Service Level Agreement

March 2010

John M. Duska  
Director, Technical Services  
Information Security Officer

Carrie A. Francart  
Manager, Support Services

Copyright ©2010 – Financial Information Systems, University of Pittsburgh

The latest version of this document is available online at www.fis.pitt.edu.
TABLE OF CONTENTS

Definition of Service Level Agreement ................................................................. 1
Goal......................................................................................................................... 1
Provider of Services .......................................................................................... 1
  Support Services .............................................................................................. 1
  Desktop Services ............................................................................................. 1
  Network Services ............................................................................................ 1
  Application Services ......................................................................................... 2
Customers of Services......................................................................................... 2
Hours and Contact Methods ............................................................................... 2
  Standard Support Hours ................................................................................. 2
  Non-Standard Support Hours ....................................................................... 2
Technical Services Request Submission Methods .............................................. 3
  Urgent Requests ............................................................................................ 3
  Non-Urgent Requests ..................................................................................... 3
  FIS Web Support Portal .................................................................................. 3
  FIS Support Hotline ....................................................................................... 4
  FIS Emergency Hotline .................................................................................. 4
System Reliability and Changes ....................................................................... 4
  Maintenance and Changes ............................................................................ 4
  Customer Commitments for Service .............................................................. 5
Service Goals ..................................................................................................... 5
  Request Submission Response Rate ............................................................. 5
  Call Abandonment Rate ................................................................................ 5
  First Contact Resolution .............................................................................. 5
  First Tier Resolution ...................................................................................... 5
  Incident Resolution Time ............................................................................. 5
  Overall Customer Satisfaction .................................................................... 6
Server Reliability ................................................................................................. 6
  PC Upgrades .................................................................................................. 6
Urgency, Severity Level, and Resolution Times .................................................. 6
  Urgent ............................................................................................................. 6
  Non-Urgent ................................................................................................... 6
  Critical .......................................................................................................... 6
  Serious .......................................................................................................... 6
  Moderate ....................................................................................................... 7
  Routine .......................................................................................................... 7
Services Provided ............................................................................................... 7
  Service Portfolio ............................................................................................. 7
Disaster Recovery ............................................................................................... 9
  Disaster Events and Disaster Recovery ....................................................... 9
    Business Continuity and Disaster Recovery .............................................. 9
    Media Storage ............................................................................................ 9
Customer Accounts ............................................................................................ 10
  Account Limits ............................................................................................... 10
  Account Modifications .................................................................................. 10
  Account Maintenance and Deletion ............................................................. 10
Reporting and Surveying ................................................................................... 11
  Reporting ...................................................................................................... 11
  Surveying ..................................................................................................... 11
Appendix A ......................................................................................................... 12
Professional Certifications .................................................................................................................. 12
ASP Developer Certification .................................................................................................................. 12
Business Continuity Professional Certification .................................................................................. 12
Certified Identity Theft Risk Management Specialist ......................................................................... 12
Certified in Homeland Security (CHS) ............................................................................................... 12
Certified in the Governance of Enterprise IT (CGEIT) ..................................................................... 12
Certified Information Security Manager (CISM) ................................................................................ 13
Certified Information Systems Auditor (CISA) .................................................................................... 13
Certified Information Systems Security Professional (CISSP) .......................................................... 13
Certified Protection Professional (CPP) .............................................................................................. 13
CompTIA Authorized Service Center Gold ....................................................................................... 13
CompTIA A+ Certification .................................................................................................................. 14
CompTIA i-Net+ Certification ............................................................................................................ 14
CompTIA Network+ Certification ...................................................................................................... 14
CompTIA Project+ Certification ......................................................................................................... 14
CompTIA Security+ Certification ....................................................................................................... 14
CompTIA Server+ Certification .......................................................................................................... 14
Dell Warranty Parts Direct Certified .................................................................................................. 15
Global Information Assurance Certification ....................................................................................... 15
HDI Help Desk Analyst of the Year (HDAOY) .................................................................................. 15
HDI Support Center Analyst (SCA) .................................................................................................... 15
HDI Support Center Team Lead (SCTL) ............................................................................................. 15
Help Desk Analyst Certification (HDA) .............................................................................................. 15
Help Desk Manager Certification (HDM) ............................................................................................ 16
ITIL v3 Foundations ............................................................................................................................ 16
Master Certified Internet Web Designer (CIW) ................................................................................... 16
Microsoft Certified Application Developer (MCAD) .......................................................................... 16
Microsoft Certified Desktop Support Technician (MCDST) .............................................................. 16
Microsoft Certified IT Professional: Enterprise Support Technician ................................................. 16
Microsoft Certified IT Professional: Database Administrator ......................................................... 16
Microsoft Certified Professional (MCP) ............................................................................................ 16
Microsoft Certified Systems Administrator (MCSA) ......................................................................... 17
Microsoft Certified Systems Administrator: Security (MCSA: Security) ......................................... 17
Microsoft Certified Systems Engineer (MCSE) ................................................................................ 17
Microsoft Certified Technology Specialist ....................................................................................... 17
Oracle Certified Associate .................................................................................................................. 17
Appendix B ......................................................................................................................................... 18
Vendor Support and Underpinning Contracts .................................................................................... 18
Microsoft Premier Support ................................................................................................................ 18
Microsoft Developer Network (MSDN) Support .............................................................................. 18
Dell Limited Warranty ......................................................................................................................... 18
Dell Laptop Complete Care Accidental Damage Service .................................................................... 19
Appendix C ......................................................................................................................................... 20
Desktop Computer Standards ............................................................................................................. 20
DEFINITION OF SERVICE LEVEL AGREEMENT

This document is an agreement between Financial Information Systems (FIS) Technical Services and the customer, which details what services can be expected given that the department follows all policies and procedures specified in this document and other applicable documents, amendments, and appendices. Any violations to documented FIS policies, including policies in this document and the Guidelines on Use of Information Technology Resources, directly affect the terms of this Service Level Agreement (SLA).

GOAL

The goal of this Service Level Agreement is to define the service provider’s purpose of an uncompromised level of technical support. To provide the highest quality of service to our customers, we use Service Level Agreements to define the roles of both the service provider and service customer, manage the expectations the service customer has for the service provider, explain to the service customer how requests are handled and executed, and enable clear communication between the service customer and service provider.

PROVIDER OF SERVICES

Technical Services, Financial Information Systems, University of Pittsburgh. FIS is committed to being a leader within the University of Pittsburgh by providing innovative solutions through the strategic use of people, processes, and technology. To support the University’s mission of teaching, research, and service, FIS is responsible for providing resources to manage projects, design processes, develop IT standards, implement and maintain systems, protect assets, secure information, and analyze data and services to enhance individual and organizational performance.

FIS Technical Services is comprised of four (4) teams:

SUPPORT SERVICES

Customer service • Incident management • Problem management • Change management • Knowledge management • Service level management • Operational level management • Communications • User consultation and training • Software testing and quality assurance • Security auditing and incident response

DESKTOP SERVICES

PC hardware and software management and support • Software packaging and deployment • Service asset and configuration management • Release and deployment management • Software licensing • Mobile computing support • System and product evaluation

NETWORK SERVICES

Application hosting • E-mail hosting • File sharing • Capacity management • Continuity management • Event management • Availability management • Data retention and recovery • Computer account management • Network printing • Server capacity and performance management • Server availability and continuity management • Disaster recovery and business continuity
APPLICATION SERVICES

Application development management • Release management • Software architecture and engineering • Business analysis and process engineering • Database administration • Web design and development • Business forms development and support • System and product evaluation

CUSTOMERS OF SERVICES

Technical Services supports approximately 600 clients in the Office of Budget and Controller, the Auxiliaries, and other areas including:

Auxiliary Administration • The Book Center • Budget & Controller Administration • Budget & Financial Reporting • The Copy Cat • Financial Information • Financial Information Systems • Financial Operations • Financial Records and Services • Food Services • General Accounting • The Health Book Center • Housing • Institutional Research and Data Management • Internal Audit • Management Information & Analysis • The Office of Finance • Organizational Development and Communications • Panther Central • Parking, Transportation and Services • Payment Processing • Payroll • Planning and Analysis • Property Management • Purchasing Services • Research and Cost Accounting • Risk Management, Insurance and Workers Compensation • Sarbanes Oxley Compliance • Supplier Management • Student Accounting and Billing • Student Appeals • Student Financial Services • Student Payment Center • Tax • Tuition Accounting and Budgeting • University Collections • US Security

These departments are located throughout the University of Pittsburgh’s Oakland campus with the exception of the Motor Pool and Mailing Services, both subsidiaries of Parking, Transportation and Services, and branch campus Panther Central offices, which are off-site locations.

HOURS AND CONTACT METHODS

STANDARD SUPPORT HOURS

*Technical support will be provided during our Standard Support Hours (SSH) from 8:00 a.m. to 5:00 p.m., Monday through Friday*, with the exception of University Faculty & Staff holidays as listed in the University Extended Calendar. Standard business week, as defined in this document, is Monday through Friday (five business days).

NON-STANDARD SUPPORT HOURS

Additional standard support can be requested by the department when support is necessary after hours or during holidays and is subject to approval by Technical Services. All requests for off-hour support must be submitted via e-mail to the Director of Technical Services and Information Security Officer, John Duska, at least five (5) business days prior to the time requested.
### TECHNICAL SERVICES REQUEST SUBMISSION METHODS

All supported computers have a label on the monitor or CPU with the FIS website address and telephone number. Technical Services will not accept requests in person or by personal phone or e-mail.

*Exceptions to these service levels will be made when the organization is in Disaster Recovery mode. See the Disaster Recovery section of this document for more information.*

<table>
<thead>
<tr>
<th>URGENT REQUESTS</th>
<th>NON-URGENT REQUESTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Support Portal and Hotline</strong></td>
<td><strong>Web Support Portal</strong></td>
</tr>
<tr>
<td>• Significant customer impact that threatens immediate productivity, regulatory compliance, cash flow or safety</td>
<td>• Issues that do not affect immediate productivity, regulatory compliance, cash flow or safety</td>
</tr>
<tr>
<td>• Significant number of customers affected</td>
<td>• Customer requests for information and services that are not immediately necessary or time-critical</td>
</tr>
<tr>
<td>• Security of system, network or data is compromised</td>
<td>• Issues that do not require immediate assistance</td>
</tr>
<tr>
<td>• Significant customer concern</td>
<td></td>
</tr>
<tr>
<td>• Network infrastructure outage</td>
<td></td>
</tr>
<tr>
<td>• Issue is time-sensitive</td>
<td></td>
</tr>
</tbody>
</table>

**Support Portal submission**

Via our website at [www.fis.pitt.edu](http://www.fis.pitt.edu). Support Portal submissions require the customer to complete the requested information and include a short description of the problem. **When submitting an urgent request through the web, an analyst will return your call within 5 minutes.** Using the Support Portal is the preferred method of contact.

**Support Hotline submission (4-FIS1)**

If you have an urgent request or are unable to gain access to a computer to submit your request via the website, you can dial **4-FIS1** (4-3471) on any campus telephone to reach our Support Hotline.

### FIS WEB SUPPORT PORTAL

Customers can submit requests for all provided services, including urgent and non-urgent needs, from the FIS Support Portal website at [www.fis.pitt.edu](http://www.fis.pitt.edu). To submit a request, click on the FIS Support Portal link from the FIS website. The Support Portal allows customers to track the status of their requests, ask for updates and changes, and request that the individual working on their incident contact them.
FIS SUPPORT HOTLINE

Technical Services can be contacted at 4-FIS1 (4-3471) during Standard Support Hours. Please only use this number if you are experiencing a technical problem that is urgent or if you cannot access the Web Support Portal.

FIS EMERGENCY HOTLINE

Technical Services offers an emergency hotline in case of an urgent problem during evening or weekend hours. The emergency hotline phone number is 1-866-PITT-FIS. This toll free number should only be used in the event of an emergency outside the Standard Support Hours.

SYSTEM RELIABILITY AND CHANGES

MAINTENANCE AND CHANGES

Technical Services strives to provide our customers with the highest level of server and desktop computer uptime possible. Occasionally, it is necessary to perform regular, routine maintenance on our servers, network, and desktop computers. To make these downtimes as convenient as possible for our customers, Technical Services performs normal maintenance during a pre-defined Normal System Maintenance Period (NSMP). This period is scheduled during off-hours and our staff dedicates themselves to performing these tasks during late evenings or on weekends when it is less likely to disrupt customer work time.

- **Access to business applications and servers are offered 24 hours a day, 7 days a week, 365 days a year, except during Normal System Maintenance Periods.**

- All changes, enhancements, and maintenances are reviewed by the Technical Services Change Management Board and are subject to their approval. The goal of the Change Management Board is to review changes to ensure that they will not cause unnecessary downtime for our customers.

  - NSMP: Regularly scheduled, non-emergency events can cause a service outage or have an impact on performance. Non-emergency enhancements and changes are scheduled as follows (the following outages may result in a possible short loss of service only and are not meant to define long periods of downtime):

    - Computers will be unavailable
      - Tuesdays at 9:00PM until Wednesdays at 6:00AM
    - Servers may be intermittently unavailable
      - Tuesdays at 6:00PM until Wednesday at 12:00AM
      - Thursdays at 6:00PM until Friday at 12:00AM
      - Various times as needed on weekends

  - Changes that are not considered routine and/or are planned for times outside of the NSMP, which result in an extended period of downtime, will be scheduled by the Change Management Board. Technical Services will notify customers of scheduled downtime via e-mail and will strive to ensure that these downtime periods are as least disruptive as possible to our customers.

Non-scheduled emergency changes which require service outages are implemented at the discretion of the Change Management Board. In the event of an emergency service outage, Technical Services will attempt to notify
customers of the outage as soon as possible. If a change is critical or urgent, advanced notification may not be sent.

CUSTOMER COMMITMENTS FOR SERVICE

- All policies listed in FIS’s *Guidelines on Use of Information Technology Resources* and this Service Level Agreement will be followed.
- All University of Pittsburgh defined *policies and procedures* will be followed.
- All requests, problems, questions, and concerns will be submitted according to the Technical Services Request Submission Methods listed above.
- Customers must supply all requested information when filling out forms and documents, including requests for service via the Web Support Portal.

SERVICE GOALS

*FIS reserves the right to take necessary precautions to protect the security of the organization and University data and assets regardless of promised service goals.*

REQUEST SUBMISSION RESPONSE RATE

At least 95% of all requests will be responded to within the above-defined response times.

CALL ABANDONMENT RATE

At least 90% of all calls made to the FIS Support Hotline will be answered.

FIRST CONTACT RESOLUTION

At least 50% of all incidents will be resolved by the first Support Analyst to make contact with the customer.

FIRST TIER RESOLUTION

At least 50% of all incidents will be resolved by Tier 1 Support. These incidents will be resolved by Support Services staff without the involvement of other areas such as Desktop, Network, or Application Services.

INCIDENT RESOLUTION TIME

At least 99% of all requests will be resolved as described below.

- If an incident requires additional time, customers will be notified of approximate resolution time and/or reason for delay.
- Additional time must be allotted for incidents that require a third party vendor involvement for resolution. This includes working with CSSD in resolving customer issues.
• Resolution time will also be affected when an extensive period passes where the FIS staff member is unable to contact the customer or the customer asks for incidents to be resolved at a later date.

OVERALL CUSTOMER SATISFACTION

At least 95% Overall Customer Satisfaction rating based on returned incident surveys.

SERVER RELIABILITY

At least 99.9% server availability during standard support hours. In the event of a disaster, Server Reliability service goals are best effort only. Technical Services has a disaster recovery contingency and server restoration plan.

PC UPGRADES

At least 95% Overall Customer Satisfaction rating based on returned PC upgrade surveys.

URGENCY, SEVERITY LEVEL, AND RESOLUTION TIMES

The following table outlines the urgency of incidents and their associated response times. The urgency of an incident is defined by the customer at the time of placing the request and is used to define the required response time. All Response Times are during standard support hours.

<table>
<thead>
<tr>
<th>Urgency</th>
<th>Response Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URGENT</td>
<td>5 minutes</td>
<td>• High impact on business or immediate productivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requests that are time sensitive</td>
</tr>
<tr>
<td>NON-URGENT</td>
<td>9 hours</td>
<td>• Low impact on business functions and does not affect immediate productivity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requests that are not time sensitive</td>
</tr>
</tbody>
</table>

The following table is used internally by FIS to prioritize incidents and define resolution times. All Resolution Times are during standard support hours.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Resolution Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>Within 1 hour</td>
<td>• Business outage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Significant customer impact that threatens immediate productivity, regulatory compliance, cash flow or safety</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Significant number of customers affected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security of system, network, or data is compromised</td>
</tr>
<tr>
<td>SERIOUS</td>
<td>Within 9 hours</td>
<td>• Significant customer concern</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Production continues, but in a significantly impaired fashion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Issue is time sensitive, but not causing immediate work-stoppage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network file restorations deemed urgent by requesting user</td>
</tr>
</tbody>
</table>
MODERATE

1 business week

• Problem that does not affect immediate productivity
• Network file restorations

ROUTINE

Scheduled with customer or vendor

• Customer requests for information
• Scheduled tasks performed for customers
• Issues that do not affect productivity in a significant way
• Issues that require third party vendor involvement after initial problem is addressed

Exceptions to these levels will be made when the organization is in Disaster Recovery mode. See the Disaster Recovery section of this document.

Please be aware that when CSSD must be involved with an incident, the resolution time may be set to Routine. Examples of incidents requiring CSSD involvement include physical computer moves, IP address requests, computer motherboard replacements, and firewall updates.

SERVICES PROVIDED

SERVICE PORTFOLIO

• Compliance with ITIL (the IT Infrastructure Library) Service Management requirements – ITIL is the industry standard for IT best practices intended to assist organizations with providing quality technical support. ITIL is a customizable framework used by organizations all over the world to help define how Service Management is applied within the organization. ITIL helps FIS align our services with the current and future needs of our customers, improve the quality of the services delivered, and reduce the long-term cost of service provision.

• Computer Hardware and Software Management and Support

• Asset and Configuration Management: Ensures that all assets impacting service are accurately identified and tracked.

• Release and Deployment Management: Ensure that software releases are properly tested before deployment.

• Software licensing and distribution

• Application development and release management: Technical Services has processes in place that handle the planning, design, build, configuration, and testing of hardware and software releases to create a defined set of release components. Release activities also include the planning, preparation, scheduling, training, documentations, distribution, and installation of internally developed applications to many users and locations.

• Website Design and Development

• Business Process Engineering

• Project Management
• System and Product Evaluation Consultation
• Customer Account Management
• E-mail Hosting
• Application Hosting
• Network Printing Services
• Capacity Management: Ensures proper tracking and reporting on server capacity, utilization and forecasting.
• Continuity Management: Ensures the development and maintenance of all server disaster recovery and business continuity plans.
• Event Management: Provides proper tracking and reporting on server events.
• Availability Management: Provides tracking and reporting on server availability.
• Data Retention and Recovery: Technical Services will attempt to recover any missing or lost files to the best of our abilities. There may be cases where files are unrecoverable due to extenuating circumstances. Files less than fifteen (15) days old can generally be restored in 24 hours. Files lost or missing for more than fifteen (15) days will require additional resources for restoration. In these cases, restoring a file could take anywhere from fifteen (15) days to a month and additional charges may be incurred by the customer. Database information can only be restored up to six (6) days without requesting a tape. If restore goes back further than a week restoration could take anywhere from fifteen (15) days to a month and additional charges may be incurred by the customer.
• Incident Management: Incidents are tracked and reported on to ensure categorization is correct and the SLA terms are met.
• Problem Management: Proactive and reactive monitoring of technical problems minimizes long term service outages.
• Knowledge Management: Knowledgebase articles are created to provide customers with information on common topics.
• Change Management: Technical Services has processes in place that control and manage request for changes to our IT infrastructure or any aspect of our IT services to minimize the risk of disruption.
• Service Level Management: Incidents are tracked and reviewed for SLA and OLA compliance.
• Information Security Management: Develops, maintains, and enforces information security policies and awareness. Ensures the confidentiality, integrity, and availability of information assets.
• Supplier Management: Ensures that the SLAs, contracts, and agreements are in place with third party suppliers.
• Financial Management of IT Services
• Best-Effort Support: If feasible, Technical Services will provide best-effort support to any product, hardware or software that we do not maintain or that is no longer supported by its vendor. *All IT Guidelines must be followed and all hardware and software must be approved by Technical Services before installation.*

## DISASTER RECOVERY

### DISASTER EVENTS AND DISASTER RECOVERY

In the event of a disaster or serious server outage during standard support hours, Technical Services will notify the predetermined Emergency Contact in each department by telephone and inform them of the situation.

*NOTE: All Service Level Response and Resolution Times listed above will be considered unavailable with the exception of a “Critical” Severity Type. A Critical incident will be attended to as quickly as possible based on an assessment of the disaster situation, but no Response or Resolution times are promised.*

## BUSINESS CONTINUITY AND DISASTER RECOVERY

• All University data should be stored on servers. All servers are backed up to disk daily, and copied to tape weekly. Disk backups are kept for two weeks. Full tape backups are completed every Friday and incremental backups are completed Saturday through Thursday. All monthly tape backups are kept indefinitely at our offsite storage facility.

• All backup media is moved to a secure off-site storage facility and is available as needed 24x7.

• The network H: drive is setup to keep shadow copies of previous file versions. If a file version is not available via Shadow Copy, a file restore can be completed by Network Services. If the file was deleted within the last two weeks, the restore can be executed and completed by Network Services in approximately four hours (depending on the size of the file). If the file has been deleted for more than two weeks, then it is necessary to have a tape returned from our offsite storage facility the following Tuesday.

• Databases located on the SQL servers are backed up every four hours. A full database backup to disk is performed twice a day, once during the day and once at night.

• All applicable servers are protected by a Disaster Recovery agreement, with 24-hour hardware replacement and relocation in the event of disaster.

• A web-based Emergency Messaging System is used as a backup e-mail service.

• Disaster Recovery plans are validated by annual exercises and audits.

## MEDIA STORAGE

Secure off-site storage for all network backup media is provided by Iron Mountain. Since 1951, Iron Mountain has been the partner that thousands of companies trust to store, manage, and protect records, media, and electronic data in any format for any length of time. Our backup media is stored in the Iron Mountain’s National
Underground Storage (NUS) facility. Iron Mountain provides us with protection of our backup media while allowing us access to it 24x7.

**CUSTOMER ACCOUNTS**

The following section outlines requirements for accounts that provide access to any of Technical Services’ computers or systems.

**ACCOUNT LIMITS**

- All customer accounts are created with:
  - 150MB warning/200MB limit on K drive space
  - 250MB warning/300MB limit on H drive space
  - 600MB warning/650MB stop sending/700MB stop receiving e-mail on Exchange server

- During Exchange (e-mail) server maintenance, the following items will be deleted:
  - Calendar items over 3 years old
  - Sent Items over 180 days old
  - Deleted Items over 30 days old
  - Junk E-mail over 14 days old

- More space will be granted upon request if reasonable business need is illustrated. Before new space is granted, customers must make an attempt to remove extraneous files that may be consuming space. This includes the removal of files that are significantly old, multimedia files and e-mail attachments. Technical Services will provide CD creation services for these files upon request.

**ACCOUNT MODIFICATIONS**

Account modifications and requests for additional account access are performed at the discretion of the requesting customer’s department administrator and Technical Services. Account modifications are subject to the following stipulations:

1. Submission of a non-urgent request
2. Submission of completed Request for Data Access Form
3. Signature of account requestor, department administrator and customer as per specific instructions outlined by Support Services at the time of the request

**ACCOUNT MAINTENANCE AND DELETION**
• It is the responsibility of the department administrator to inform Technical Services of employees leaving the department or University a minimum of one (1) day prior to employee’s last day.

• Any data and/or information can be gathered from the departing employee’s hard disk, network share, or e-mail and delivered to the department administrator as requested up to one (1) week after employee’s last day.

• All computers will be rebuilt by Technical Services before being redistributed to other employees.

• Unless otherwise backed up and informed of extended leave or absence of employee:
  o Technical Services will disable any accounts left unused for 30 days.
  o Technical Services will delete any accounts that have been disabled for more than 90 days.

REPORTING AND SURVEYING

REPORTING

Technical Services will provide monthly reports via our website containing information on actual performance achieved compared to service level objectives. These results can be viewed at www.fis.pitt.edu/customers/performance.htm

Additional reports for management will be made available upon request.

SURVEYING

It is our goal to provide the highest support and customer service possible. To accomplish that we survey customers based on incident submissions and new computer installations. We strive to achieve at least a 50% sample size of closed incidents and 100% of PC installations. FIS utilizes the Help Desk Institute’s Customer Satisfaction Index (CSI) service to survey customers and measure satisfaction. These surveys are extremely important to our operations. It is the responsibility of the recipients of these surveys to answer in the most truthful and thorough way possible.
APPENDIX A

PROFESSIONAL CERTIFICATIONS

Technical Services is committed to providing the highest quality of service possible. To do so, our staff is required to hold various professional certifications. We pledge to maintain these certifications and update them as industry standards change. Technical Services staff currently hold the following certifications:

ASP DEVELOPER CERTIFICATION

The ASP Certification from W3Schools proves fundamental knowledge of web development using ASP, SQL and ADO. This proves the ability to develop and maintain dynamic and interactive web pages and also retrieve and update data from a database over the internet.

BUSINESS CONTINUITY PROFESSIONAL CERTIFICATION

DRI International was founded in 1988 as the Disaster Recovery Institute in order to develop a base of knowledge in contingency planning and the management of risk, a rapidly growing profession. Today DRI International administers the industry's premier educational and certification programs for those engaged in the practice of business continuity planning and management. DRII provides industry certification that is well respected and recognized world-wide. Certification as a Business Continuity Professional is intended for individuals who have demonstrated knowledge and work-related skill in the business continuity/disaster recovery industry on an enterprise-wide level.

CERTIFIED IDENTITY THEFT RISK MANAGEMENT SPECIALIST

The Institute of Fraud Risk Management offers the Certified Identity Theft Risk Management Specialist™ (CITRMS) training and certification course. The CITRMS is the nation’s only professional certification program specifically developed to train and equip professionals to understand and address Identity Theft and related fraud. The comprehensive CITRMS course addresses risks and issues for consumers, employees, and businesses / professional practices.

CERTIFIED IN HOMELAND SECURITY (CHS)

Since its inception in March 2003, the Certified in Homeland Security (CHS) program has earned a reputation as the professional membership association dedicated to the certification, training, and continuing education of professionals in Homeland Security from across the nation. The CHS program has at the core of its membership some of the world’s leading professionals who have significant experience with and links to Homeland Security.

CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT (CGEIT)

The CGEIT addresses the business need for a certification that recognizes expertise in IT governance, and helps enterprises identify professionals who have exceptional IT governance knowledge and experience. The credential focuses on the five areas of IT governance: strategic alignment, value delivery, risk management, resource management,
and performance management. It also focuses on frameworks that provide support for IT governance such as CobiT and ITIL.

**CERTIFIED INFORMATION SECURITY MANAGER (CISM)**

The CISM certification promotes international practices and provides executive management with assurance that those earning the designation have the required experience and knowledge to provide effective security management and consulting services. Individuals earning the CISM certification become part of an elite peer network, attaining a one-of-a-kind credential.

**CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)**

The mark of excellence for a professional certification program is the value and recognition it bestows on the individual who achieves it. Since 1978, the Certified Information Systems Auditor (CISA) program, sponsored by the ISACA®, has been the globally accepted standard of achievement among information systems (IS) audit, control and security professionals.

**CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)**

Global Recognition for Top Information Security Professionals

As the first credential accredited by ANSI to ISO Standard 17024:2003 in the field of information security, the Certified Information Systems Security Professional (CISSP®) certification provides information security professionals with not only an objective measure of competence but a globally recognized standard of achievement. The CISSP credential demonstrates competence in the 10 domains of the (ISC)² CISSP® CBK®.

**CERTIFIED PROTECTION PROFESSIONAL (CPP)**

The American Society for Industrial Security (ASIS) offers the Certified Protection Professional (CPP) credential to senior security professionals. The CPP indicates board certification in security management and is recognized worldwide as the highest recognition accorded a security practitioner. The CPP is a coveted credential and often serves to identify qualified senior staff who can manage security matters at executive levels, such as in the role of Chief Security Officer or Chief Confidentiality Officer. Successful CPPs have demonstrated competency in the areas of security solutions and best-business practices through an intensive qualification and testing program encompassing all areas of security management: Physical Security, Security Principles and Practices, Investigations, Business Principles and Practices, Personnel Security, Emergency Practices, Information Security, and Legal Aspects. CPPs must also possess a minimum of nine years of relevant work experience.

**COMPTIA AUTHORIZED SERVICE CENTER GOLD**

The CompTIA Gold Authorized Service Center program showcases service centers that offer higher levels of repair and customer service capabilities. CompTIA A+ Certification. To qualify for this program, a company must prove that at least 75% of their PC service technicians are CompTIA A+ certified, demonstrate that at least 50% hold other CompTIA technical certifications and have 75% of technicians enroll in and pass the CompTIA Customer Service Skills Accreditation. The CompTIA Authorized Service
Center designation is proof of our department’s capabilities and provides visibility to our customers.

**COMPTIA A+ CERTIFICATION**

CompTIA A+ certification is an international industry credential that validates the knowledge of computer service technicians with the equivalent of 500 hours of hands-on experience. It is the standard for foundation-level, vendor-neutral certification for service technicians. Only A+ Certified Professionals are permitted to work on customer PCs and peripherals.

**COMPTIA I-NET+ CERTIFICATION**

CompTIA i-Net+ certification is an international industry credential that validates the knowledge of technical and non-technical professionals alike with experience in Internet, Intranet, Extranet, and e-commerce technologies.

**COMPTIA NETWORK+ CERTIFICATION**

CompTIA Network+ certification is an international industry credential that validates the knowledge of networking professionals with experience in network support and administration. This standard demonstrates that technician posses the knowledge and skills needed to install, configure, and troubleshoot network hardware, protocols, and services.

**COMPTIA PROJECT+ CERTIFICATION**

CompTIA Project+ certification is a global credential that validates the knowledge required to effectively manage information technology-related projects throughout the entire project life cycle.

**COMPTIA SECURITY+ CERTIFICATION**

The CompTIA Security+ certification tests for security knowledge mastery of an individual with two years on-the-job networking experience, with emphasis on security. The exam covers industry-wide topics, including communication security, infrastructure security, cryptography, access control, authentication, external attack and operational and organization security.

**COMPTIA SERVER+ CERTIFICATION**

CompTIA Server+ certification is an international industry credential that validates the knowledge of individuals with experience in Industry Standard Server Architecture (ISSA) technology.
DELL WARRANTY PARTS DIRECT CERTIFIED

Allows FIS staff members to independently service Dell systems and provide our own maintenance without the need of a Dell technician. By having this certification, we are able to improve configuration and installation accuracy of Dell desktops, servers, and laptops, improve our repair time efficiency, and minimize impact to business activities and transactions.

GLOBAL INFORMATION ASSURANCE CERTIFICATION

The SANS Institute founded GIAC (Global Information Assurance Certification) in 1999 in response to the need to validate the skills of security professionals. The purpose of GIAC is to provide assurance that a certified individual holds the appropriate level of knowledge and skill necessary for a practitioner in key areas of information security. SANS training and GIAC certifications address a range of skill sets including entry level Information Security Officer and broad based Security Essentials, as well as advanced subject areas like Audit, Intrusion Detection, Incident Handling, Firewalls and Perimeter Protection, Forensics, Hacker Techniques, Windows and Unix Operating System Security. GIAC is unique in measuring specific skill knowledge areas instead of general purpose security knowledge.

HDI HELP DESK ANALYST OF THE YEAR (HDAOY)

This award recognizes a local help desk analyst that exemplifies the best qualities among support practitioners. The winner will have demonstrated extraordinary commitment, dedication, and service to customers while consistently exceeding performance objectives. Technical Services Support Analysts have been awarded this honor twice in the last four years.

HDI SUPPORT CENTER ANALYST (SCA)

Ensures that support professionals know the core strategies for effective customer care and problem resolution. In addition, SCA’s know the fundamentals for help desk, support center, and customer support processes and tools, and ITIL processes.

HDI SUPPORT CENTER TEAM LEAD (SCTL)

The support center team lead serves as the champion for the customer and the focal point for support center analysts. A team lead must be customer focused, be able to drive change and process improvements, provide training, and deliver customer support.

HELP DESK ANALYST CERTIFICATION (HDA)

Ensures that support individuals have the tools, techniques, and skills to achieve success as front-line analysts. HDAs are empowered to transform the support operation from a cost center to a productivity center that enhances the organizations’ overall effectiveness.
<table>
<thead>
<tr>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HELP DESK MANAGER CERTIFICATION (HDM)</strong></td>
<td>Ensures that managers have mastered the art of building and retaining great teams that can successfully deliver effective, helpful, and respectful service to the organization.</td>
</tr>
<tr>
<td><strong>ITIL V3 FOUNDATIONS</strong></td>
<td>The IT Infrastructure Library (ITIL) v3 is the current version of the most widely adopted best practice framework for IT management. Achieving the Foundation certification represents clear demonstration that you can contribute to improving the maturity of an IT organization in the areas of service management as a practice, processes, and service management functions and roles.</td>
</tr>
<tr>
<td><strong>MASTER CERTIFIED INTERNET WEB DESIGNER (CIW)</strong></td>
<td>Master CIW Designers develop and maintain websites using authoring and scripting languages, create content and digital media, and employ standards and technologies for both business-to-business and business-to-consumer e-commerce websites.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED APPLICATION DEVELOPER (MCAD)</strong></td>
<td>An individual who holds this credential proves that they have the skills to build powerful applications using Microsoft Visual Studio .NET and Web services on the Microsoft .NET Framework.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED DESKTOP SUPPORT TECHNICIAN (MCDST)</strong></td>
<td>An individual who holds an MCDST Certification proves that they have the skills to successfully support end users and to successfully troubleshoot desktop environments running on the Microsoft Windows operating system.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED IT PROFESSIONAL: ENTERPRISE SUPPORT TECHNICIAN</strong></td>
<td>The Microsoft Certified IT Professional (MCITP) credential validates that an individual has the comprehensive set of skills necessary to perform a particular job role. The Enterprise Support Technician designation proves that candidates have experience deploying Windows Vista, managing security, and troubleshooting network-related issues with Windows Vista.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED IT PROFESSIONAL: DATABASE ADMINISTRATOR</strong></td>
<td>The Microsoft Certified IT Professional (MCITP) credential validates that an individual has the comprehensive set of skills necessary to perform a particular job role. The Database Administrator designation proves that the candidate has experience optimizing and maintaining database solutions and is familiar with the phases of the product life cycle.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED PROFESSIONAL (MCP)</strong></td>
<td>An individual who holds an MCP Certification has verified their expertise at implementing a Microsoft product or technology as part of a business solution in an organization.</td>
</tr>
<tr>
<td>Certification</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED SYSTEMS ADMINISTRATOR (MCSA)</strong></td>
<td>An individual who holds this credential proves that they have the skills to successfully manage and troubleshoot Windows based operating environments.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED SYSTEMS ADMINISTRATOR: SECURITY (MCSA: SECURITY)</strong></td>
<td>An individual who holds this credential proves that they have the skills to manage Windows based operating environments while specializing in managing, maintaining, and implementing security on a Microsoft platform as part of a secure computing environment.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED SYSTEMS ENGINEER (MCSE)</strong></td>
<td>An individual who holds this credential proves that they have the expertise in designing and implementing the infrastructure for business solutions based on the Microsoft Windows platform and Windows Server System.</td>
</tr>
<tr>
<td><strong>MICROSOFT CERTIFIED TECHNOLOGY SPECIALIST</strong></td>
<td>The Microsoft Certified Technology Specialist (MCTS) certifications provide the foundation for Microsoft Certification. These certifications are designed to validate skills on the features and functionality of key technologies.</td>
</tr>
<tr>
<td><strong>ORACLE CERTIFIED ASSOCIATE</strong></td>
<td>An individual that holds this credential is recognized for their achievement in mastering the fundamental skills necessary to administer and manage Oracle database software.</td>
</tr>
</tbody>
</table>
APPENDIX B

VENDOR SUPPORT AND UNDERPINNING CONTRACTS

MICROSOFT PREMIER SUPPORT

Premier Support provides Technical Services with dedicated technical professionals from Microsoft to supervise our support needs, problem resolution support that covers our systems 24x7, and training and workshops to help us keep up-to-date on the latest technologies.

- A dedicated Microsoft Technical Account Manager acts as our internal advocate at Microsoft to help ensure that the appropriate resources are engaged to resolve our support issues.
- Microsoft Support Professionals deliver expert assistance by phone and onsite for technical problems that occur when we use a Microsoft product.
- Preventative, prescriptive guidance on a variety of issues – from answers to basic "how-to" questions to the discussion of best practices around deployments, migrations, and operations in our IT environment.
- Knowledge transfer services help our IT staff develop the skills and resources to mitigate potential IT issues.
- Only FIS Technical Services and CSSD possess this level of support at the University.

MICROSOFT DEVELOPER NETWORK (MSDN) SUPPORT

MSDN Support provides Technical Services with dedicated technical professionals from Microsoft to supervise our development needs, problem resolution support that covers our systems 24x7, and training and workshops to help us keep up-to-date on the latest technologies.

- A dedicated Microsoft Technical Account Manager acts as our internal advocate at Microsoft to help ensure that the appropriate resources are engaged to resolve our requests.
- Ability to obtain the latest Microsoft technologies.
- Access to Microsoft Professional Support for Developers for guidance on application related requests or support issues.
- Knowledge transfer services to inform our IT staff of latest technologies and developments.

DELL LIMITED WARRANTY

Dell provides a four year desktop and laptop warranty on parts and labor. This limited warranty covers defects in materials and workmanship for the Dell-branded hardware products, including Dell-branded peripheral products, except for the following Dell-branded hardware:

- Laptop batteries carry a 1-year limited warranty.
- Projector lamps carry a 90-day limited warranty.
- Memory carries a lifetime limited warranty.
- Monitors carry the longer of either a 3-year limited warranty or the remainder of the warranty for the Dell computer to which the monitor will be connected.
- PDAs, MP3 players, earphones, remote inline controls, and AC adapters carry a 1-year limited warranty.
• Other add-on hardware carries the longer of either a 1-year limited warranty for new parts and a 90-day limited warranty for reconditioned parts or, for both new and reconditioned parts, the remainder of the warranty for the Dell computer on which such parts are installed.

This limited warranty does not cover:

• Software, including the operating system and software added to the Dell-branded hardware products through our factory-integration system, third-party software, or the reloading of software
• Non-Dell branded and Solution Provider Direct products and accessories
• Problems that result from: External causes such as accident, abuse, misuse, or problems with electrical power
• Servicing not authorized by Dell
• Usage that is not in accordance with product instructions
• Failure to follow the product instructions or failure to perform preventive maintenance
• Problems caused by using accessories, parts, or components not supplied by Dell
• Products with missing or altered Service Tags or serial numbers
• Products for which Dell has not received payment

DELL LAPTOP COMPLETE CARE ACCIDENTAL DAMAGE SERVICE

Provides Technical Services with a four year warranty for all Dell laptops on accidental damage. CompleteCare Accidental Damage Service is a repair and replacement service that covers most accidental damage (spills, drops, surges, and breakages) to select systems or peripherals that is not covered under limited warranty.

Coverage:

Some examples of non-intentional damage that are covered are:

• Cause of Failure Resolution Description
• Liquid spilled on or in unit Repaired or unit replaced
• Drops, falls, and other collisions Repaired or unit replaced
• Electrical surge Repaired or unit replaced
• Damaged or broken LCD due to a drop or fall Repaired
• Accidental breakage (multiple pieces) Repaired or unit replaced

Not-Covered:

Damage caused by intentional acts, fire, theft or loss, is not covered under CompleteCare Accidental Damage Service. Some examples of damage that would NOT be covered are:

• Cause of Failure Resolution Description
• Damaged in a fire Not covered - insurance coverage
• Intentional damage (hammer marks) Not covered - user responsible
• Stolen unit Not covered - insurance coverage
• Normal wear (does not affect system performance) Not covered
• Consumables (batteries, bulbs) Not covered
DESKTOP COMPUTER STANDARDS

All desktop computers have the following standard hardware and software:

- **Standard Hardware**
  - Dell OptiPlex PC with:
    - 19 inch or 22 inch Monitor set at least 1024 x 768 resolution, with minimum of 32-bit color
    - Quietkey Keyboard & Mouse
    - Pentium or Core 2 Duo Processor: Minimum of 2GHz
    - SVGA Graphics with at least 32 MB of RAM
    - 1024 - 4096 MB of RAM
    - 30 GB - 320 GB Hard Disk Drive
    - 100– 1024 MB Ethernet Network Interface Card
    - DVD-ROM 8x to 48x drive
    - Parallel, serial, USB Ports
    - Sound card and stereo speakers

- **Standard Software**
  - Windows XP SP3 or Windows Vista SP2
  - Microsoft Office 2007 Enterprise Edition
    (Access, Excel, InfoPath, OneNote, Outlook, PowerPoint, Publisher, Word)
  - Adobe Acrobat Reader
  - Adobe Flash Player
  - CenterTools DriveLock agent
  - CoreFTP
  - Diskkeeper Professional Edition
  - Identity Finder
  - Internet Explorer 7
  - Java Standard Edition
  - KeePass
  - Microsoft App-V client
  - Microsoft Baseline Security Analyzer
  - Microsoft Configuration Manager client
  - Microsoft Office Live Meeting
  - Microsoft Operations Manager agent
  - Microsoft Silverlight
  - PDF Creator
  - PRISM 11i
  - QuickTime
  - RightFax Client
  - SecureZip
  - Symantec EndPoint Protection Anti-virus
  - WebEx Playback Client
  - Windows Media Player