Service Level Commitment
for
The College of Agriculture & Life Sciences
at
Cornell University

Our web page: http://www.cals.cornell.edu/cals/cals-it/
Our online HelpDesk: http://www.cals.cornell.edu/cals/cals-it/remedy.cfm

I. Overview and Context

Information Technology (IT) support in CALS is provided through the CALS Office of Information Technology (CALS OIT) by teams of IT professionals, working in service areas. Service areas are groups of units (departments and non-academic functions) assembled on the basis of factors such as geographic location and synergy between units, and range in size from about 1200 to 1600 workstations. These support teams consist of an IT Manager overseeing assigned technical staff that may include full-time, part-time, and student employees. Support teams also cooperate in a larger college-wide group to pool skills and resources to solve college-wide IT issues and to cover extended absences.

Funding for support of the actions and activities laid out in this document will be provided by the CALS dean’s office except where such actions and activities are department-specific and/or are described in service area addendums (see section IX.)

II. CALS OIT Support Services

CALS manages a number of centralized services to aid in providing IT support to all service areas. These include:

a. CALSNet and CALS Public Access domains
   i. Managed workstation security policy
   ii. CALS-wide authentication
   iii. Automated patching for Windows systems
b. Managed antivirus with multiple updates daily
c. Security scanning (routine and upon request)
d. Security awareness training
e. IT Intranet web site
f. Business continuity planning and risk assessment

III. Supported Systems

Hardware and software supported under this Service Level Commitment must meet the following criteria:

a. Computers
   i. Computers purchased in consultation with CALS-OIT and owned by Cornell University
   ii. In order to ensure a complete level of support, we strongly encourage departments and faculty to purchase standardized computer equipment for graduate students in consultation with CALS –OIT. Computers owned by currently enrolled graduate students will be supported to the extent feasible given time, circumstances and licensing constraints.

b. Hardware
   i. Computer equipment and peripherals that are under warranty.
   ii. Out-of-warranty equipment will be supported to the extent feasible given time, circumstances and licensing constraints.
iii. In order to ensure support, purchase of equipment must have prior approval of the local technical staff.

c. Software

i. Operating system versions that are fully supported by their vendors. As of March 2010 this includes:
   1. Windows XP SP3 and above
   2. MacOS OS 10.4 and above

ii. All applications that are centrally maintained by Cornell University for University administrative support will be maintained for workability. All other applications eligible for support will be current or one version behind current and will have continued vendor support.

iii. Operating systems or applications installed or configured without the knowledge and oversight of the local support team or in violation of CIT or CALS security policy will not be supported.

d. Equipment located off-campus

i. Support staff will attempt to resolve minor issues with Cornell-owned computer equipment off-campus by phone and/or remote access.

ii. More substantial problems will be resolved by the user bringing the computer to campus.

iii. IT staff will not go to non-Cornell-owned locations to provide support.

e. Networking

In order to avoid potential widespread network problems:

i. Support team members will be tasked with planning, purchasing, installing, and managing network equipment not managed by CIT. Recommendations will meet industry standards. Decisions to utilize other solutions will be the sole responsibility of the department/individual involved.

ii. All networking projects will meet building codes and campus policies and will comply with campus “IT Roles and Responsibilities” (http://www.cit.cornell.edu/oit/Reports/2003/IT_R&R.pdf).

iii. Team members assign and track IP addresses (or manage dynamic lists) on CALS-OIT managed subnets.

iv. The support team acts as a liaison with CIT.

v. CALS-OIT does not support wireless networking that does not use the Cornell Red Rover infrastructure.

IV. Secure Computing

Cornell policy states that “Cornell University expects all individuals using information technology devices connected to the Cornell network to take appropriate measures to manage the security of those devices.”

In order to protect university systems, networks and data, it is critical that secure computing practices be followed. A breach on one person’s computer can affect many people, causing loss of time and resources, and possibly loss of confidential data with widespread ramifications.

a. All systems receiving support from CALS-OIT must be in compliance with the following three policies:

i. Cornell’s “Baseline Security Requirements” policy (http://www.cit.cornell.edu/security/depth/requirements/)


It is the responsibility of all faculty and staff to familiarize themselves with these documents.

V. CALSNet Windows Domain
   a. As described in section IV on Secure Computing, CALS OIT is obligated to uphold the policies of the University regarding secure management of institutional information. To this end, only computers and systems that meet the guidelines as referenced in section IV, shall be granted access to CALSNet resources.

      Note: Access to CALSNet is required in order to access many college administrative systems and information.

      Computers that do not meet the guidelines for joining CALSNet will be provided network access via unmanaged subnet assignment.

VI. Backup of data
   a. All computer systems that support the administration of the college are to be backed up using the campus EZ-Backup service.
   b. Except for some legacy systems, which will cease operation as of July 1, 2010, the service areas do NOT provide local backup solutions. Fileshare services provided by service areas must not be considered viable backup alternatives for any Cornell University data.

VII. Priorities and Response Times
      Response to requests will be handled as quickly as possible given the situation. Response times below refer to the expected time by which initial contact with a support team member will be made, and assume a full complement of IT staff, and normal business hours.
      a. Critical – business critical service down or large number of users affected, response time: 2 hours, other projects may be placed on hold. In order for an issue to remain at the critical level, the requester must be available for consultation if deemed necessary by the IT support staff.
      b. Normal – localized problem affecting normal work, response time 1 business day

VIII. Software Licensing
      a. All software must be properly licensed
      b. End-users who procure and/or install their own software are solely responsible for the legality of said software
      c. Departments/units track and are responsible for software licensing.

IX. Service Area-Specific Exceptions
      In addition to this core shared document, each service area may have exceptions to detail support elements and situations unique to the service area. Exceptions may expand upon or further clarify certain core elements as they relate to the local area, based on available resources in each area. Exceptions may not reduce the amount of service provided as outlined in this document. Exceptions may modify security elements in the core document only with consultation with the CALS Security Officer. Funding for activities and resources in exceptions will be provided by the department. Exception documentation will detail the necessity of the exception, risks incurred, and releases CALS-OIT from responsibility for the stated risks generated by the exception. Exceptions will be reviewed yearly with an eye toward finding a solution that satisfies all parties.

X. Opting out of this Service Level Commitment
   a. Single systems or groups may opt out of this service level commitment.
   b. Anyone opting out of this service level commitment forges support from and resources provided by CALS-OIT
   c. CALS-OIT will be released from all responsibility related to management of these situations.
   d. These situations will be documented and signed off by departments.
e. A separate document, “SLC Outside of the Service Areas” describes this scenario in more detail.

XI. **Overall Structure of the CALS Office of Information Technology**

a. IT Reporting lines are generally as follows (an org chart is available on the IT Intranet website):
   i. Service area technicians report to the local IT Manager
   ii. IT Managers report to the Director of IT.
   iii. Central services staff report to the Director of IT.
   iv. The Director of IT reports to the Associate Dean for Business Administration