OPERATING LEVEL AGREEMENT (OLA) CornellAD	
OLA Number:	Related Service Level and Operating Level Agreements:
Comments: The audience for this OLA is campus IT staff in units wishing to use CornellAD for their Active Directory needs instead of running their own service.	
OLA Revision History	

Date	Author	Version	Description
1/22/10	Andrea Beesing	1.0	First draft
2/22/10	Andrea Beesing	1.1	Revised draft based on Source Review comments
3/15/10	Andrea Beesing	1.2	Revised based on second round of review comments
4/26/10	Andrea Beesing	1.3	Separate general service level commitment from agreement
6/7/2010	Andrea Beesing	1.4	Add service level commitment information back to the body of doc

SCOPE

This agreement is made between <CUSTOMER> ("Customer") and Cornell Information Technologies ("Service Provider") and covers the provision and support of CornellAD, the campus enterprise Active Directory service. CornellAD is the integration of Microsoft Active Directory with Cornell's central IT infrastructure that provides such functionality as access management, account provisioning and deprovisioning, and LDAP directory services. Active Directory is Microsoft's implementation of standard directory and authentication services. It enables unit IT support staff to efficiently manage the computing resources on their network. CornellAD eliminates the need for the local unit to maintain the core Active Directory infrastructure themselves. Campus IT staff can focus on needs specific to their local units.

This agreement is valid for the period beginning 12:01 AM Eastern Time on <START DATE>. It will be reviewed annually with the customer just prior to the beginning of the new fiscal year in July. Addenda may be appended to this agreement, providing they are mutually endorsed by both the Customer and the Service Provider.

CONTACT INFORMATION

Name	Position	Phone Number	E-Mail
Andrea Beesing	Asst Dir, Identity Management	254-7441	amb3@cornell.edu
Steve Edgar	Group Lead, Identity	255-0019	se10@cornell.edu

Steve Edgar	Group Lead, Identity Management	255-0019	se10@cornell.edu
Pete Bosanko	Group Lead, Identity Management	254-8683	pb10@cornell.edu
<Unit head or ITMC representative>			
<Unit AD primary admin>			
<Unit AD primary admin>			

SUPPORTING SERVICE DESCRIPTION

CornellAD is a component of a campus productivity enhancement project launched in 2008.Campus units now running their own Active Directory (AD) instances can choose to migrate to CornellAD and eliminate the costs associated with running their own AD infrastructure. Campus units that have not yet deployed their own Active Directory instances may join CornellAD to avoid the costs of running this infrastructure themselves. CornellAD is designed to delegate as much local authority as possible to campus IT support providers, thereby granting each campus unit maximum functionality, while maintaining a robust, secure infrastructure which adheres to University policy and industry best practices.

In this service model CIT is responsible for keeping the Active Directory directory infrastructure running and providing general campus service functions such as authentication, authorization, and account provisioning. In turn, campus Active Directory OU administrators and IT service providers leverage this infrastructure to deliver services to their end users.

CornellAD benefits and functionality include:

- Capacity planning, redundancy, backup, security, disaster recovery and routine maintenance of the servers which run the CornellAD forest
- Automated population and deactivation of Cornell NetIDs as Active Directory user accounts
- Distributed mechanism with workflow for the creation of GuestIDs and sponsored NetIDs and full integration of these accounts with Active Directory functions such as group membership and the application of Group Policy
- Synchronization with identity data from PeopleSoft and the campus enterprise (LDAP) directory
- Integration with campus IT infrastructure services such as Kerberos authentication, self-service password management, Exchange
- Authentication services
- Authorization services via Active Directory groups
- Ability to use reference groups to control access to local AD-managed resources
- AD Domain infrastructure for desktop management
- Capability of running local versions of software that rely on Active Directory
- Web-based (Quest Active Roles Server) and MMC-based tools
- Central collection and archiving of security event logs for access and changes

Campus IT service providers can determine whether to take advantage of the full range of benefits by becoming CornellAD OU administrators or whether to use only general campus service features such as authentication, authorization, group management and GuestIDs.

SUPPORTING SERVICE HOURS

The core Active Directory infrastructure (domain controllers) and Quest service receive 24x7 support. Support for routine requests from local Active Directory administrators is during regular business hours (Monday through Friday, 8:00 AM to 5:00 PM, exclusive of University holidays). The service is designed to permit routine planned maintenance without service interruption or impact.

SUPPORTING SERVICE AVAILABILITY AND CAPACITY

Availability targets are for the Active Directory infrastructure and do not factor in downtime for services on which Active Directory depends, such as the network and electrical power.

Target availability is to experience no more than three to four hours of total unplanned downtime of the Active Directory infrastructure throughout the calendar year. This target is based on the time it would take to effect an authoritative restore of the Active Directory database. The risk of an event requiring an authoritative restore is considered low.

Target availability is to experience no more than two hours total unplanned downtime for Quest Active Roles Server throughout the calendar year.

Availability targets are for the Active Directory infrastructure only and do not take into account availability targets for supporting infrastructure such as the network and electrical power. It is assumed that such supporting "utilities" have comparable targets.

CornellAD architecture is designed to provide continued service throughout planned maintenance activities.

SUPPORTING SERVICE TARGETS

Account provisioning for NetIDs is concurrent with the creation or reactivation of the NetID. For GuestIDs provisioning is concurrent with the approval of the administrator.

Data synchronization from PeopleSoft to Active Directory, including the update of reference groups: One business day with an overnight batch process

Data synchronization from the enterprise (LDAP) directory to Active Directory: One hour

Response to request for a new top-level OU: One business day for a CIT staff member to contact the customer. Availability of the OU will be negotiated with the customer based on their specific needs. Once the top-level OU is created the unit administrator can add any new OU's below it without the need to contact CIT.

Response to a request to make a change in CornellAD to support a service: 1 business day for a CIT staff member to contact the customer. The schedule for making a decision about the change and implementing an approved change will be negotiated with the customer based on the circumstances.

Time to resolve data error not related to inaccuracy of source data: one hour to two days. The outside time to resolution would apply to a situation where a full synch of from PeopleSoft to Active Directory is required. Errors in PeopleSoft data are the responsibility of the functional office or the individual if the data element is modified by a self-service application (Employee Essentials, Student Center).

Target for turnaround of routine service requests from OU administrators is one business day either for the fulfillment of the request or for a CIT staff member to call or email the requester for additional information. A business day is Monday through Friday, 8:00 AM to 5:00 PM, exclusive of University holidays. Examples of routine requests include 1) the addition or removal of a primary administrator for the top-level OU, 2) password resets for primary administrators, 3) restoring objects in AD, 4) creating a new access template in Quest, 5) approving a DHCP server, 6) adding "allowed DNS suffix" for a department's DNS name.

Examples of non-routine requests include 1) support for the implementation of a new AD-based service 2) schema changes and 3) creating a virtual attribute.

CIT maintains a complete test Active Directory that is integrated with the test instances of other Identity Management infrastructure components. The primary data source for the test system is the PeopleSoft user test instance. The currency of data elements synchronized from PeopleSoft to the test Active Directory is limited to the frequency with which PeopleSoft test is refreshed from PeopleSoft production, usually based on upgrade and testing needs of the customer.

INCIDENT AND PROBLEM MANAGEMENT

Priority 1 and 2 incidents should be reported to the CIT Network Operations Center on any day of the week at any time of day, including holidays: 255-9900 or noc@cornell.edu. Target response time:

Priority 1: CornellAD not available at all - 1 hour or less

If the root cause of the outage is another service on which Active Directory depends (network connectivity, power to the CIT data centers) we will communicate an expected time for restoral (ETR) based on the ETR for that service.

Priority 2: Problem with CornellAD functionality affecting a service critical to the entire campus or security of information for the entire campus (e.g. directory data issue, inconsistency in search results related to indexing) - 1 day or less

Priority 3: Problem with CornellAD functionality affecting non-critical service or having only local impact - negotiated with the customer based on impact to the business unit

AD administrators can report priority 3 incidents by submitting a Remedy ticket to: idmgmt@cornell.edu. Target response time is one business day for a CIT staff member to communicate with the requester with a solution or request for additional information. A business day is Monday through Friday, 8:00 AM to 5:00 PM.

CHANGE MANAGEMENT

CIT's Change Management Process is followed. It includes the following provisions:

- The "standard" maintenance window, which is 5 AM to 7 AM Monday through Friday, and 6 AM to 12 NOON on Sunday mornings. Exceptions may apply.

- Which campus customers are to be consulted before the change is scheduled.
- The purpose of the change and potential impact.
- Procedures for testing the change both before and after the change.
- Backout procedures.
- What additional staff resources will be required during the change window.
- Escalation procedures during complications.
- The Network Operations Center's responsibilities for communicating with the customer throughout the process.

CIT-initiated changes with potential customer impact will be posted to the campus list for notification of planned changes and unplanned interruptions in service: net-announce-l.

RELEASE MANAGEMENT

Servers will be patched according to the process currently in place for the CIT Server Farm: Test servers are patched on the Tuesday following the release of the patch, the test delayed replication server on Wednesday. Production servers are patched on Wednesday in two hour intervals, the production delayed replication server on Thursday morning.

SECURITY AND GOVERNANCE

The individuals designated as primary administrators for each top-level Active Directory OU will be required to read and acknowledge "CornellAD Organizational Unit (OU) Administrator Account Terms of Use" <URL here> prior to the activation of the OU. Any local administrator who creates an administrative account below the top-level OU is responsible for ensuring that the new local administrator has read and acknowledges an understanding of this document.

The CornellAD service will adhere to security requirements as outlined in "IT Security Requirements for Confidential Data": http://www2.cit.cornell.edu/security/requirements/secreqs-confidentialdata.html. The IT Security Office has chosen to treat passwords as confidential data; therefore servers housing passwords or software with privileged access to those servers are managed according to confidential data security standards.

The CornellAD Planning Committee will be the governing body for matters affecting the entire campus AD forest/domain. Each CornellAD top-level unit will be entitled to have a representative on this committee. Examples of questions the Planning Committee will address include: schema changes, naming conventions, security standards/best practices, criteria for granting exceptions to the standard service offering of the OU within the cornell.edu domain.

SERVICE CONTINUITY MANAGEMENT

CornellAD is designed to survive the loss of one of either of the CIT data centers (Rhodes or CCC), with no service interruption. As a priority tier 1 service in CIT's disaster recovery plan, CornellAD will be one of the first services restored following any disaster which takes both data centers out of operation. A documented disaster recovery plan is in place.

CIT is using a combination of on-disk backups, scheduled backups using Tivoli Storage Manager (Ez Backup) and a delayed replication site to ensure the ability to restore data that is inadvertently deleted through human error or malfunctioning processes.

SERVICE LEVEL MANAGEMENT

The Assistant Director for Identity Management in the IT Security Office is responsible for defining this Operational Level Agreement and meeting service level targets.

COST

The CornellAD core infrastructure is a general campus service funded by the appropriation. CIT assumes the costs of the domain controllers, hardware required to support Quest admin tools, and the cost of the Quest software. Costs associated with local campus unit operation of an Active Directory OU and local services it supports are the responsibility of the campus unit. If the campus unit is migrating from a local implementation of Active Directory, CIT will provide documentation and backline support to the unit AD administrators. Hands-on work to move clients and local resources to the CornellAD domain will be the responsibility of the unit. CIT can provide information on contractors available for hire in the area.

RESPONSIBILITIES

The service owner for CornellAD is the Assistant Director for Identity Management in CIT's IT Security Office. This individual is responsible for ensuring that the core CornellAD infrastructure and staffing levels are capable of meeting the service levels described in this OLA and that the OLA is modified as needed to reflect changes in the service offering.

The unit head is responsible for ensuring that there are always two primary Active Directory administrators for the top-level OU and that staff with AD administrator roles have the required skills.

Local AD administrators are responsible for managing users and resources within their own OU's and act as the liaison between the local users and CIT staff who manage CornellAD. Local users should work through the local AD administrators to resolve any problems they are experiencing with the service.

Local AD administrators will subscribe to net-announce-l as the mechanism CIT uses to announce changes to the campus IT infrastructure that may impact their users. It is highly recommended that local AD administrators subscribe to activedir-l and attend the monthly Active Directory Special Interest Group meetings. The logistics for each SIG meeting are posted here: https://confluence.cornell.edu/display/ACTIVEDIRECTORY/Active+Directory+Special+Interest+Group+(ADSIG)

DOCUMENTATION

General documentation about the service is available at: <URL for site describing service> and will be modified as part of the project when changes are made which impact functionality. Documentation for Active Directory administrators is available at <URL for AD admins> and will be modified throughout the year as CIT receives suggestions from the campus community or as we become aware of the need for additional information via forums such as the SIG and discussion list.

ESCALATION

Customers named in the Contact Information section of this agreement should notify one of the Identity Management staff members listed there with complaints and any other matter requiring escalation, starting with the Assistant Director. If that individual is not available, proceed through the other CIT staff on the list. If the customer has difficulty reaching any of the CIT contacts, the Network Operations Center at 255-9900 or noc@cornell.edu can assist in making the connection.

GLOSSARY OF TERMS
A glossary of terms associated with this service is available here: http://www.cit.cornell.edu/services/active_directory/glossary.cfm

APPROVALS:

Name	Position	Signature	Date

AMENDMENT 1

Amendments to this OLA should be listed and approved.

APPROVALS:

Name	Role	Signature	Date

AMENDMENT 2

Amendments to the OLA should be listed and approved.

APPROVALS:

Name	Role	Signature	Date

APPENDIX A:
This space is reserved for any appendix which may have been referenced in the main document.

APPENDIX B:
This space is reserved for any appendix which may have been referenced in the main document.