

Priority Periods:

There may be certain times during the year when Student Affairs’s business needs require (APPLICATION) to be as reliable as possible and when response to critical problems will be crucial. These priority periods are:

- The week before and two weeks after the beginning of a term
- NSE periods
- Priority registration periods
-
-

Planned Maintenance:

There will be times when EIS needs to carry out planned maintenance activities that may affect (APPLICATION)’s operation. The (business office) Contact will be notified by EIS detailing the nature of the work to be carried out and the time table for completion of the work effort.

EIS will schedule planned maintenance activities around the above Hours of Operation and Priority Periods.

Basic Support:

Information Services (of which EIS is a division) offers a number of services for computing equipment running in its data center. The following services are included in this Service Level Agreement:

- Halon fire suppression
- Uninterrupted power (UPS)
- Conditioned air
- Secured data center
- 24 x 7 operators on duty
- 24 x 7 monitoring of servers
- Problem reporting and tracking
- 24 x 7 Network support

What Happens in Case of a Problem?

Problems with (APPLICATION) can be identified by either (business office) or by EIS.

Problems should be reported to EIS personnel who will create a trouble ticket and assign the ticket to the person who will work on the problem. Problems may also be reported to the Information Services Help Desk (2-3970) who will create a trouble ticket to route to EIS for resolution.

There may be occasions when EIS will identify a problem with (APPLICATION) before it is noticed as a problem by Student Affairs. In these cases EIS will create a trouble ticket to record the problem and then resolve the problem.

The (business office) Contact will be notified whenever a (APPLICATION) trouble ticket is being worked on and when it is resolved.

How a Problem is Worked On

Computer systems today consist of a complex array of servers, workstations, operating systems, database management systems, application software, middleware, web interfaces, networks, etc. (APPLICATION) is no exception in this regard. The following is a general guide as to how EIS will diagnose a problem:

1. Is it a network problem?
Is the campus network experiencing problems? Has there been a failure within the network?
2. Is it a hardware problem?
Is there power to the servers? Does it appear the servers are running? Is there a disk failure? Are there any warning lights or other indicators suggesting problems with hardware?
3. Is it a virus attack?
Is there a known vulnerability for this server configuration? Have all patches been applied?
4. Is it an operating system problem?
Can the server be accessed through standard protocols? Are there indications the server is not responding, or that excessive amounts of memory is being consumed? Is the operating system generating error messages?
5. Is it a middleware problem?
Are Apache, Tomcat and other middleware services running correctly?
6. Is it a database management system (DBMS) problem?
Can we access data? Is the DBMS responding? Are error messages being reported by the DBMS? Are indexes or data files corrupted?
7. Is it an application program problem?
Is the application not functioning as designed? Are error messages being generated? Does it appear incorrect data is either being retrieved or updated? Has a recent update or upgrade of the software been moved to production?
8. Is monitoring software sending out messages?
Are messages indicating server failure? Are messages indicating services failure?

Challenges:

EIS is committed to making every reasonable effort to support (APPLICATION) as noted in this SLA. However, there are things beyond EIS control:

- Attacks by viruses or hackers, including denial of service attacks against the campus network;
- Emergency maintenance;
- Issues with 3rd party software or 3rd party e-mail systems;
- The ability of hardware/software companies to provide support;
- Inadequately tested software.

The (business office) Contact will be contacted by EIS whenever any of the above challenges are encountered to minimize the impact on (APPLICATION). EIS will respond and help identify and resolve the problem as quickly as possible.

Backup Servers:

Only Service Level 5 provides for multiple production servers. Quality assurance, development or spare servers may be deployed as production servers in emergency situations when mutually agreed upon by (business office) and EIS. However, during the time these servers are used for production purposes this SLA will be set to Service Level 2.

Cancellation:

This SLA may be cancelled in 90 days with written notification at any time by (business office) or EIS.

SLA Version and Dates:

Version 1 Begin Date October 19, 2005 End Date August 31, 2006

SLA Review and Updates:

This SLA (including Appendix A-C) can be updated at any time. Any updates must be agreed to in writing by both (business office) and EIS.

This SLA will be reviewed prior to the above End Date by (business office) and EIS.

Signed:

(business office): _____ Date _____

EIS: _____ Date _____

Associate Vice
Chancellor for
Information Services _____ Date _____

Appendix B: List of Related Services

Instructions: List any other services not covered in this SLA that this service relies upon, e.g. EnRoll relies on WAM.

Related servers in Nebraska Hall will be covered under other SLA's.

Appendix C: Service Levels and Supported Activities

Service Level 1	Server installed in IS data center. Basic support is provided.
Service Level 2	A service for which there are only production servers.
Service Level 3	A service for which there are production servers and quality assurance servers. Production servers must have vendor support providing at least 4 hour response.
Service Level 4	A service for which there are production servers, quality assurance servers, and development servers. Production servers must have vendor support providing at least 4 hour response.
Service Level 5	A service for which there are multiple production servers, quality assurance servers, and development servers. The production servers must have highest level of hardware and software vendor support.

Activity	Description	Service Level				
		1	2	3	4	5
Installation	<ul style="list-style-type: none"> Install hardware, software and products in IS managed facilities Ascertain that the hardware/software is properly installed and functioning 	X	X	X	X	X
Basic Support	<ul style="list-style-type: none"> Halon, UPS, etc. 	X	X	X	X	X
Production Support	<ul style="list-style-type: none"> Maintain limited knowledge of the functions of the specific hardware and software required Provide technical support for the software and hardware 		X	X	X	X
Update/Upgrades	<ul style="list-style-type: none"> Maintain the software to the current service release/patch level Notify Contact of service releases/patches Notify users of service releases/patches 		X	X	X	X
Help Desk	<ul style="list-style-type: none"> 7:30 a.m. – 11:30 p.m. every day 	N	N	N	N	N
EIS Support Availability*	<ul style="list-style-type: none"> Normal business hours Extended business hours** Weekend hours** 24 x 7** 		X	X	X	X
Backup/Recovery	<ul style="list-style-type: none"> Backup of data and software Verified recovery of data and software** Offsite storage 	N	X	X	X	X

X – provided N – negotiable

*These are the times during which EIS will respond to reported critical and non-critical problems. The customer must provide appropriate staff and resources to sustain any communications and work efforts beyond normal business hours.

**Requires Help Desk Support.

***Backups of data and software are a reliable way of protecting data and software assets. However, periodic recovery exercises are additional insurance that, in the case of a disaster, a service can be recovered in a timely and reliable manner. EIS recommends that verified recovery exercises be conducted at least once a year.

Glossary:

Critical problems – a complete loss of a core organizational or business process where work cannot reasonably continue; EIS will respond to critical problems within 15 minutes.

Development Server – Environment used for development or enhancement of an application.

Multiple Production Servers – Environment consists of at least two production servers identically configured and connected in a manner that permits the shutting off of any one server without disrupting the service.

Non-critical problems – affected business processes that cause work to be impaired. EIS will respond to non-critical problems within 4 hours.

Production Server – Environment used to run a production application.

Quality Assurance Server – Environment is the same as the production server and used to apply and test new patches and versions of software prior to moving the updates to production.