

# Policies and Services

---

**Information Technology Support Services**

**Office of the Provost**

## Table of Contents

Service Level Agreement—Desktop Support.....	3
Service Level Definition.....	3
ITSS Desktop Support Provided Services.....	3
Service Level Policies.....	5
Service Hours.....	5
Service Expectations.....	5
Contact Methods.....	5
Service Level Agreement—Server Support.....	7
Service Level Definition.....	7
ITSS Provided Services.....	7
Service Level Policies.....	9
Service Hours.....	9
Service Expectations.....	9
Contact Methods.....	10
Services by Department: ITSS Supported Groups.....	11
Sub-Unit Administrator Policy.....	15
Duties.....	15
Responsibilities.....	15
Network Policy—Attaching to File Shares.....	17
Network Policy—New Accounts.....	19
Network Policy—Retired or Release Individuals.....	20
Network Policy—Laptop Administrative Rights.....	22
Glossary.....	23

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

# Service Level Agreement—Desktop Support

## Service Level Definition

A service level policy is a general statement of goals for a service providing organization. Usually, IT service providers create and publish service level policies to clarify expectations and procedures for the delivery of the services provided. A client or user of a service with a service level policy may consistently expect to receive the stated level of service or better. When service is below the stated policy level, a client may expect remedial actions to occur to improve service.

In practice, a service level policy definition includes a number of clauses related to expected types of service. Services may include hours when a phone call or email is answered, response time for incidents involving a production system. Services may be provided at different levels for different times of the day or week.

## ITSS Desktop Support Provided Services

The following services are available from the ITSS group managed through Academic Affairs:

- Computer & Peripheral Support—this provides for general support of computers and attached devices (i.e.—printers) used by a unit
  - Patching/updating
    - Maintaining the patch level of the operating system
    - Maintaining the virus definitions for the virus scanning system
    - Updating software, as needed
  - Hardware Maintenance
    - Hardware diagnostics
    - Replacement of worn/damaged parts internal to the computer
  - Back-up/restore
    - Back-up and Restore of files (limited to files in specific locations)
  - Installation of computer peripherals
    - Printers
    - Keyboards/Mice

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- Etc.
- Installation of Approved and Licensed Software
  - Office
  - Adobe products
  - Etc.
- Outage response
- Automation Support—Automation support consists of services that automate the processes dealing with: software installation, malware protection, and the management and updating of individual client machines (faculty and staff machines). Most of the automation is provided for Windows clients although some automation is available for Apple clients.
  - Group Policy
    - Policies for:
      - Security
      - Drive mapping
      - Printer installation
    - Creation
    - Maintenance
  - ePolicy Orchestrator
    - maintenance of virus scanning
    - notification of infections
  - Systems Center Configuration Manager
    - Software installation
    - Remote tools
  - WSUS
    - Updating windows based machines with:
      - Security patches
      - New operating system features (i.e.—Internet Explorer 7)
  - Print Server

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Service Level Policies

### Service Hours

ITSS Desktop Support offers both in-office and on-call support.

Office hours include Monday through Friday from 8 a.m. to 5 p.m. excluding holidays and other times during which the university may be closed (i.e.—homecoming.)

On-Call support is available during all non-office hours for high priority incidences

### Service Expectations

Service expectations are the expected response intervals from time of support request/incident until resolution.

- Office hours
  - Response within approximately 1 business day of notification
  - Time will be set for a service call based on current work load and severity of issue
- On-Call
  - Not available unless part of service outage deemed mission critical

### Contact Methods

- ITSS support form web site
  - <http://www.aa.ufl.edu/itss>
  - preferred means of contact
  - must be filled out regardless of contact method
  - For use during business hours and for on-call
- Phones
  - Office phone
    - (352) 392-9782
    - For use during business hours—for emergencies involving inability to access computer
  - Cell phones

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- Robert—(352) 256-6347
- Jason—(352) 224-8390
- For emergency use during on-call hours

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

# Service Level Agreement—Server Support

## Service Level Definition

A service level policy is a general statement of goals for a service providing organization. Usually, IT service providers create and publish service level policies to clarify expectations and procedures for the delivery of the services provided. A client or user of a service with a service level policy may consistently expect to receive the stated level of service or better. When service is below the stated policy level, a client may expect remedial actions to occur to improve service.

In practice, a service level policy definition includes a number of clauses related to expected types of service. Services may include hours when a phone call or email is answered. Services may include a response time for incidents involving a production system. Services may be provided at different levels for different times of the day or week.

## ITSS Provided Services

The following services are available from the ITSS group managed through Academic Affairs:

- Sever Support—this provides for general support of servers used by a unit
  - Patching
  - Hardware Maintenance
  - Backup/restore
  - Outage response
- Automation Support—Automation support consists of services that automate the processes dealing with: software installation, malware protection, and the management and updating of individual client machines (faculty and staff machines). Most of the automation is provided for Windows clients although some automation is available for Apple clients.
  - Group Policy
    - Policies for:

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- Security
      - Drive mapping
      - Printer installation
    - Creation
    - Maintenance
  - ePolicy Orchestrator
    - maintenance of virus scanning
    - notification of infections
  - Systems Management Server (SMS)
    - Software installation
    - Remote tools
  - Windows Server Update Services (WSUS)
    - Updating windows based machines with:
      - Security patches
      - New operating system features (i.e.—Internet Explorer 7)
  - Print Server
- Security Response—security response means that the service provider will act as the local Information Security Manager (ISM) for the unit.
  - Responsible for any security tickets opened with University of Florida Incident Response Team (UFIRT)
  - Notification of Helpdesk support personnel of compromised machines
- User Management
  - Creation of exchange accounts
  - Network Managed By (NMB) attribute (for auto groups)
  - Creation and maintenance of groups for security and resource access
- On-call consulting to help with support issues
  - During business hours
  - To be handled through local help desk personnel

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Service Level Policies

### Service Hours

ITSS offers both in-office and on-call support.

Office hours include Monday through Friday from 8 a.m. to 5 p.m. excluding holidays and other times during which the university may be closed (i.e.—homecoming.)

On-Call support is available during all non-office hours for high priority incidences

### Service Expectations

Service expectations are the expected response intervals from time of support request/incident until resolution.

- Sever support
  - Outages
    - Office hours—response within approximately one hour of notification
    - On-call—response within approximately 2 hours of notification
  - Restore from backup
    - Office hours—response within approximately 2 hours of notification
    - On-call—response handled next business day unless deemed mission critical
- Automation Support
  - Available during office hours
- Security Response
  - Office hours
    - Response within approximately one hour of notification
  - On-call
    - Response within approximately 2 hours of notification
- User Management
  - Office hours

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- Response within approximately 8 hours of notification
- On-call
  - Not available unless part of service outage deemed mission critical
- On-Call for Help Desk Consultation
  - Office hours
    - Response within approximately 8 hours of notification
  - On-Call
    - Not available unless part of service outage deemed mission critical

### Contact Methods

- ITSS support form web site
  - <http://www.aa.ufl.edu/itss>
  - preferred means of contact
  - must be filled out regardless of contact method
  - For use during business hours and for on-call
- Phones
  - Office phone
    - (352) 392-9782
    - For use during business hours—for emergencies involving inability to access computer
  - Cell phones
    - Robert—(352) 256-6347
    - Jason—(352) 224-8390
    - For emergency use during on-call hours

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Services by Department: ITSS Supported Groups

The following is a list of the departments supported by the ITSS group, and an individual listing of which services are being provided to each of the supported departments.

- Provost Office
  - Honors, Faculty Development, Office of Institutional Planning and Research, DASS, the Center, Ombudsman, Retention Office, Office of the CIO
  - Services provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
    - Full Desktop Support
- Office of Audit Compliance and Review
  - Services provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
    - Full Desktop Support
- ROTC
  - ARMY, NAVY, AIR FORCE
  - Services provided:
    - Full server support

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- Back-up
- Automation support
  - WSUS (Windows Server Update Services)
  - ePolicy Orchestrator—central management of virus scanning policies
- Security Response
- User Management
- Full Desktop Support
- Phillip’s Center for Performing Arts
  - Phillip’s Center, Baughman Center, University Auditorium
  - Services provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
    - Full Desktop Support
- Web Admin
  - Services provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
- Registrar
  - Services provided:
    - Server Support (Housing and Maintenance)
    - Back-up
    - Automation Support
      - WSUS (Windows Server Update Services)

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- ePolicy Orchestrator—central management of virus scanning policies
- College of Fine Arts
  - Services provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
- Askew Institute
  - Services provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
    - Full Desktop Support
- Graduate School
  - Services Provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
    - Full Desktop Support
- Academic Advising Center
  - Services Provided:
    - Full server support
    - Back-up
    - Automation support

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- WSUS (Windows Server Update Services)
    - ePolicy Orchestrator—central management of virus scanning policies
  - Security Response
  - User Management
  - Full Desktop Support
- AIM
  - Services Provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management
- OASIS
  - Services Provided:
    - Full server support
    - Back-up
    - Automation support
      - WSUS (Windows Server Update Services)
      - ePolicy Orchestrator—central management of virus scanning policies
    - Security Response
    - User Management

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Sub-Unit Administrator Policy

Due to the different needs of a development group as compared to a more standard office environment as well as non-standard working hours, a sub-unit of academic affairs may need a local administrator for their group's computers. This person would be demonstrably capable of first-tier support, i.e.—basic troubleshooting as well as software installation and removal. The local administrator would not be responsible for any second tier support, such as hardware installation or troubleshooting, computer operating system reloads, etc. The local tech would also be constrained from changing any policies set on the computer from the main administrative group.

Need for such a local administrator must be determined and approved by the department head, Provost, and ITSS department head (or network administrator.)

### Duties

- Respond to requests to install software on a machine, while still maintaining the security and integrity of the machine.

### Responsibilities

- Responsible for troubleshooting all software installs which are non-standard
  - Will also be responsible for maintaining patch levels of all non-standard software
- Responsible for first response to all security events (virus, compromise, etc.)
  - In the event of a compromise, will remove machine from network and deliver intact to ITSS

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- Responsible for removal of any unnecessary non-standard software installations
- Will maintain an inventory list of machines
  - List to include:
    - Machine name
    - Non-standard software installed (per machine) with version of software
- May not remove any standard software from machine
- May not reload the machine OS or change policies
  - Any and all reloads will be handled by ITSS staff
- Hardware installation to be handled by ITSS staff

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Network Policy—Attaching to File Shares

- ITSS Maintains file shares for the storage of departmental data
- Access Requirements:
  - A PC or Mac joined to University of Florida Active Directory
  - Installed and updated virus scanning software
  - Computer must have all currently available software updates installed
  - Authorization from departmental supervisor to access data in file shares
- Access Restrictions:
  - Files not work related are prohibited from being placed in the file shares
    - These include:
      - Personal MP3 files
      - Personal pictures
      - Personal movies
      - Etc.
      - This does not include files of this type required for job performance
    - Files found not in compliance with these restrictions will be deleted with 1 (one) business days notice
  - Access from personal/home computers is prohibited
    - Personal/Home computers are unable to encrypt traffic between the File share and the computer
    - Verification of virus scanning and update compliance is not possible, posing a security risk to departmental files
  - Users must accept statement of usage for University of Florida Computers and Network, which will be displayed at logon for each machine joined to University of Florida Active directory and is as follows:

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- The user understands and acknowledges that the computer and network are property of the University of Florida. The user agrees to comply with the University of Florida Acceptable use Policy and Guidelines. The university monitors computer and network activities without user authorization, and the university may provide information about computer or network usage to university officials, including law enforcement when warranted. Therefore, the user should have limited expectations of privacy.

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Network Policy—New Accounts

- Information necessary for creation of new network account:
  - Name (full name including middle initial)
  - UFID number
  - Gatorlink user name
  - Department
  - Position
  - Building & room number
  - Phone number
- Due to work loads, please notify network administrator(s) one (1) week prior to employee's start date for set up of new accounts
- Account requests must come from department heads or appointed designee (designee to be on file with network administrator)
- Email accounts will be created as follows:
  - First initial, last name @department.ufl.edu (i.e.—John Smith: jsmith@aa.ufl.edu)
  - Email accounts will only be created for students at the request of the department.
- Home drives
  - Provided for staff for storage of all work documents. Pictures, movies, and MP3's are prohibited unless work-related
  - Home drives will be provided for students only at the request of the department

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Network Policy—Retired or Release Individuals

- Network Access
  - Department heads (or designee) are required to notify the network administrator(s) of any change in status of an employee which may necessitate a change in that persons network access. This could include:
    - Retirement
    - Termination or non-renewal
    - Leave of absence or sabbatical
    - Transfer, promotion, or other change in job duties
  - Whenever possible, notification should take place no less than one (1) week prior to change in status of employee.
  - Employee may retain email access and address for a period of 30 days after status change, after which the account and any emails contained therein will be deleted. In certain cases, the department head may decide to terminate access on or before the final day of work.
  - Account access to any university systems will be terminated on or before the final day of work (Administration Systems (PeopleSoft, Student Systems, etc), Financial systems, Gatorlink, etc.)
  - Any phone services (such as cellular) will be discontinued or must be transferred to the person or another department.
- Data
  - On or before the final day of work, individuals are required to return to the appropriate responsible authority any and all data owned by the University. They are also required to remove such data from any equipment such as portable hard drives or flash drives or any data that may have been transferred to personal computers via such devices. Note: All record retentions laws must be followed.
    - Examples of data:
      - Student, staff, or financial records
      - Work related text documents, spreadsheets, PowerPoint files, etc

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

- Equipment
  - Equipment must be returned on or before the final day of work.
  - Individuals are required to return to the appropriate responsible authority any and all equipment issued for the performance of their duties, i.e.:
    - Computers, Computer monitors, Printers
    - Fax machines, Copiers
    - Laptops
    - Routers or other network hardware
    - External data devices
      - Hard drives
      - USB storage devices
    - Carrying cases for equipment
    - Phones and accessories
    - Etc.

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Network Policy—Laptop Administrative Rights

- Administrative Rights on laptops restricted to tech support personnel
- A local account to be set up on the machine with administrative privileges
  - Each laptop to have the same admin user name, but different passwords
  - Passwords will be maintained by the computer support department
  - Password to be given out only in the event that a user is remote, and must have admin privileges to correct a problem causing the laptop to be unusable
- Persons leaving on international trips may request the password in advance for emergency use in the event the IT staff is not available
- Laptops must be brought in, after using the local admin password, for diagnostics and to allow the password to be reset

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*

## Glossary

Full server support—General support of servers used by a unit including patching, hardware maintenance, back-up and restore of files, outage response

Back-up—Back-up of data for the purposes of disaster recovery and recovery in the event of file loss

Automation support—services which allow for the remote installation of software, drive mapping, patching of machines, updating of virus scanning programs, etc.

Security Response—taking corrective steps in the event a machine is compromised either by a virus or a malicious hacker

User Management—creation and population of security groups for access to network resources such as file shares and printers, management of the Network Managed By (NMB) for the UF directory

Full Desktop Support—includes installing initial operating system and ancillary programs, installation of specialty software, installation of peripherals (printers, scanners, etc.), troubleshooting errors, replacement of hardware (i.e.—replacing a dead video card)

*Any exceptions to this policy must be approved in writing by the department head, Provost, and the ITSS department head or network administrator.*