Directory Services

The intent of this document is to describe the various directory services offered and supported by the Office of Information Technology (OIT), define boundaries of such services, and identify levels of services all users should expect.

A directory service is a software application—or a set of applications—that stores and organizes information about a computer network's users and network resources, and that allows network administrators to manage users' access to those resources. Several methods are available for individuals and for applications to access data stored in the University's Central Authentication Hub, the X.500 directory.

Definition of Services Provided

The Identity Management group supports the following directory service access methods, which are used to look up information about individuals and services stored in the University's X.500 directory:

**Lookup**

http://www.umn.edu/lookup

The Lookup service provides individuals with basic directory access to “public” information about individuals. Suppressed information is never provided through this access method. Searching with Lookup services can be narrowed through various selection criteria and searching can be done by Internet ID or Display Name (i.e., the person’s name). The Lookup service uses multiple servers and is highly redundant.

**LDAP**


LDAP is a protocol for accessing online directory services. It runs directly over TCP, and is used by applications such as email to obtain “public” information about individuals. Two LDAP servers are used to provide redundancy.

**Finger/Whois (fingerd, whoisd)**

http://en.wikipedia.org/wiki/Finger_protocol
http://en.wikipedia.org/wiki/Whois

Finger and Whois services may be used to identify users and services supported on a variety of servers. The Finger protocol originated as a method to provide status reports on a particular computer system or a particular person at network sites. The WHOIS system originated as a method that system administrators could use to look up information to contact other IP address or domain name administrators. Two Finger/WHOIS servers are used to provide redundancy.
Internet Relay Chat (IRC)

http://en.wikipedia.org/wiki/Internet_Relay_Chat

Internet Relay Chat (IRC) is a form of real-time communication that can be used for synchronous conferencing. It is designed for group discussion forums called channels, but also allows one-to-one communication via private message and data transfers via direct client-to-client. The Internet Relay Chat service is not redundant; service is provided on a single server.

MyAccount

http://www.umn.edu/myaccount

This interface provides users with a mechanism to set passwords, activate account options, and set email options for their individual X.500 directory entry. Access requires login with Internet ID and password. The MyAccount service uses multiple servers and is highly redundant.

Directory Database Feeds

This access method is available in both batch mode and real-time access mode. It provides applications access to both “public” and “non-public” data as deemed appropriate by official data custodians. Approval is needed from sources outside the Identity Management group before access is provided. Requests for access can be made via the Access Request Form at http://www.umn.edu/datasec/security (select X.500 Real Time Data Feed). The Directory Database Feeds service is not redundant; service is provided on a single server.

UCard Photo Retrieval

This allows access to the photos that are stored in the UCard system and which appear on the identification cards of individuals. Access to photos requires the approval of official data custodians. Contact the UCard Office for more information. Two UCard Photo servers are used to provide redundancy.

Service Performance

Hours of Operation

It is the goal of Identity Management to provide directory services 24x7x52. Normal work hours for the Identity Management group are between 8 a.m. and 5 p.m., Monday through Friday, with on-call staffing for after-hour emergencies. Systems are monitored 24x7x52. System status is available at: http://systemstatus.umn.edu.

Change Management

Change Management is the structured approach OIT uses to manage changes to the University of Minnesota IT environment via formal request and approval mechanisms. By employing a consistent, structured approach to change management, we are able to ensure that all changes are efficiently and promptly handled, thereby minimizing the impact of change-related incidents on service delivery. Changes are approved before they go into production as part of the project management (ITGP) process. Directory Services does not go through the CAB process because redundancies built into Directory services will ensure availability of service during scheduled maintenance periods. Maintenance activity is typically done during the business week.

Service-Impacting Maintenance

If a scheduled maintenance activity is expected to impact service, OIT intends that information regarding that maintenance activity will be communicated via the System Status page, the EMAIL-L.
and NET-PEOPLE mailing lists, and other appropriate venues no fewer than 10 business days in advance of the maintenance activity. Redundancies built into Directory services ensure availability of service during scheduled maintenance periods, therefore service impacting maintenance is rarely scheduled.

**Communications**

Communications about maintenance will include the start time, anticipated end time, and a description of the maintenance to be performed (upgrades, patches, etc.).

**Dependencies**

Directory Services is dependent upon the University Data Center power, network, and related systems. The availability of those systems will have a direct impact on the availability of this service.

<table>
<thead>
<tr>
<th>Service</th>
<th>Dependency on Service</th>
<th>Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>There must be power to servers that provide directory services and the X.500 servers</td>
<td>OIT</td>
</tr>
<tr>
<td>Network</td>
<td>There must be network access to servers that provide directory services and the X.500 servers</td>
<td>OIT</td>
</tr>
<tr>
<td>Environment</td>
<td>A room temperature environment is required for servers that provide directory services and the X.500 servers</td>
<td>OIT</td>
</tr>
</tbody>
</table>

**Service Provider and Customer Responsibilities**

**Staffing**

OIT monitors, maintains, and repairs Directory Services systems.

**OIT Duties and Responsibilities**

OIT staff provides support to IT staff in local units in addition to the support offered by the University's 1-HELP service. Any University of Minnesota unit that wishes to use one of these Directory Access Services is encouraged to consult with OIT to determine the appropriate mechanism to deploy for the proposed service. Local service providers can make arrangements with OIT’s identity management group to help with implementation of the appropriate access mechanism. In many cases, servers must be registered with OIT in order to use any of the mechanisms.

All of the stated services use the central X.500 electronic directory services. (Information about X.500 can be found here: [http://en.wikipedia.org/wiki/X.500](http://en.wikipedia.org/wiki/X.500))

OIT will be expected to:

- Communicate and coordinate with IT staff in local units to minimize disruption to end users.
- Meet response and resolution times associated with service-related incidents

**Customer Duties and Responsibilities:**

- Adhere to any related policies, processes, and procedures
- Report problems using reporting procedures described in this service statement
- Provide input on the quality and timeliness of service

**Problem Management**
The operational status of University systems is available online at: http://systemstatus.umn.edu. Whenever possible, users are encouraged to check the status page before contacting technical support.

Users are strongly encouraged to contact technical support resources in their local unit if they are experiencing problems with computers or applications before contacting 1-HELP. Local technical staff will be able to resolve many problems or escalate them to the appropriate levels, helping to increase the speed and effectiveness of the service response. Response time is dependent on the local unit’s technical support processes and policies.

If local technical support resources do not exist or are not available (e.g., outside of normal work hours) users are encouraged to contact the University’s 1-HELP service. (http://www.oit.umn.edu/help):

- On-campus – 1-HELP (1-4357)
- Off-campus – (612) 301-HELP (4357)
- Email – help@umn.edu

1-HELP hours are found at: http://www.oit.umn.edu/help/contacts/

Monday-Friday: 7:30 a.m. - 8:00 p.m.
Saturday: Noon - 5 p.m.
Sunday: closed

Outside of these hours, or on University holidays, callers may leave a message, which will be responded to the following business day.

1-HELP will escalate incidents, when necessary, to appropriate service providers. All incidents and changes reported to 1-HELP will be logged into Service Center, a tracking system.

**Disaster Recovery**

Directory Services is an important service. In the event of a disaster, recovering Directory Services is at a high level of importance. Redundancies are built into the Directory Services system to minimize outages and to ensure that service is restored as quickly as possible in the event of a disaster. Key directory services (Lookup, LDAP, Finger/Whois and MyAccount) utilize multiple servers located in three data centers to provide redundancy.

All directory services currently use DNS round robin, therefore the failover will depend on our removing the affected IP from the DNS. After the IP has been removed, the IP will have to “age out” of various caches. Windows in particular does not always honor the DNS “Time to live” (TTL), although a reboot of the desktop will usually force it to re-check.

If there is a total failure of the service, then all three Data Centers would have been affected. Expected recovery time for the service would be two to four hours after recovery of a Data Center.

Degraded or failed service receives immediate attention and all available resources are brought into force to recover full operations.
Communication
In the event of unexpected service interruption, OIT will update the System Status web page within 15 minutes of service loss identification by OIT's identity management group. A post-mortem analysis will be released after the resolution of the interruption.

Policies
University of Minnesota Information Technology policies are available on the web at: http://www.policy.umn.edu/Policies/it/index.htm

Policies related to this statement include:
Acceptable Use of Information Technology Resources
http://www.policy.umn.edu/groups/ppd/documents/Policy/Acceptable_Use.cfm

User Authentication for Access to University Computer Resources
http://www.policy.umn.edu/Policies/it/Use/SECUREDATA_PROC01.html#authentication

More Information
For more information about this and other OIT services, visit the OIT service catalog.

Service Statement Maintenance
This statement of service will be reviewed annually.
Last revision: June 2010
File Name: Directory Services.doc