPID may be used to authenticate a person and retrieve their UID.
6. Services will not store any directory information, with the exception of the UID, for longer than a user's application session, at the end of which the information must be destroyed. Services electing to cache a person's information will only store the information in memory (preferably in an obfuscated manner).
7. Services will respect a person's privacy flags such that:
 - a. Services of type "personal" will only display a person's suppressed information to that person.
 - b. Services of type "private" or "public" will never display a person's suppressed information.
 - c. A service will only expose a person's membership in a group to other members of that group if the person's privacy flag for that group is set to "group".
 - d. A service will never expose a person's membership in a group if the person's group privacy flag is set to "private".
 - e. Services used by administrative staff may display any of the above information if it is required to perform their job.
8. Middleware and IRM staff reserve the right to periodically audit, either passively or actively, services to ensure they comply with all rules stated above, or appoint a third party to do so.
9. IRM reserves the right to update these rules as necessary.

____ James Powell _____
IAD, Director

____ Karen Herrington _____
IRM, Representative