Service Agreement

Cornell
Information Technologies

Universal Agreement: Replace items in Blue

TRACKING NUMBER							
Serial #					Version		
0	0	3	5	6	.	0	0

SERVICE AGREEMENT NAME:	
Customer Division/Unit	CIT Service Being Provided
Division/Department	Systems Support

CUSTOMER REPRESENTATIVE NAME	PHONE NUMBER	E-MAIL ADDRESS
Mr. Dobbs	254-1111	abc1
CUSTOMER BUSINESS/FINANCIAL REPRESENTATIVE NAME	PHONE NUMBER	E-MAIL ADDRESS
Ms. Dawson	255-2221	xyz1
CUSTOMER BILLING CONTACT NAME	PHONE NUMBER	E-MAIL ADDRESS

TERM/DURATION OF SERVICE AGREEMENT (check appropriate box and complete associated dates)

☐ ONE-TIME SERVICE	DATE PREPARED	EST. COMPLETION DATE	ACTUAL COMPLETION	CLOSE-OUT DATE	

☐ ONGOING FOR FIXED TIME PERIOD OR WITH EXPLICIT SET OF DELIVERABLES

DATE PREPARED	ESTIMATED SERVICE START DATE	TERM (months/years)	ACTUAL SERVICE START DATE	REVIEW DATE	CLOSE-OUT DATE

X ONGOING WITH NO END DATE	DATE PREPARED	ESTIMATED SVC. START DATE	ACTUAL SERVICE START DATE	REVIEW DATE	CLOSE-OUT DATE
	June 2, 2007	July 1, 2007			

CIT SPONSORING DIVISION		
Systems & Operations		
CIT SERVICE AGREEMENT SPONSOR/OWNER NAME	PHONE NUMBER	E-MAIL ADDRESS
Mariann Carpenter	255-7707	mgc1
CIT SPONSORING PROGRAM MANAGER NAME	PHONE NUMBER	E-MAIL ADDRESS
Brian N Messenger	255-1558	bnm3
CIT SPONSORING DIVISION DIRECTOR NAME	PHONE NUMBER	E-MAIL ADDRESS
Rick MacDonald	255-7409	rsm6
CIT BILLING CONTACT NAME	PHONE NUMBER	E-MAIL ADDRESS
Sophia Darling	255-5025	sad82
CIT ACCOUNT MANAGER NAME (optional)	PHONE NUMBER	E-MAIL ADDRESS

CIT REVENUE ACCT NUMBER for ONE-TIME CHGS					CIT REVENUE ACCT for RECURR'G/PERIODIC CHGS				
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)
R52	4870	1130							

ONE-TIME CHARGES:
Systems Support Rate: $87/hour

CUSTOMER ACCT NUMBER for ONE-TIME CHGS					CUSTOMER ACCT NUMBER for RECURRING CHGS				
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)
					G88	3761			

RECURRING (state whether monthly, yearly, etc.) OR PERIODIC CHARGES (state rate, increment, etc.):

TOTAL VALUE OF SERVICE AGREEMENT*	COLLEGE AFFILIATION (or ADMINISTRATIVE UNIT)
FY08 Estimates: $2,500	Administrative Department

*One-time charges **plus** 12 months of any recurring/periodic charges

SERVICE AGREEMENT

Customer Division/Unit: Administrative Department/Division
CIT Service Being Provided: Systems Support

CUSTOMER ACCOUNT NUMBER DETAIL:

CUSTOMER ACCT NUMBERS for ONE-TIME and RECURRING CHARGES					TO BE USED FOR
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	Detail server names and services in this area. Include account numbers to the left.
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	TO BE USED FOR
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	TO BE USED FOR
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	TO BE USED FOR
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	TO BE USED FOR
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	TO BE USED FOR
Div (3)	Subledger (4)	Obj Code (4)	Proj (3)	Duo (3)	TO BE USED FOR

SERVICE AGREEMENT

Customer Division/Unit: Division/Department
CIT Service Being Provided: Systems Support

Executive Summary

This agreement specifies the terms and conditions of an agreement between Cornell Information Technologies and Division/Department (subsequently to be referred to as "the Customer") for Systems Support Services to be provided by CIT, and the fees to be paid by the Customer (and "Other Party") for the provision of these services.

Statement of Work

Services Description

System Administration services are provided in accordance with vendor recommendations, University policy, and Cornell Information Technologies (CIT) best practices.

Services include:

- Vendor Quotes
  - Currently supported hardware configurations are defined here:

    http://www.cit.cornell.edu/services/systems_support/hardware.html

  - Coordination of hardware delivery and installation in the Rhodes Hall (757) and CCC (B03) datacenters. NOTE: Due to security concerns, shipments that are delivered to CIT without prior coordination with Systems and Operations may be turned away.

- Operating System (OS) Installation Currently supported software is here: http://www.cit.cornell.edu/services/systems_support/os.html

- Signup for the following CIT services:
  - Server Farm
  - Data Network service
  - Storage Farm Disk Space, SAN Storage Area Network: Use is preferred for non-CIT customers and required for CIT customers.
  - EZ-Backup: Use is preferred for non-CIT customers and required for CIT customers.
    - A backup of the Operating System will be configured and maintained by CIT Systems Support. Application and user data backup is the responsibility of the Customer, not CIT Systems Support. See http://nocdocs.cit.cornell.edu/bin/view/Document/BackupPractices

- Systems Software configuration/management: Includes but is not limited to user account creation and changes, groups, DNS, TCP/IP, DHCP, Active Directory, Windows Registry, system configuration, OS startup and shutdown scripts/processes, performance tuning, storage management, auditing/logging, file access permissions, and fail-over software for HA systems (highly available systems, see the Glossary).
- Installation of Remote Management Tools for Systems Support staff use.
- OS Upgrades and Maintenance Patches
- Hardware and System Software Troubleshooting: If the hardware, OS, or specified system utilities do not function according to the vendor's specifications, the problem will be diagnosed and the vendor will be supplied with information necessary for them to resolve the problem. CIT Systems Support will act as the point of contact for vendor support efforts, coordinate vendor access to servers for maintenance work, when necessary, and apply resulting software fixes.
- Operations Support and System Monitoring: In collaboration with the Network Operations Center (NOC), we will provide 24/7/365 monitoring based on NetVigil monitoring software of the health of the server hardware, operating system, and system availability. See http://nocdocs.cit.cornell.edu/bin/view/Document/MonitoringPractices
- Hardware capacity planning assistance.

Service Location

CIT offers support for servers that are located in the CIT Server Farm (Rhodes Hall, 7th floor) and the CCC (B03) data centers.

Service Hours

The target goal for system availability is 24/7/365 except for system maintenance windows or a service break. A service break is a failure that:

- brings the service down in a disruptive fashion (e.g., database crash, web server outage, service failure) and
- is a result of an Operating System software and/or hardware failure.

Maintenance Windows

Maintenance activities will be scheduled during CIT's standard maintenance windows:

- 5 A.M. to 7 A.M. Monday through Friday
- 6 A.M. to 12 noon on Sunday mornings
- Beginning 6PM Wednesday evenings for Windows OS updates.

All maintenance will be coordinated with an authorized Customer Representative designated by the Customer (see "Customer Responsibilities"). Schedules will be mutually agreed upon.

Exceptions may include, but are not be limited to, work which must be done to prevent or minimize physical risk or damage to people and facilities (smoke, fire, etc.), liability/litigation risk (unauthorized access to protected information), risk to other servers (including security hacks or vulnerabilities), or other such conditions that warrant emergency response.

Change Management

Customer requests for changes during CIT's standard maintenance windows need to be negotiated with the Manager of Systems Administration. Campus notification of all changes are processed through CIT's Change Announcement process.

http://www.cit.cornell.edu/services/noc/change/change-announce.html

It is the responsibility of the application owner and/or the Customer to notify the staff that uses those applications of these scheduled outages.

Customer Support

Routine requests (such as user account creation/changes, troubleshooting of non-critical issues, and any work which can be coordinated in advance) must be made by email to systems-support@cornell.edu

For urgent matters (such as the complete outage or severe impairment of a server/service) call the NOC at (607) 255-9900.

Work requests entered into the NOC log or the systems-support email log will constitute Customer authorization for work to be done by CIT. Only authorized Customer Representatives can make requests for services defined in the terms of this agreement. If appropriate, the Customer may provide an authorization list by server.

Response and Resolution Goals

CIT's goal is to respond to non-urgent support requests that are sent to systems-support@cornell.edu within two business days. The response will include both a confirmation that the problem has been assigned to a systems team member, and the best available estimate of when a resolution to the problem can be achieved.

Urgent requests, made during or outside of normal University business hours (M-F, 8:00AM-5:00PM), should be made by calling the NOC (607-255-9900). The NOC will contact the on-call Systems Support staff to respond to the problem.

Notification Procedure

When the NOC staff and/or automated systems monitoring tools detect a problem related to the server hardware, operating system, or supported systems utilities (not applications), the NOC will follow the System Support predefined on-call procedures.

When the NOC, CIT Systems Support staff, and/or automated systems monitoring tools detect a problem related to an application (not hardware or systems software) the Application/Service Owner will be notified through the predefined on-call procedures provided by the Customer.

Security

We comply with CIT's published security policies. Some Customers require exceptions, which are resolved on a case-by-case basis with CIT's Security Office, using the best available technologies to meet the business requirement, while minimizing security risks. Application security is the responsibility of the Customer, not Systems Support.

Printing

Print queues are defined as required by the Customer. Printers are not supported by Systems Support. We work as necessary to link print queue definitions to those printers as appropriate.

Service Reviews

Regular meetings with Customers are routinely scheduled and service level concerns can be addressed at those meetings.

Unsatisfactory service provisions, or failure to meet the terms and conditions of this agreement by

either party, should be documented as close as possible to the event in question. This documentation should be emailed to the CIT and Customer Representatives listed on the cover sheet of this Agreement.

The CIT Service Agreement Sponsor/Owner will query the Customer Representatives to evaluate and assess the services provided under this agreement and to review anticipated additions or deletions.

Cost Recovery and Billing Information

Non-CIT servers housed in the Server Farm are charged on an hourly basis at the published CIT hourly rate shown on the cover sheet of this Agreement; CIT servers are charged for System Administration services via an internal Client/Systems annual "building block" assessment. Billing will be affected monthly by the CIT Finance Office via the university's Journal Entry Management System (JEMS). Questions concerning billing should be addressed to the "CIT Billing Contact" listed on the cover sheet of this Agreement.

Unless otherwise stated, pricing is subject to change at the beginning of each university fiscal year (July 1). Every attempt will be made to notify the Customer of the impact of such annual pricing changes on or about April 1. A formal revision to this Agreement (or amendment, if appropriate) will be provided for Customer signatures prior to the implementation of any such pricing changes or the Customer may request modification or termination of this Agreement at that time without any termination penalty.

Customer Responsibilities

The Customer is directly responsible for the following:

- Provide (locally or via contract) the technical knowledge to fully run and support their service application. Systems and Operations does not provide application level support.
- Accept the responsibility for defining their service requirements.
- Accept the responsibility for securing their application/service in accordance with Best Practices defined by the CIT Security Office. http://www.cit.cornell.edu/security/
- Designate the appropriate number of (at least a primary and secondary) Customer Representative(s).
  NOTE: Only authorized Customer Representatives can make requests for services defined in the terms of this agreement. If appropriate, the Customer may provide an authorization list by server.
- If new servers are ordered for shipment to CIT, the Customer will consult Systems and Operations for proper delivery instructions. NOTE: Due to security concerns, shipments that are delivered to CIT without prior coordination with Systems and Operations may be turned away.
- Negotiate and procure service/consulting contracts and fees including hardware, OS, and software maintenance contracts for non-CIT owned systems in accordance with customer service requirements.
- Define and enter notification procedures for their application/service into the NetVigil Monitoring software.
- Build NetVigil tests for their application/services, including defining thresholds and on-call procedures.
- Build or buy reporting tools (outside of what is available on NetVigil) as required to meet

customer service requirements.
- Coordinate data backup for application/user data to the EZ-Backup service.
- Promptly notify the NOC if a security compromise is detected or suspected, and comply with University Policy related to computer security.

The Customer will work with CIT to:

- Schedule down time for required maintenance.
- Troubleshoot issues that are not clearly identifiable as either application or system issues, or are identifiable as related to both.
- Adhere to University policy, vendor recommendations and Customer/CIT Best Practices.
- Review NetVigil monitoring tests and thresholds for OS, hardware, and system utilities.

Appendix A

Uptime is determined over a period of one (1) calendar year and is dependent on machine class. The calculation for system uptime does not include maintenance windows, or downtimes due to outages outside of the direct control of Systems and Operations.

Machine Classes

Class A: HA Clusters spanning buildings are targeted for 99.99% uptime
Class B: HA Clusters contained in one building only are targeted for 99.9% uptime
Class C: Standalone systems are targeted for 99% uptime

Availability	downtime per year	downtime per month	downtime per week
98%	7.3 days	14.6 hours	3.3 hours
99%	3.65 days	7.3 hours	1.7 hours
99.5%	1 days 19 hours	3.6 hours	50.4 min
99.9%	8.75 hours	43.7 min	10.1 min
99.99%	52.5 min	4.3 min	1.0 min
99.999%	5.25 min	26.2 sec	6.0 sec
99.9999%	31.5 sec	2.6 sec	0.6 sec

All CIT-supported systems must meet the following minimum baseline configuration to meet availability targets. Systems that do not meet the minimum baseline configuration are less reliable and maintainable and, as a result, are generally less available (i.e., have increased downtime).

Redundancy:
- Redundant power supplies
- Redundant boot drives
- All application/data drives are protected through redundant configurations

Remote Management capability:
- Remote console for Solaris/Linux
- RSA cards for Windows

Serviceability:
- All Systems must have a hardware and software maintenance agreement in place that matches their service requirements (5x9 or 7x24).

Appendix B

Maintaining the confidentiality, integrity, and availability of the data that resides on your service is a shared responsibility. The following guidelines should be followed for the systems that comprise your service. Delegating the responsibility for performing these tasks should occur before the service is brought into production.

Server Configuration

Servers must be configured to reduce any exposures to vulnerabilities that reside in the operating system and applications. This can be done a number of ways:

Patch Management – Operating system and application patches should be applied regularly. Patches should be tested on development systems before they are applied. Patches for remotely-exploitable vulnerabilities should be applied as soon as possible. Other patches can be applied during a regular maintenance window.

Remote Access – Administrative access to the operating system and applications should be restricted to a small set of mechanisms and from a minimal number of sources. To administer Windows systems, Remote Desktop (RDP) should be used. For Unix systems ssh should be used. Through IPSEC filters and Edge ACLs, access to RDP and ssh should be restricted to only those IP addresses or address ranges that require network access to those services.

Monitoring

Operating System and Application Integrity Verification – Integrity verification software checks that files and processes that should not change remain unchanged. Alerts or reports will be generated to indicate when unauthorized or accidental changes occur. CIT monitors certain system processes and configuration files on servers. Customer should consider acquiring additional integrity verification software to monitor their data and applications.

Logs – System and application logs provide a great deal of information to help audit the host and its processes. Analysis of available logging should be performed and reports should be generated regularly.

System Health – Server health describes the availability of the host and its services and the state of the system memory and storage. CIT can perform 24x7 monitoring of system health through the Network Operation Center (NOC). Specific expectations for what constitutes a "healthy system" should be codified before the system is placed in production. These expectations, along with reporting and incident notification expectations should be shared with the NOC.

Intrusion Detection – Intrusion detection software can monitor network traffic and host activity, watching for signatures of unauthorized access. For hosts maintaining sensitive data, an intrusion detection system should be considered as a way to further protect that data.

Network Security

Packet Filtering – Network access to the systems in question should be restricted to only those protocols and IP address ranges that require access to the host. For example, if a service is web-based, only ports tcp/80 and tcp/443 would need to be opened to the host. The rest of the ports could be blocked, which would protect the host from attacks on other services. IPSEC filters or host firewall software should be applied to each host. Complimentary packet filtering can be done via access control lists on the routers (Edge ACLs).

Secure Communications – Where possible, network sessions should be encrypted. This is typically done with SSL. CIT can provide SSL certificates free of charge.

Security Assessment and Consulting

The IT Security Office offers security consulting and assessments to help departments make more informed decisions regarding the security of their services. Vulnerability scanning is available to assess the security of the configuration of the hosts and applications. Ideally, assessments should be performed before a service is placed in production and then quarterly thereafter. These assessments can be scheduled with the IT Security Office directly.

Other Parties to Agreement

Not applicable.

Termination of Agreement

The Customer may terminate this Agreement upon sixty (60) days written notice to CIT.

CIT may terminate this Agreement upon sixty (60) days written notice to the Customer. CIT will attempt, whenever possible, to give the Customer as much advance notice as possible and will make reasonable efforts to minimize any impacts to the Customer, but will not be responsible for any termination penalties not itemized in this Agreement.

Annual Review Process

This Agreement will be reviewed by CIT on an annual basis. If changes/updates are necessary, the Agreement will be modified, reviewed with the Customer and circulated for approval by all required parties.

Modifications to Agreement

Any modifications to this Agreement must be made in writing (via revision or amendment) and will not become effective until approved by all required parties. Either party to this Agreement may request modifications at any time during the life of the Agreement. When modifications are deemed necessary, the party requesting the modifications will contact the other party to initiate discussions and determine how the modifications will be effected. The Customer should contact the CIT person listed as the "CIT Service Agreement's Sponsor/Owner" and CIT will contact the person listed as the "Customer Representative". Once modifications have been agreed upon, the Agreement will be revised by CIT and circulated for approval by all required parties.
As the information contained in the linked pages noted in this agreement is modified, email notification to the Customer will be sent to alert you of the change.

Glossary

This glossary provides explanations of abbreviations and terminology used to assist in the Customer's understanding of the terms and conditions of this Agreement.

HA Clusters[1]

High availability clusters (also known as HA Clusters) are computer clusters that are implemented primarily for the purpose of improving the availability of services that the cluster provides. They operate by having redundant computers or nodes that are then used to provide service when system components fail.

HA cluster implementations attempt to build redundancy into a cluster to eliminate single points of failure, including multiple network connections and data storage which is multiply connected via storage area networks.

HA clusters usually use a heartbeat private network connection that is used to monitor the health and status of each node in the cluster.

Availability[2]

Availability is the ability of an IT Service or component to perform its required function at a stated instant or over a stated period of time. Availability is correlated to the reliability and maintainability of the IT Infrastructure and effectiveness of the IT support organization: Availability depends on the:

- availability of components
- resilience to failure
- quality of maintenance and support
- quality, pattern and extent of deployment of operational process and procedures
- security, integrity and availability of data

Reliability[2]

The reliability of an IT Service can be qualitatively stated as freedom from operational failure. The reliability of an IT Service is determined by the:

- reliability of each component within the IT Infrastructure delivering the IT Service, i.e. the probability that a component will fail to provide its required functions
- level of resilience designed and built into the IT Infrastructure, i.e. the ability of an IT component failure to be masked to enable normal business operations to continue.

Maintainability[2]

Maintainability relates to the ability of an IT Infrastructure component to be retained in, or restored to, an operational state. Maintainability of an IT Infrastructure component can be divided into 7 separate stages:

- the anticipation of failures
- the detection of failures
- the diagnosing of failures
- the resolving of failures
- the recovery from failures
- the restoration of the data and IT Service
- the levels of preventive maintenance applied to prevent failures occurring.

Serviceability[2]

Serviceability describes the contractual arrangements made with Third Party IT Service providers.

[1] From Wikipedia
[2] From ITIL Service Delivery

SERVICE AGREEMENT APPROVALS

Customer Division/Unit: Administrative Department/Division
CIT Service Being Provided: Systems Support

Check appropriate boxes and fill in staff names as needed

Put "X" in box if signature needed — If you would like a copy of final SA, put "X" in box

CIT Approvals:

X	SA SPONSOR/OWNER NAME[1]	SIGNATURE	DATE	
X	PROGRAM MANAGER NAME[1]	SIGNATURE	DATE	
X	DIVISION DIRECTOR NAME[2]	SIGNATURE	DATE	
X	BUSINESS ANALYST NAME[2]	SIGNATURE	DATE	
	FINANCE DIRECTOR NAME[3]	SIGNATURE	DATE	
	VICE PRESIDENT NAME[3]	SIGNATURE	DATE	

[1] Only signatures required for Simple Service Agreement (SSA)
[2] Required for all Service Agreements except SSA
[3] Required for any Service Agreement with value of $100,000 or more

Customer Approvals:

X	REPRESENTATIVE'S NAME	SIGNATURE	DATE	
	Mr. Dobbs	Signature	Date	
X	BUSINESS/FINANCIAL REP'S NAME	SIGNATURE	DATE	
	Ms. Dawson	Signature	Date	
X	Other APPROVALS - Name	SIGNATURE	DATE	

*** * * Area below for CIT/BSC use only * * ***

BSC Checklist

RECEIVED BY:		INITIALS		DATE	
DATA BASES UPDATED BY:		INITIALS		DATE	
COPIES MAILED BY:		INITIALS		DATE	
BILLING VERIFIED BY:		INITIALS		DATE	