

Office of Information Technology

WHAT'S INSIDE

For deans, directors, and other unit heads:

Planning, budgeting, staffing, security, privacy, accessing university data, disaster recovery and business continuity planning, and policies and guidelines

For Local Area Network (LAN) operations staff:

Networking, servers, voice services, video services, and security

For end-user support staff:

Desktop and laptop computers, security, and training

For faculty and staff:

Security, intellectual property and academic integrity, and instructional and research technology

A sample unit IT plan

A list of OIT support resources

A matrix of OIT and unit IT responsibilities

GUIDE TO INFORMATION TECHNOLOGY FOR ACADEMIC AND ADMINISTRATIVE UNITS 2005–2007



Computing Help Desks

Camden

Camden Campus Center, lower level

856/225-6274

help@camden.rutgers.edu

<http://computing.camden.rutgers.edu>

FAQs: <http://faq.camden.rutgers.edu>

Newark

Engelhard Hall, Room 308c

973/353-5083

help@newark.rutgers.edu

<http://ncs.newark.rutgers.edu>

FAQs: <http://faq.newark.rutgers.edu>

New Brunswick/Piscataway

Busch Campus, Hill Center, Room 013

732/445-HELP (4357)

help@nbcs.rutgers.edu

<http://www.nbcs.rutgers.edu/helpdesk>

FAQs: <http://faq.rutgers.edu>

Detailed technical information is available at

<http://techdir.rutgers.edu/>

Table of Contents

Introduction	· 1
For deans, directors, other unit heads	· 3
<i>Planning</i>	· 3
<i>Budget</i>	· 4
<i>Staff</i>	· 5
<i>Security</i>	· 7
<i>Privacy</i>	· 7
<i>Accessing university data</i>	· 8
<i>Disaster Recovery and Business Continuity Planning</i>	· 8
<i>Policies and guidelines</i>	· 9
For IT operations staff	· 11
<i>Networking</i>	· 11
<i>Servers</i>	· 12
<i>Voice services</i>	· 12
<i>Video services</i>	· 13
<i>Security</i>	· 14
For end-user support staff	· 17
<i>Desktop and Laptop Computers</i>	· 17
<i>Security</i>	· 18
<i>Training</i>	· 18
For faculty and staff	· 21
<i>Security</i>	· 21
<i>Intellectual Property and Academic Integrity</i>	· 22
<i>Instructional and Research Technology</i>	· 22
Appendix 1: Sample Unit IT Plan	· 25
<i>Table of Contents</i>	· 26
<i>Introduction by the IT Committee</i>	· 26
<i>Reviewing the scope of activities that rely on IT</i>	· 27
<i>Assessing successes, gaps, and needs</i>	· 28
<i>Aligning resources with areas critical to what we do</i>	· 30
<i>Attachment 1: Equipment Inventory – Record 1</i>	· 32
<i>Attachment 2: Sample project plan: Online course registration exemptions</i>	· 33
<i>Attachment 3: Project plan to address immediate security issues</i>	· 37
Appendix 2: OIT Support Resources	· 39
Appendix 3: OIT Services at Rutgers	· 41
Glossary	· 49

Introduction

Information Technology (IT) is an integral part of many university activities. Faculty and staff utilize a wide variety of systems, technologies, and services during any given day. IT, as an enabling facility, will continue to grow in importance at the university. Features and capabilities that are luxuries today will be viewed as basic necessities tomorrow. Establishing and maintaining an IT infrastructure that addresses the needs of research, teaching, learning, outreach, and administration involves ongoing efforts.

The purpose of this document is to guide units* in planning for the use of IT. This includes use of facilities and services provided by the Office of Information Technology (OIT) and others, as well as services provided by the units themselves.

The guide will also help units:

- Manage their IT resources to optimize the payback on investment;
- Protect the information assets entrusted to their care;
- Ensure all staff members understand and fulfill their obligations for IT support and use.

To take full advantage of the opportunities provided by technology, units should establish and maintain IT infrastructures in a planned and coordinated fashion. An IT strategy requires recognition and support from **deans, directors and other unit heads**. It requires the adoption of industry best practices at the **operational level**. It requires familiarity with technology and end-user support at the **support level**. It requires understanding at the **faculty and staff level**.

This document is organized around these four groups. It is intended for all involved in the delivery and consumption of IT services. It is recognized that staff are often pressed into an IT role for a variety of reasons. Because of this, and to facilitate greater understanding among the respective roles, each section is specifically written to be read both by an individual serving in that role as well as by others. Sections are deliberately broad and basic, for consumption by a wide audience.

Three appendix sections are included:

1. a sample IT plan
2. a list of OIT-provided support resources
3. a description of IT services at the university, including information about OIT services and services that are the responsibility of units.

The document also includes a glossary of IT terms.

* The term, "units," will be used throughout this document to refer to campuses, colleges, schools, departments, centers, bureaus, institutes, and other academic and business units throughout the university.

Who should read this guide

Deans, department chairs, other unit heads

- Planning
- Budgeting
- Staffing
- Security
- Privacy
- Accessing university data
- Disaster recovery and business continuity planning
- Policies and guidelines

IT Operations staff

- Networking
- Servers
- Voice services
- Video services
- Security

For end-user support staff

- Desktop and laptop computers
- Security
- Training

For faculty and staff

- Security
- Intellectual Property and Academic Integrity
- Instructional and Research Technoloav

For deans, directors, and other unit heads

Deans, directors, and other unit heads have high level responsibility for the creation, management, and evolution of IT facilities and services. In addition, they have responsibility for leading overall IT security in the unit including approving plans, reviewing procedures, enforcing compliance with the unit's and university's procedures/policies, supporting IT staff who set security requirements, and obtaining assurance (preferably in writing) that appropriate security measures are in place. Often, unit-based IT committees assist by exercising budget authority, creating IT strategic plans, overseeing IT security, and coordinating IT project planning to ensure that the evolution of IT services are aligned with the unit's academic and business needs.

PLANNING

Formulating an IT plan (see Sample Plan in Appendix 1, p. 25) involves:

Establishing an IT committee. Conduct focused IT planning through a unit-based IT committee involving faculty and IT staff for academic departments; and administrators and IT staff for administrative units. Develop strategic plans that identify, examine, and support deployment of new technology. Employ the committee to keep the unit current in IT areas relevant to the unit's discipline or function. In academic units, a faculty member of this committee should take a lead role and participate in the it_faculty_liaisons@email.rutgers.edu mailing list. In administrative units, a key administrator should take a lead role and participate in the it_admin_liaisons@email.rutgers.edu mailing list.

Reviewing the scope of unit-based activities. Develop a list of major academic and administrative goals. These goals should outline the most important ways in which the unit intends to use IT to support its goals and the goals of the university. They should focus on what is to be accomplished, not specific technologies. They should provide a vision for the way in which the unit wants to operate. Examine where IT can have the biggest impact. Look at all categories of operations, including instruction, research, administration, and outreach.

Assessing successes, gaps and needs. Identify areas where the application of IT within a unit is successful, unsuccessful, or insufficient. Identify goals that will help capitalize on successful areas to help support those in need.

Aligning resources with areas identified as critical to unit business. Identify areas of IT that do not contribute to major goals and that are consuming resources. Redirect those resources to areas of need. Consider existing operations. Are there things being done that are no longer needed or that are now available from other sources? Are there ways to automate tasks? Talk to OIT and other units that may have services or ideas that can be used.

For deans, directors, and other unit heads

- Planning
- Budgeting
- Staffing
- Security
- Privacy
- Accessing university data
- Disaster recovery and business continuity planning
- Policies and guidelines
- For IT operations staff
- For end-user support staff
- For faculty and staff

BUDGETING

TCO calculations include:

- Original cost of the hardware and software
- Hardware and software upgrades
- Additional equipment and software for projects
- Maintenance – hardware and software
- Technical support
- Training – end user and technical staff development
- Networking – equipment and infrastructure (wiring)
- Security

Implementation of information technology requires funding. Many units do not allocate specific budgets for IT activities. Best practices in this area recommend developing a Total Cost of Ownership (TCO) budgeting model, which includes all direct and indirect technology costs and works in an equipment replacement plan (see page 31 for an example). Budgeting must also include funds for temporary IT staffing.

Designing and implementing an IT budget involves:

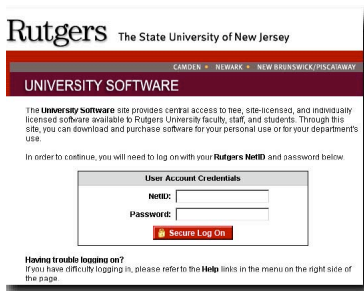
Identifying resources. Many potential sources of funding should be considered when developing an IT budget. Consider using operational budgets to fund unit-based IT staff and infrastructure. When developing grant proposals, consider the project's IT needs in terms of equipment, software, data, and technical support. Some units establish recurring IT accounts and assess standard computer support charges from grants (e.g., 2% of direct costs.) Monies collected are used to assist in providing infrastructure IT support. Talk with colleagues and OIT to see what funding models may be available.

Prioritizing needs/objectives. There is rarely enough funding to support all of the activities an organization can perform. Identify and prioritize activities based on their degree of relevance to a unit's mission. As part of this process, a cost/benefit analysis should be performed.

Taking advantage of university-based cost saving opportunities. Before doing major hardware or software purchases, it is worth talking with OIT or the Purchasing Department to see whether there are existing contracts or purchase arrangements that can be used. For example, at least once a year, the Rutgers Computer Store makes a bulk purchase of PCs for use in the campus computing labs. Other units at Rutgers are invited to join in this purchase. OIT also has a number of site licenses (visit <http://software.rutgers.edu/> for more information) and can facilitate software purchases involving multiple units. Through the it_faculty_liaison@email.rutgers.edu mailing list and the it_admin_liaison@email.rutgers.edu mailing lists, faculty and administrators can be involved in OIT's software collection development process to help evolve the collection of software available through site-licensing.

Units can save on costs by utilizing central services for common functions such as email, web hosting, and other services included on page 16.

Allocating/Reallocating. IT budget management is not a one-time activity. Goals, projects and priorities should be reassessed periodically to adapt to changes in unit needs and resource availability.



STAFFING

Unit heads should have a clear understanding of the role of IT staff. Both IT staff and others need to understand priorities and how they are set. This will involve setting up mechanisms that allow the unit to balance short-term “hot button” items with projects that have longer term but more strategic goals. Staff must be permitted sufficient time to develop and maintain a solid IT infrastructure.

Hiring. Document the responsibilities of IT staff and the role of the unit head and committees as they relate to IT. In general, IT staff can do technical planning, but unit heads or their designates should be responsible for setting goals and monitoring progress. It is best to have a single faculty /staff member supervising technical staff and chairing a unit-based IT advisory committee. OIT campus computing divisions and the Office of Instructional and Research Technology (OIRT) can assist in these processes. OIT’s Human Resources Office can also assist in building applicant pools for IT recruiting.

Development. Training/professional development programs should be created for all IT staff. Development typically includes training, conferences, and time set aside for study in both technical and customer relations areas. A budget will be needed for staff development, and at least two to three weeks a year should be set aside for these activities. Managers should encourage IT staff to attend technical support meetings such as those listed in Appendix Section 2, p. 40.

Time Allocation. Allocate time for staff to do planning, including collecting usage data and statistics that are needed to guide planning.

Reviewing Staff Priorities. In addition to overall IT goals set once or twice a year, the faculty /staff member assigned to act as liaison between IT staff and the unit should review the specific tasks on which IT staff are working regularly. It is important to be sure that their priorities reflect the units’, and that the faculty /staff committee understands what IT staff are doing.

Performance Review. Develop measurable ways to assess whether goals are being met. This includes technical measures such as system reliability and performance, progress reporting on projects, documented procedures, and goals relating to user service quality. University Human Resources and OIT campus divisions can assist in establishing such measures.

Hiring assistance

Camden	856/225-6274
Newark	973/353-1731
New Brunswick	
Piscataway	732/445-6950
	732/445-3088
OIT HR office	732/445-2741 x6508

Have a clear understanding of how staff will use their time

Balance system administration with end-user support. A unit may find it useful to create formal processes for faculty and staff to make requests of staff. It’s much easier to balance priorities with such a process.

Recruitment: A Hiring Checklist

This checklist is intended to help units evaluate candidates for IT positions.

- ✓ Set clear goals for the new position that fit into the overall unit IT goals as defined in the unit's formal IT plan (see page 3 for guidelines for developing such a plan).
- ✓ Develop a job description with a clear description of tasks for at least the next year. Be clear on the level of experience and skills needed for the position.
- ✓ Identify general areas in which staff should operate. Areas include working with faculty, understanding the discipline, and budget and administration. Specific technology areas may include:

- System administration
- Security
- Network administration
- Application support
- User support
- Programming
- Hardware diagnosis/repair
- Telephone system support
- Video technologies

Staff may have strengths in one or more of these areas but may not have expertise in all areas.

- ✓ Ensure that the salary level is properly matched to the skills. The university's Human Resources Department can provide advice on this. In this process of analysis, be sure that at least one experienced IT manager is involved. It may be helpful to work with OIT campus divisions, OIRT, IT managers from nearby units, or IT managers on a campus.
- ✓ Allocate sufficient resources for the person to succeed. This includes budget, hardware, staffing, training, and help from unit leaders/managers.
- ✓ Make sure that there is a clear reporting/oversight relationship for the position.
- ✓ Before posting a position, understand how candidates are going to be evaluated. Normally, an interview committee including both technical members and members representing end- users will be formed to assess both technical and customer service skills. Often it is best to assess each type of skill separately. The interview committee should include at least one experienced IT manager at least for final candidates. As with the analysis, this manager may come from OIT or another unit.

SECURITY

Information in its many forms has become a critical university asset, impacting nearly all of the university's core missions. Because of the university's decentralized nature, in both operations and computing, the protection of information is a shared responsibility between central operations and business units. With this in mind, it is important that all unit heads take appropriate steps to create an environment that complies with appropriate laws and regulations and that protects information and enhances a secure computing environment.

Information security is not a product one buys "off the shelf." It is a continuous process of measuring, analyzing, and mitigating risk. Protecting information is as much a people and process issue as it is a technology issue and any comprehensive program is a dynamic process.

Setting policies and procedures for information protection, data security, and physical security should become a regular part of a unit's routine. University executive vice presidents require all units to have a security plan.

To assist in developing a security plan, OIT has developed several tools. Staff from OIT are available to meet with units to assist in reviewing current IT security conditions and developing security plans.

PRIVACY

Privacy is an important part of trust: Faculty, staff, and students must be able to trust that computing staff will not exceed their authority to snoop through their information just because it happens to be on systems where they have privileges. The Rutgers Acceptable Use Policy, available at <http://oit.rutgers.edu/acceptable-use.html>, establishes an expectation of privacy on Rutgers systems, and note that staff have an obligation to treat end-users' information as confidential.

It is the position of the university to protect its information assets and allow the use, access and disclosure of such information only in accordance with university interest and applicable laws and regulations. All university employees providing services or working with the university's information are responsible for protecting it from unauthorized access, modification, destruction, or disclosure

Security tools

<http://rusecure.rutgers.edu/>

- An online baseline security checklist
- A guide to developing a security plan
- Pointers to more in-depth resources for staff operating servers and more complex configurations
- Guidelines for complying with state and federal security legislation

In general, staff should only look at end-user information in the following situations:

- When that information is public.
- When staff are handling a help request from an end-user, and they need to see files to answer the request.
- When staff are dealing with end-users who have left the University or are otherwise inaccessible.
- For investigations of cheating and other university policy violations.
- For investigations of security, abuse, and operational problems

ACCESSING UNIVERSITY DATA

The university owns all data in shared databases. OIT is a primary maintainer of a repository of this data. The respective administrative functional area associated with the data, known as the data custodian or business process owner, exercises an access control role. Authorization to data that is granted by the respective data custodian is honored by OIT.

A list of data custodians can be found at:

<http://www.acs.rutgers.edu>

Units must establish that there is a “university business reason” when submitting requests for staff members’ access. In addition, units must only request the level of access necessary to accomplish this purpose. Units are responsible for ensuring their staff members’ access privileges are promptly revoked/adjusted if the “university business reason” no longer applies or has changed. Conditions leading to revocation/adjustments include staff members’ leaving the University, transferring to other university units, or changing job duties. Units need to keep the full inventory of their staff members’ various access privileges to determine what privileges need to be revoked/adjusted.

Authorization. Access to university data for business purposes requires authorization from the appropriate data custodian. Individuals or units requiring access must seek approval of the data custodian. Authorization is generally granted on a “need to know” basis.

Access. After obtaining access authorization from the data custodian and approval from the unit head, OIT will work with the administrative functional area and the requestor to coordinate both the frequency of retrieval and method of access to the requested data.

DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING

Planning for business continuity in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster affecting the administrative functions of the university or a unit requires the cooperative efforts of many organizations in partnership with the functional areas.

Units increasingly depend on computer-supported information processing and telecommunications. This dependency will continue to grow with the trend toward decentralizing information technology to individual organizations within units throughout the university. The increasing dependency on computers and telecommunications for operational support poses the risk that a lengthy loss of these capabilities could seriously affect the overall performance of the unit.

A risk analysis should be conducted to identify the critical systems holding high valued investments of the business unit and the critical data flows on which the units relies for day-to-day operations. This risk assessment process should be repeated on a regular basis to ensure that changes to processing and environment are reflected in recovery planning.

All units should have a documented disaster recovery plan that details steps to perform in case of a major or minor disaster. These plans identify important IT services and how these services will continue in the event of various disaster scenarios. Outlining system backup procedures, including location of off-site storage facilities, is also an important part of any disaster recovery plan. A sample plan can be found at <http://computing.camden.rutgers.edu/disaster/sampleplan>.

POLICIES AND GUIDELINES

The university has developed a broad array of policies, including the Acceptable Use Policy for Computing and Information Technology, to cover much of the business conducted in units. Requirements imposed by granting agencies may require units to develop and enforce more specific IT policies. Complying with statements about security, confidentiality, and access to data found in federal and state legislation, such as the Graham Leach Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), is also the responsibility of the unit. More information about compliance can be found at <http://rusecure.rutgers.edu/compliance>.

A key policy issue for unit administrators is software licensing. It is the unit's responsibility to ensure that all software in use is appropriately licensed. Illegal use of software can expose the university to significant legal liability.

Deans, directors, and other unit heads are responsible for the enforcement of policies in their area. Enforcement duties should not be left to IT staff without a proper policy framework set up by the unit.

A list of key IT and related policies can be found below. The detailed policies can be found at <http://policies.rutgers.edu>.

- Rutgers Acceptable Use Policy (AUP) for Computing and Information Technology
- Email Address Policy
- Guest Accounts Policy
- NetID Policy
- Surplus Property Policy
- Wireless LAN Policy

Guidelines for use of IT throughout the university are listed below:

- Campus Computing Lab Usage Guidelines
 - Camden: <http://computing.camden.rutgers.edu/gen95009.html>
 - Newark:
<http://ncs.newark.rutgers.edu/ciflabs/CampusCompPolicy.html>
 - New Brunswick/Piscataway:
<http://www.nbcs.rutgers.edu/ccf/main/rules/>
- Data Access Guidelines: <http://www.rutgers.edu/agreement>
- Guidelines for Use of Email for Official Purposes.
<http://oit.rutgers.edu/official-email.html>
- Network Guidelines: <http://www.td.rutgers.edu/policy/>
- Public Access to Government Records: <http://records.rutgers.edu/>
- Residential Networking (ResNet) Guidelines: <http://resnet.rutgers.edu/>
- Security Requirements: <http://oit.rutgers.edu/security-9-23-2003.html>
- Standards for Management of Computer Systems at Rutgers:
<http://oit.rutgers.edu/host-acct-req.html>

For IT operations staff

Unit-based IT operations comprises the management of facilities, systems, and infrastructure, including physical facilities, network design, servers and services, storage, applications, and security at the local level. IT operations staff are responsible for implementing / maintaining infrastructure security in the unit including participating in risk self-assessment, developing strategies, performing security administration, and responding to possible intrusions. As directed by the unit-based IT committee, operations are commonly managed by project (see sample project plan on page 33) and are therefore aligned with the strategic goals of the unit.

NETWORKING

OIT, and not the unit, is responsible for all aspects of networking between buildings and the campuses, as well as for most equipment that connects a building to the network.

Units, working with OIT, should make the following decisions about networking:

- Organization and scope of the local area network (LAN)
- Number of different areas to be defined (segments/subnets)
- Use of networks, e.g. client network, server network, private network
- Use of OIT network services, such as domain name system (DNS) and time synchronization (NTP)

Equipment Rooms. OIT creates, implements, and coordinates maintenance programs for new and modified equipment rooms. OIT is responsible for allocating all space within equipment rooms. Placement of unit-based equipment within this space must comply with all applicable standards and policies.

OIT can also assist building /unit representatives with the design, upgrade or modifications of these rooms. This includes space enlargement, power needs, cooling requirements, rack design, physical security, and applicable code/permit requirements. Units with equipment room needs should send email to noc@rutgers.edu or phone 732/445-0327.

Network Equipment – Wiring and Installation. To ensure integrity of the Rutgers network, OIT must be involved in all data, video, and voice projects. OIT maintains building network maps showing cable locations, as well as a fiber and cable management database. Units with networking needs should contact OIT at the email address and phone number listed in the previous paragraph.

In new construction projects, OIT is an integral part of the building design team. A telecommunications budget, funding data, video, and voice electronics and all wiring needs, is generally included in the building budget. These budgets

For deans, directors, and other unit heads
For IT operations staff
Networking
Servers
Voice services
Video services
Security
For end-user support staff
For faculty and staff

usually do not include associated recurring costs for electronics support and maintenance, which must be taken into account during a unit's budget planning.

Local Area Networks (LANs). Local area networks are the responsibility of individual units. OIT provides no-cost support and maintenance for switches installed as part of the RUNet 2000 project. OIT will provide no-cost support for switches under service contract and installed through projects managed by OIT. To obtain the status of a switch in your unit, or arrange IP allocations for a new LAN, contact OIT at the email address and phone number listed above.

Hostname and address allocation and related services. Each computer and device attached to the Rutgers network requires an IP address. Normally, each system is also assigned a name. The addresses and names are registered in the Domain Name System (DNS), which is managed at Rutgers through a service known as "hostmaster." OIT can also delegate ranges of hostnames (subdomains) to a unit for its own management. To arrange IP allocations, contact OIT at the email address and phone number listed above.

Wireless Networking. Units are encouraged to utilize existing wireless campus infrastructures. More information is available through local campus help desks.

Wireless infrastructure is generally the responsibility of building occupants. Units are responsible for consulting with others in the same or nearby buildings to ensure that wireless implementations in nearby areas do not interfere with each other. Units should contact OIT as noted on page 41 prior to installing a wireless network to ensure that university wireless networking policies are followed.

SERVERS

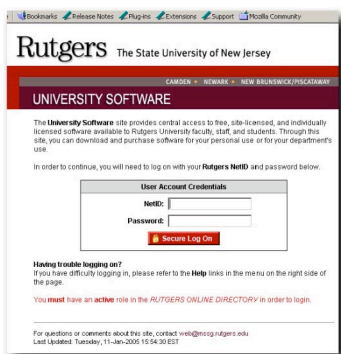
Shared Services. OIT and many larger units provide shared services that can reduce the unit burden of providing duplicate services. These services can be tailored to be unit-specific.

File storage, email, and web hosting are examples of shared services that may be provided at the unit level. Services should be implemented using standard technologies in common use at the university to permits staff to get help from OIT and other IT staff and to give users an experience that is similar to colleagues in other units. For units that manage their own services, OIT can provide support. This includes open source software repositories, site licensed software, help for unit staff in dealing with system problems, fee-based system administration and hosting services, and general planning assistance and consulting. More information is available through local campus computing services.

VOICE SERVICES

The OIT Telephone Office coordinates all aspects of voice services for the university. This includes planning and oversight of administrative, academic,

OIT campus divisions provide support, including advice in planning and troubleshooting, for unit staff operating LANs. LAN implementation and support is available on a contract basis through these divisions. See Appendix Section 2 for contact information.



and student voice needs. Requests to have telephone lines and/or sets installed, disconnected, moved or repaired; questions and/or service requests for additional line features such as call waiting, caller ID and voice mail; and billing questions are addressed on the respective campuses.

VIDEO SERVICES

General information and links to video services throughout the university can be found at <http://oit.rutgers.edu/videoservices>.

Streaming servers. OIT in Newark and Camden, the Division of Continuous Education and Outreach, and the NJEDge.Net organization run streaming video servers, which can be used to make video available over the IP network. The Rutgers community can view these video clips asynchronously or live. See Appendix 3 for contact information.

Videoconferencing. Units throughout Rutgers use videoconferencing for remote delivery of instruction, conducting meetings, making connections with K–12 entities, hosting collaborative events, and for one-to-one contact with individuals at remote locations. Technical standards and recommendations can be found at <http://oit.rutgers.edu/videoconferencing>. The Division of Continuous Education and Outreach maintains many services that support video. See <http://videoconference.rutgers.edu/videoconferencing.jsp> for more information. The Teleconference Lecture Hall in Alexander Library is also available. See <http://www.scc.rutgers.edu/scchome/facilities/facilities.htm> for more information. NJEDge.Net also offers videoconferencing services. See <http://njedge.net> for more information.

Video classrooms. The Division of Continuous Education and Outreach provides interactive video classrooms and seminar rooms, which are available for distance education as well as videoconferencing and other departmental needs. See <http://videoconference.rutgers.edu/> for more information.

Televising research seminars Research seminars are presented on RU–tv’s Research Channel. To add content, contact 732/445-3710, ext. 6210.

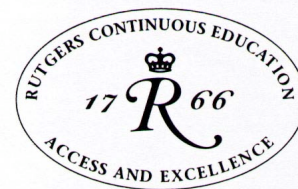
University Relations sponsored features. Rutgers’ Department of University Relations produces featured promotions and offers a suite of distribution alternatives including RU–tv channels, streaming, DVD, and VCR tape. Promotions can emanate from a number of sites on campus. For more information, contact RU–tv at 732/445-3710, ext. 6210.

Satellite teleconferences. Satellite delivered video teleconferences may be received and retransmitted on RU–tv Channel 14 to connected locations throughout the New Brunswick/Piscataway campus. For more information, or to schedule a conference, contact RU–tv at 732/445-3710, ext. 6210.

Multimedia production. The Digital Media Lab, part of New Brunswick Computing Services, provides facilities for video, audio, and graphic editing are

Voice services

Camden	856/225-1766
Newark	973/353-5342
NB/P	732/445-2769



available for faculty, staff, and students. For more information, visit <http://dml.rutgers.edu/>

Video production. The Division of Continuous Education and Outreach provides a range of television and other media services including recording of events or speakers and studio and documentary programs ready for broadcast or distribution on DVD. Satellite uplink, ISDN, and radio connections are also possible. To learn more, visit <http://rutgers.tv/>

SECURITY

OIT provides a set of tools that allow units to conduct vulnerability scanning, perform Intrusion Detection System (IDS) event analysis, vulnerability remediation, and reporting. For more information on the scanning program, see <http://infoprotect.rutgers.edu/ruscan/>.

Abuse and incident handling. OIT provides information and advice to departments on responding to a computer incident. In the event of a computer intrusion, re-installation, patching, and hardening of the operating system are recommended. Malware can often be removed with antivirus and anti-spyware products. When OIT receives reports of abuse, staff review and forward reports to departmental computing staff for resolution. Additional information is available at <http://infoprotect.rutgers.edu/cirt>.

Servers. The key to providing quality support is to develop a standardized method of installing, configuring and updating servers. New installations should be done behind a firewall or with no network connection, in order to prevent them from being compromised before security precautions are fully in place. Security-related patches must be installed within a few days of availability.

Servers should be housed in climate-controlled, restricted-entry locations. They should be backed up regularly and copies of the backups should be kept off-site to facilitate disaster recovery.

Firewalls and service minimization. Units are advised to carefully select which services are provided and obtained through the network (e.g. web services, FTP) and install regularly updated network or host-based firewalls on systems. Where a unit has many computers of the same type (e.g. many systems on faculty desks), units should develop a common guideline for which vulnerable services to disable and how to set up host-based firewall software.

Backups. Data, applications, and system files should be backed up on a regular schedule (normally, at least weekly). Backups can be done to tape drives, external hard drives, zip drives, flash drives, and writeable CDs, depending on the amount of data. A copy of all backups should also be stored at an off-site location, which could be based in a university unit in another building or on another campus. OIT can provide backup services to units on a contract basis. More information is available through local campus computing services as noted in Appendix 2.

Security for unit-based applications. University policy requires all members of the University community to create a NetID and associated password, allowing access to certain online university services. OIT recommends that units use the NetID and password for any services that will be generally available, so that

Local OIT campus divisions can help a unit prepare security plans, review system security, and help plan and deploy firewalls. Doing a full firewall deployment for a unit is a chargeable service, but consulting and reviews are available at no charge.

users will not need to remember separate information for each system that they use. OIT provides services to help units do central authentication based on NetIDs. These include RADIUS and LDAP.

OIT maintains a set of RADIUS servers, which can be used by units to check usernames and passwords in their applications. To arrange access to a RADIUS server, contact radius-support@dmx.rutgers.edu

LDAP can be used to verify that a NetID is legitimate, check a user's password, and check certain information about the user (e.g. whether he or she is a faculty member, student, etc). Contact ldap-support@rutgers.edu for more information.

Password security and one-time passwords. Passwords, alone, often do not provide high enough security for accessing data. For this reason, OIT recommends the use of one-time passwords for those staff who access sensitive data. The OIT Safeword authentication service provides a two-factor one-time password authentication system used to secure access to various systems and services run by OIT. This service may be utilized by groups within Rutgers if desired. For further information, send email to safeword_support@email.rutgers.edu.

Selected university-wide services that IT operations staff should consider using

Email

OIT maintains a central email service, which is available to all faculty, staff and students. Arrangements can be made to provide email service for units using OIT facilities, with email addresses using the department name rather than a generic name such as rci.rutgers.edu. Contact your OIT Campus Computing Division, or visit <http://email.rutgers.edu> to obtain information about departmental email services provided by OIT.

Mailing Lists

OIT maintains mailing list systems which are available to the Rutgers community. The software used on these systems permits lists to be maintained by a list owner, with the ability for end-users to enroll themselves automatically if desired.

Lists can also be generated automatically from administrative information. For example, a list can be created by authorized staff that includes all faculty, staff and students who are members of a particular unit or enrolled in a particular course.

Visit <http://email.rutgers.edu> for more information on both types of mailing list services operated by OIT.

Web Hosting

OIT maintains central web servers, which any unit can use. These provide services that allows web-based applications using such information sources as databases and forms. Unit web sites hosted on OIT servers can use a unit domain name. Contact your OIT campus computing division for more information.

Features of OIT hosted systems include linked SQL database systems, PHP programming facilities, enterprise class servers, server load balancing, and log analysis.

File Storage

OIT provides file space on central servers for individuals and units. This space can be used locally from the server for applications such as web services. It can also be used to store backup copies of desktop files. Contact your OIT campus computing division for more information.

For end-user support staff

Unit-based IT support includes the responsibility for systems and services utilized directly by faculty, staff, and students associated with the unit. The scope will vary greatly across disciplines and the complexity will increase with size. The model for support in units should be determined by the unit-based IT committee and should be determined by several factors including staffing level, equipment and application complexity, and individual preference for assistance. IT support staff should participate in risk self-assessment, perform system administration, respond to possible intrusions, propose security guidelines, and conduct training for end-users.

DESKTOP AND LAPTOP COMPUTERS

Management. The key to providing quality support is to develop a standardized method of installing, configuring and updating systems. Depending upon the size and complexity of the unit, this may involve a standard set of software that is installed by hand, or automated configuration tools. As part of the overall IT plan, a plan for systems management is a good way of managing this area of responsibility. A full plan should include approaches for:

- **Installing and configuring new systems.** A standard set of software should be installed and configured. New installations should be done behind a firewall or with no network connection, so as to prevent them from being compromised before security precautions are fully in place.
- **Doing patches and other software updates.** Security-related updates must be installed within a few days of availability. In almost all cases, automated tools should be used. Microsoft's Windows Update, running in automated mode, may be sufficient, although some departments prefer to use more sophisticated tools.
- **Specifying what faculty and staff should not do.** At a minimum, faculty and staff must not disable antivirus software or software updates. In some units, there will be further restrictions on installing software that has not been reviewed by IT staff.
- **Implementing security tools.** Security tools such as host-based firewalls and antivirus software, configuration strategies that minimize the number of services exposed to access from the Internet, and tools for automating software updates are often used.
- **Setting up desktops to enable a password protected screen saver after several minutes of inactivity.** This is important from a security standpoint if users walk away from their desktops.

IT staff in each unit should maintain contact with OIT and the rest of the university IT support community. OIT has a number of services to help units administer systems. In addition, contact with other units that have similar problems will often help identify tools and solutions. Information for support staff is available at <http://techdir.rutgers.edu>

For deans, directors, other unit heads
For IT operations staff
For end-user support staff
Desktop and laptop computers
Security
Training
For faculty and staff

A regular replacement cycle for hardware is important. Many units within the university replace desktop systems every 3 – 4 years. For many types of equipment, there are opportunities at least once a year to get particularly favorable pricing through the Rutgers Computer Store.

Storage. Business, financial, employee, research, academic, and other sensitive information should be stored on a centralized server whenever possible. Units may choose to host their own file server or to utilize OIT's remote file access service (Samba), which allows faculty and staff to store their data centrally. Contact your local campus computing services division for more information.

Software purchasing. Desktop software expenses can be reduced by taking advantage of special university pricing and site licensing arrangements. The software portal at <http://software.rutgers.edu/> simplifies the various license arrangements by presenting an appropriate view for faculty and staff and for students. To help the software collection evolve, OIT works with faculty and administrative liaisons through a software collection development process. Refer to <http://oirt.rutgers.edu/cmn/collection-development.html> for more information.

Applications support. Support for applications should be tailored to the faculty and staff in the supported community. This may include support for academic applications, business applications, and personal productivity software (like email and word processing). Contact your local campus computing services division for more information about these services.

SECURITY

Make sure that old equipment is disposed of following university procedures. Securely erase any disk that may have contained confidential information.

End-user support staff must ensure that faculty and staff are appropriately using antivirus software, exercising caution when opening email attachments, selecting hard to guess passwords and keeping them private, periodically changing passwords, backing up important files, using a password protected screen saver, and locking their computer when not in use.

TRAINING

New IT staff working in units throughout the university are required to complete the IT Certification Program, offered through the Department of Human Resources. Other staff are also encouraged to attend this program. Additional information is available at <https://uhr.rutgers.edu/profdev/pdp-programs.asp>.

Faculty and staff should receive IT documentation when they begin working in a unit. This may include brochures produced by the unit and by OIT, and information about websites containing additional resources.

IT staff should instruct faculty and staff to take advantage of training opportunities throughout the university such as those listed on the next page.

University-wide training opportunities

OIT. OIT offers free hands-on computer training and self-paced learning materials in applications such as email packages, web design and web programming, Unix, Microsoft Office, Macintosh operating systems, and statistical programs including SAS and SPSS. For more information, visit:

Camden: <http://edseries.camden.rutgers.edu/>

Newark: <http://edseries.newark.rutgers.edu/>

New Brunswick/Piscataway: <http://edseries.rutgers.edu/>

Libraries. The Rutgers University Libraries provide a range of instructional services to assist individuals and groups in learning about the library system, library services, information resources, and research tools. For more information, visit

http://www.libraries.rutgers.edu/rul/lib_instruct/lib_instruct.shtml

Division of Continuous Education and Outreach. The Division of Continuous Education and Outreach provides training on the eCompanion/eCollege course management system. For more information, and to register, visit

<http://ecompanion.rutgers.edu>

University Human Resources Professional Development Program

<http://uhr.rutgers.edu/profdev/>

Camden Campus – Instructional Design and Technology

The Office of Instructional Design and Technology provides training on the WebCT course management system. For more information, visit

<http://idt.camden.rutgers.edu/>

Newark Campus – Office of Academic Technology

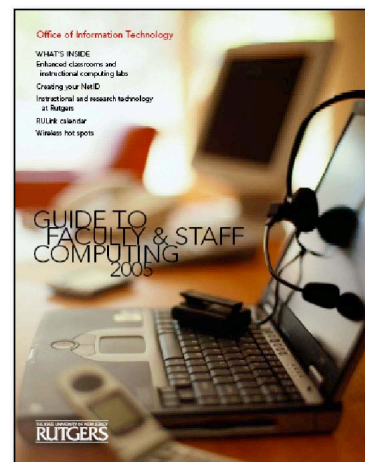
The Office of Academic Technology provides training on the Blackboard course management system. For more information, visit

<http://oat.newark.rutgers.edu/>

New Brunswick/Piscataway Campus – Center for Advancement of Teaching

The Center for Advancement of Teaching provides training in many software packages, including WebCT and Microsoft Office. For more information, visit

<http://cat.rutgers.edu/workshops/>



<http://oit.rutgers.edu/facstaffguide>

Fee-based training is also available from:

Center for Continuing Professional Development (CCPD)

<http://ccpd.rutgers.edu/>

Office of Continuous Education and Outreach

<http://ce1766.rutgers.edu/>

OIT Shared Services that Support Staff Might Consider Implementing

Rutgers Antivirus Delivery Service

The Rutgers Antivirus Delivery Service (RADS) ensures that freely available university site licensed antivirus software is kept up-to-date and that the virus scanning policy is set-up to keep your system virus-free. For more information, see <http://oit.rutgers.edu/rads/>

It is the responsibility of units to ensure that unit-based equipment has appropriate virus protection software, and both software and virus definition files are kept up to date.

Calendar Service

OIT operates a calendar server. It can be used to maintain individual calendars, as well as calendars for unit-based resources such as conference rooms. It has facilities for doing group scheduling. While the primary access is via the web, it will synchronize with Microsoft Outlook and handheld devices. Information on this service can be found at <http://rulink.rutgers.edu/>

Rutgers University Standard Software

The Rutgers University Standard Software (RUSS) is a compilation of common software that is available on a single installer. Antivirus software and the automated RAD client are included. RUSS is available at <http://software.rutgers.edu>.

For faculty and staff

This section is intended to provide general guidelines for faculty and staff who use IT facilities and services. Units should include this material or similar material in educating faculty and staff on local procedures and documentation.

Specific information aimed at faculty and staff can be found in OIT's "Faculty and Staff Guide to Computing at Rutgers." Because security, intellectual property and academic integrity, and instructional and research technology are such important issues, information about these areas is also included in this document.

SECURITY

A quick guide to security best practices and other resources and documentation is available at <http://infoprotect.rutgers.edu>.

Physical Security. All security starts by securing the physical machine from unauthorized users. To this end, computers should be locked to a piece of furniture – this is especially true for laptop computers.

Firewalls. Host-based firewalls are software that can be installed on a computer to restrict what is allowed in or out. They can be added to workstations and/or servers. It is a good idea to install a firewall if there is not already a network-based firewall or if all computers on the network are not secure. Firewall software can be found at <http://software.rutgers.edu/>.

System Updates. Software system updates enhance functionality and performance and correct deficiencies and security holes. Create a plan for upgrades and set aside funding that will enable you to stay ahead of the threat.

Antivirus Software. It is very important to have current antivirus software installed on personal and Rutgers-owned computers to prevent viruses from becoming operational problems. This software should not be disabled. OIT offers the Rutgers Antivirus Delivery Service (RADS) to assist in protecting computers. Information about RADS is available at <http://oit.rutgers.edu/rads>.

Passwords. Passwords are a readily available mechanism to prevent one individual from assuming another individual's identity. If an individual is logged into a computer and another user works at that computer, any actions performed by that user will be attributed to the original individual. The same is true if someone uses an individual's password to logon. It is important not to share passwords nor to let individuals work on a computer that they have not logged into.

Spam management. OIT offers spam management tools on all central systems. Further information is available at <http://email.rutgers.edu/>. For unit-based systems, reduced cost software is available by visiting <http://software.rutgers.edu>.

For deans, directors, other unit heads
For IT operations staff
For end-user support staff
For faculty and staff
Security
Intellectual Property and Academic Integrity
Instructional and Research Technology

Treat your password like your toothbrush. Don't let anyone else use it and get a new one every 6 months.
~ Cliff Stoll

DO NOT open attachments that are not expected, since email attachments are a prime way for viruses to be promulgated. Do not click on links to web pages that arrive in e-mail from unknown sources.

Working from home. Remote access to university data presents additional security concerns. If an individual's home computing environment is not secure, they can compromise the integrity of data on unit-based infrastructures, as well as on Rutgers-owned machines that they use. It is recommended that home computers not be used for university business unless they use antivirus protection and are regularly backed-up. They should also implement all security procedures discussed elsewhere in this document.

When logging into Rutgers resources from home, individuals should use a secure connection such as SSL, SSH, or the university's Virtual Private Network (VPN), which authenticates the individual as affiliated with Rutgers. Software for accomplishing this is available at <http://oit.rutgers.edu/vpn>.

Identity theft. Identity theft is a federal crime in which an imposter obtains information under false pretenses for personal gain. Information, such as social security numbers, drivers license numbers, and credit card numbers, can be stolen in several ways, however, computers have contributed significantly to the surge in identity theft over the past several years. Information about taking a proactive role in keeping your identity safe is available at http://rusecure.rutgers.edu/sec_aware/phish.php.

Data Backup. It is important to back up data regularly. Data can be backed up on removable media such as flash drives, CDs, DVDs, zip disks, and external disk drives or on a unit-based or central-based server or off-site location.

INTELLECTUAL PROPERTY AND ACADEMIC INTEGRITY

All Rutgers faculty and staff are responsible for respecting the intellectual property of others. This includes abiding by copyright and other restrictions, using others' work only with their permission, and properly acknowledging use of others' work. See <http://www.libraries.rutgers.edu/rul/copyright/copyright.shtml> for the proposed Rutgers copyright policy, as well as frequently asked questions.

Information about fostering academic integrity, strategies for preventing cheating, reporting violations, and policies on academic integrity for undergraduate and graduate students is available at <http://cat.rutgers.edu/integrity/index.html>

The Division of Continuous Education and Outreach provides access to and training in the application of Turnitin, a web-based class management tool that aids in the detection of plagiarism and more. Information is available by phoning 732/445-1907, ext. 6612.

INSTRUCTIONAL AND RESEARCH TECHNOLOGY

At Rutgers, instructional and research technology services are provided by a large number of units. Activities in this area are constantly evolving. A

complete and up-to-date guide to these services can be found at <http://oirt.rutgers.edu>.

Campus-based instructional support. In addition to support from staff in the Office of Instructional and Research Technology, campus-based instructional support staff offer services for faculty. The Office of Academic Technology in Newark also provides campus-specific coordination of instructional support activities.

Course management systems. Course management systems can be used to create entire online courses or to make supplementary materials available through the web. Features include electronic course rosters, a bulletin board system, online chat, student progress tracking, group project organization, grade maintenance and distribution, and auto-marked quizzes.

Enhanced/smart classrooms. Enhanced/smart classrooms contain equipment and network connections that can be used for multimedia instruction. For more information in Camden, <http://smartclassrooms.camden.rutgers.edu>; in Newark, http://tecn.rutgers.edu/classroom_support/smart_classroom_list.stm; and in New Brunswick/Piscataway, <http://cat.rutgers.edu/ecs>.

Gradebooks, rosters, and mailing lists. Gradebooks and automatically generated course rosters and class mailing lists are available on the web. (Gradebooks are also available through the course management systems, described above.) More information is available at <http://fas.rutgers.edu/computing/gradebook/index.shtml> and <http://www.acs.rutgers.edu/Apps/adminweb.htm>

RAMS, the Rutgers Automated Mass-Mailing System, allows an automatically updated email list to be generated based on demographic information. More information is available at <http://rams.rutgers.edu/>.

Instructional computing labs. Instructional computing labs provide facilities for hands-on computer instruction. These facilities can also make specialized software available for student use. For reservations in Camden, <http://computing.camden.rutgers.edu/reservations>; in Newark, http://www.ncs.rutgers.edu/forms/room_reservation.html; and in New Brunswick/Piscataway, <http://www.nbcs.rutgers.edu/ccf/main>.

Learning support. Rutgers Learning Centers include tutoring, academic coaching, course-specific study groups (supplemental instruction), course support, workshops, services for students with disabilities, and, in New Brunswick/Piscataway, interactive video review sessions on RU-tv hosted by faculty and tutors during exam periods. In Camden, writing assistance is also provided by the Learning Center. <http://rlc.rutgers.edu>

Campus-based instructional support

Instructional Design and Technology
<http://idt.camden.rutgers.edu>

Office of Academic Technology
<http://oat.newark.rutgers.edu>

Center for the Advancement of Teaching
<http://cat.rutgers.edu>

Course management systems

Blackboard
<http://blackboard.newark.rutgers.edu>

eCourse/eCompanion
<http://ecompanion.rutgers.edu>

Sakai
<http://sakai.rutgers.edu>

WebCT
<http://webct.rutgers.edu>

The Rutgers University Libraries provide many indexes, databases, electronic journals, electronic reserves, and other full-text resources. More information is available at <http://www.libraries.rutgers.edu/>

The Libraries also provide hands-on facilities for instruction. More information is available at <http://www.scc.rutgers.edu/scchome/facilities/facilities.htm>.

The New Brunswick/Piscataway Writing Centers (<http://plangere.rutgers.edu/index.html>) and the Newark Writing Center (<http://andromeda.rutgers.edu/~nwc>) provide tutoring in a full range of expository writing. The Writing Program also provides tutorials in basic software programs. More information is available at <http://getit.rutgers.edu>.

The Math and Science Learning Center on the Busch and Douglass campuses in New Brunswick/Piscataway provide study sessions, reserve materials, and K-12 outreach programs. More information is available at <http://mslc.rutgers.edu>.

Research support. The Office of Instructional and Research Technology (OIRT – <http://oirt.rutgers.edu/>) and Campus Computing Services work with researchers and their units to develop standards and recommended approaches for key technologies. Technical support is available on a wide variety of issues ranging from high performance computing with Linux clusters to licensing of software and data. OIRT provides consulting services to researchers in such areas as proposal development, facility design, and technical hires. OIRT also acts as a liaison to external initiatives and resources such as Internet2 and national supercomputing centers.

The Science Vision Group in Camden (<http://science.vision.rutgers.edu/>) coordinates computing activities of the Departments of Computer Science, Chemistry, Physics, and others.

Statistical work can be done on all OIT central systems, with special provisions for large disk space on rci.rutgers.edu, the New Brunswick/Piscataway campus central system. Users with specific needs for large-scale statistical work should write to help@lds.rutgers.edu.

Appendix 1: Sample Unit IT Plan

SCHOOL OF PUBLIC AWARENESS
THE DEPARTMENT OF SOCIAL ACTIVITIES
INFORMATION TECHNOLOGY PLAN

FY 2005

TABLE OF CONTENTS

Introduction by the IT Committee •	26
Reviewing the scope of activities that rely on IT •	27
Assessing successes, gaps, and needs •	28
Aligning resources with areas critical to what we do... •	30
Attachment 1: Equipment inventory •	32
Attachment 2: Sample project plan: Online Course Registration Exemptions •	33
Attachment 3: Project plan to address immediate issues •	37

INTRODUCTION BY THE IT COMMITTEE

The IT Committee was established in 2004 to create, manage, and evolve IT facilities and services. We coordinate strategic IT planning, IT project planning, and budget planning for IT for the department. We meet monthly with our IT staff to ensure alignment with overall departmental goals. Members include:

Chair – Professor A, a key faculty technology leader

Faculty

Professor B

Professor C

Associate Professor D

Associate Professor E

An involved teaching assistant

Staff

Person F, a technology support staff person

Person G, an administrative support staff person

Person H, the business manager

Students

Student I, undergraduate representative

Student J, graduate student representative

This document sets out our formal Information Technology (IT) plan for FY2005–2009, reviewing the scope of unit-based activities; assessing successes, gaps, and needs, and aligning resources with area identified as critical to unit business. It also includes project plans for the projects identified as critical for the next six month period. [Editor’s note: A project plan template is included in this sample plan]

The document will be reviewed in six months for updates to projects and budgets.

REVIEWING THE SCOPE OF ACTIVITIES THAT RELY ON IT

Our department's mission is to prepare students who are able to carry out the mandates of the social activities profession as generalists with a variety of people and with the most vulnerable members of society. The department seeks to develop a cadre of diverse, competent, practitioners who adhere to social activities' ethics and values and serve as advocates for social and economic justice.

Our goals are to:

- provide for the instructional needs of social activities students
- conduct cutting-edge research that contributes to the field of social activities
- perform public service in support of the needs of the citizens of the state

Overall Information Technology (IT) goals in support of the departments goals include:

For Instruction

- To use current teaching and learning technologies to enhance the educational experience for students and faculty

For Research

- To investigate advanced technologies to assist researchers in data collection
- To utilize IT to enhance research collaborations within and external to the university

For the Administration

- To develop interactive web applications for routine functions

For the Department

- To ensure an adequate, robust, reliable, and secure IT infrastructure within the department
- To identify and provide adequate technical support staff lines
- To upgrade the infrastructure to meet new requirements

Specific goals for the next year include:

For Instruction

- To advance technology use in the curriculum to include 30% of the courses offered

For Research

- To pilot Sakai as a vehicle to improve involvement of graduate students in departmental research
- To develop a better approach for modeling data collected by several of our research groups

For the Administration

- To develop an interactive web application for course registration exemptions

For the Department

- To establish an on-going funding mechanism with a calculated total cost of ownership (TCO)

Project plans for each of these activities will be developed following the template in Attachment 2. Progress toward attainment of specific goals will be analyzed twice yearly by the IT committee, which will provide status updates to the department chair at those times.

ASSESSING SUCCESSES, GAPS, AND NEEDS

To date, we have had many **successes** in using technology to support our goals. Some examples are listed below:

Technology Integration into the Curriculum

- The Department of Social Activities currently has 20% of its courses utilizing a variety of technologies.
- Of the 20%, half of the courses have utilized WebCT for course management. Of the WebCT users, most do not utilize full functionality of the application. Some only use it to distribute handouts.
- Some faculty have utilized email lists with class rosters for communication and discussion.
- Shared course calendars are utilized as a means to schedule and communicate events.
- Some faculty have put quizzes online for students requiring remote access.
- In some cases, study groups have been established and videoconferencing is used.

Technology in Research

- Desktop systems are used for most research
- The department has worked with the Psychology department to get access to software to administer and evaluate questionnaires
- Key software used for research includes SAS, SPSS, and Matlab. The department has worked with OIT to determine the best way to license this software
- The department is one of a group of departments participating in the New York Remote Data Center, giving access to detailed census data.
- Professor Hillary Bush is working with the Office of Instructional and Research Technology (OIRT) to pilot Sakai to provide discussion groups, mailing lists, and other collaborative approaches for involving faculty and graduate students in discussions about research in the department
- The departmental computing advisory committee has developed several strategies for using IT in grant-funded research. These include asking all grants to include 5% of their budget to support shared research facilities for the department, and a policy of working with the OIRT to evaluate the IT portion of all grant proposals.

Technology in Department Administration

- The business office uses a shadow accounting system to supplement the central system.
- The departmental administrator receives the class rosters from the central administrative computing services via a text feed.
- A shared calendar is utilized to schedule advisor meetings.

Technology Infrastructure and Staffing

- Our software and hardware inventory is up to date [Editor's note: A sample equipment inventory record is contained in Attachment 1.]
- Our IT staff member is provided with 2 days per month for study and training. In addition, she attends monthly events sponsored by OIT, and participates in relevant IT mailing lists.

We also have some **gaps**. Although we have a current network diagram, we do not know the following:

- Wiring plant : Is the cabling to code? Is the design optimal?
- Bandwidth: Is the capacity sufficient for our needs?
- Subnet allocation: Is our address space adequate? Is our subnet logically designated? Do we utilize private address space where appropriate?
- Security: What security measures are in place? Do we utilize a firewall? Do we have adequate physical security for our equipment closet?

Once we learn the answers to these questions, we may need to consider upgrading our infrastructure. A project plan will need to be developed to examine this.

In addition, we believe that our single IT staff member's responsibilities are misunderstood by the department as a whole. She should be:

- **Planning** – It is the responsibility of the IT staff member to maintain the LAN in “state of the art” condition. The UCS is routinely expected to assess the quality and reliability of existing hardware, software, operating systems and network components that comprise the LAN, and make recommendations for upgrade or replacement where necessary.
- **Performing server backups** – The IT staff member is responsible for conducting and verifying the validity of daily backups of the servers.
- **Providing user support** – The IT staff member represents the level one support for account holders on the LAN. In situations where she cannot answer technical questions or solve technical problems, it is her responsibility to use all available technical resources to discover and relate a solution back to the user.
- **Conducting network monitoring** – The IT staff member is responsible for monitoring the state of the network and general network throughput. Any serious degradation in performance of the network should be diagnosed to the extent possible. All unresolved network problems should be reported immediately to the appropriate central IT division.
- **Ensuring security** – The IT staff member also acts as the security officer for the LAN and is accountable for ensuring that all recommended security measures are in place for the LAN (firewalls/private address space) as well as the desktop equipment (updates/patches) in the department.
- **Coordinating research and instructional support:** The IT staff member works with the faculty advisory committee to recommend software and services to support research and instruction. She maintains regular contact with staff in other departments with similar research interests and technology, and with OIT staff such as those in the Office of Instructional and Research Technology.

The responsibilities of our IT staff person do not include affixing paintings on the walls, getting quotes for roofing repairs, or carrying heavy boxes. Using IT support in this way takes away time from important IT-related activities.

During the past year, we conducted a security audit of our department as requested by the EVPs on September 23, 2003. We looked at the following questions:

- What security risks exist?
- Is sensitive data stored locally?
- What security measures are in place to protect the integrity of that data?
- Do data management practices conform with institutional and governmental regulations and guidelines?
- Are faculty and staff educated to the dangers of Internet intrusions/viruses?
- Are operating systems properly updated and patched?
- Are firewalls utilized?
- Is antivirus software kept current?
- What guidelines are in place for the management of accounts and authorization and secure access to specific services?

We learned that we had a great **need** for planning and action in this area. A modified project plan was developed for this activity, since timing was immediate and cost not a significant issue. A copy of this brief project plan can be found in Attachment 3. We do not recommend using this type of project plan for longer term projects as it omits several important pieces of information. For that, we recommend using the template in Attachment 2.

Another immediate need is end-user training. Training can be handled through hands-on classes, lecture-style demonstrations, online tutorials, self learning materials, and individual on-on-one sessions. We will continue to examine this area as we move forward with our planning and attempt to ensure that training is incorporated into all project plans.

ALIGNING RESOURCES WITH AREAS CRITICAL TO WHAT WE DO

IT project prioritization

Our next step is to develop project plans for the specific goals listed on page 27. Following the submission of all of the project plans, the IT Committee will prioritize the various projects for implementation. Considerations will include whether there could be any economies realized by utilizing the same equipment, infrastructure upgrades, or staff resources. Investigations will also include discussions with other residents of our building as appropriate to determine if opportunities exist for cost-sharing. All proposed projects will be researched with central IT units to determine if planned upgrades to their infrastructure possibly affect our plans, or if there are services they afford the university that might be leveraged to fulfill some of the planned proposals. Further investigations will consider whether each project's implementation will integrate with existing technologies and will measure the potential challenge posed by incompatibilities.

Life cycle budgeting for IT

At the same time that we are planning for projects, we must also be planning for:

- **People** – training faculty, staff, and IT staff to make optimal use of cost-controlling processes and technologies.
- **Processes** – automating some tasks and streamlining others, ranging from asset tracking to software updating.
- **Technologies** – deploying information technologies that minimize and in some cases eliminate the widest range of labor-intensive tasks.

The historical budgetary view of IT equipment needs was that it was handled on a one-time capital basis for large, enterprise systems and on an as needed basis for desktop systems. This pattern has left us with a hodge-podge of equipment of various ages resulting in increased complexity for faculty, staff, and IT staff.

A Total Cost of Ownership (TCO) calculation will accomplish this more effectively. TCO will:

- Reveal costs and enables accurate measurement
- Improve decision-making; make justification more rational
- Improve IT cost management and budget controls
- Improve performance
- Enhance productivity and functionality
- Generate higher customer satisfaction
- Provide standard, consistent data
- Mitigate risks encountered within the IT environment
- Raise business value

TCO calculations include:

- Original cost of the computer and software
- Hardware and software upgrades and security considerations
- Additional equipment and software for projects
- Maintenance – hardware and software
- Technical support
- Training – end user and technical staff development
- Networking – equipment, infrastructure (wiring), and security considerations

Our TCO calculation for a three year cycle is shown below. We selected three years because the majority of our hardware warranties are of that length.

TCO /per client for three year cycle for our department of 60 members

'05 IT Projects		\$250.00	Internal funding
Workstation	Dell	\$550.00	Pentium® 4 3.0Ghz w/ Hyper-Threading 512MB 333MHz SDRAM (2 DIMM)
MS WinXP	license	\$50.00	
MS Office 2004	license	\$65.00	
Adobe Acrobat	license	\$50.00	
Exchange CAL	client	\$2.00	
WinZip	license	\$10.00	
Training	user	\$250.00	
Upgrades / Spare parts	client	\$50.00	Hard drives, Memory, cables, etc.
SMS	client	\$30.00	Remote control/Soft. management.
Server/Printing	client	\$50.00	Server upgrades/Printers
Network	client	\$20.00	Switch replacement
Support Staff	client	\$ 833.00	One full time technical support
	TOTAL	\$2,210.00	Per client/2004

Departmental budgeting will need to take these calculations into account.

ATTACHMENT 1: EQUIPMENT INVENTORY – RECORD 1

Computer Information

Fully-Qualified DNS Hostname:	homel.rutgers.edu
Machine Class:	Laptop
Machine Type:	PC
Manufacturer:	DELL
Model:	Latitude C640
CPU(s):	Intel Pentium 4 2000 MHz
Memory Module(s):	256 MB DIMM, 256 MB DIMM
Hard Disk(s):	IDE 40 GB
Monitor(s):	Standard DELL 17"
CD / DVD(s):	DVD-ROM/CD-RW
Network Card(s):	Onboard 3Com 10/100 Mbps (IP: 128.6.265.28) Onboard 3Com 10/100 Mbps (IP: 0.0.0.0)
Display Adapter(s):	ATI Radeon 7500 Onboard
Removable Media:	Floppy Drive 1.44 MB
Sound Card(s):	Onboard
Printer(s):	
Storage Card(s):	
Scanner(s):	
Software:	Microsoft Office XP w/ FrontPage 10.0, Adobe Photoshop 7.0 ActiveState PERL 5.8
OS:	Windows XP
OS Service Pack Number (if any):	1
Machine Has USB:	Yes
Machine Has USB2:	No
Service Tag:	89ZB354
System Is In Production:	Yes
Purpose:	Office workstation
RU Property ID:	33829746
Serial Number:	BN9896754f3
Date of Purchase (YYYY-MM-DD):	2002-11-15
Purchase Order Number:	R897654
Warranty Expires (YYYY-MM-DD):	2005-11-30
Service Information:	
Created By:	smith
Created On (YYYY-MM-DD HH:MM:SS):	2003-02-09 14:03:57
Last Updated By:	smith
Last Updated On (YYYY-MM-DD HH:MM:SS):	2003-02-11 14:49:45

Location and Contact Information

Equipment Location (Campus):	South
Equipment Location (Building):	Tower II
Equipment Location (Room):	14
Department / School:	Unit of Social Work/School of Social Awareness
Responsible Person (First Name):	John
Responsible Person (Last Name):	Smith
Primary Backup Person (First Name):	
Primary Backup Person (Last Name):	
Owner (First Name):	John
Owner (Last Name):	Smith
Created By:	Smith
Created On (YYYY-MM-DD HH:MM:SS):	2003-02-09 14:03:57
Last Updated By:	Smith
Last Updated On (YYYY-MM-DD HH:MM:SS):	2003-02-11 14:49:45

ATTACHMENT 2: SAMPLE PROJECT PLAN ONLINE COURSE REGISTRATION EXEMPTIONS

Goal

The goal of this project is to provide an online application for course registration exemptions. The current manual process is that the student must obtain a form, go to the professor and obtain permission, get the form signed, then go to the department business office, turn in the signed form; and only then will s/he be issued an exemption code. Next, the student has to go to the Registrar's office and submit the exemption code to properly register for the course.

The objective of the online application will be to eradicate the need to physically go from place to place in order to obtain an exemption code for a course. The application design will enable a student to access the request form online and submit it online. The student will be logging on with his/her NetID which will then pull the student's data and pre-populate the form with the usual demographics. The student will then identify the course for which s/he is requesting the exemption and submit the form.

The form submission will trigger a query to the registration database and identify the number of remaining exemptions (if any). At this point one of two things will happen. Either a code will automatically be generated and a message sent to the student's email address (with a copy to the department) indicating a link to obtain the code (after authenticating); or, if the professor has requested review and authorization privileges, then an email would be sent to the professor with a link to the submitted form. The professor can query the registration database to determine how many exemptions remain for any given course. The professor will then approve or not and the appropriate email will then be sent to the student with a copy to the departmental business office.

After obtaining the code, the student will be pointed to a link on the Registrar's website to formally submit the exemption and register for the course online.

Process

After meeting with OIT staff to discuss the project, we determined that the following is necessary:

- A description of the functionality requirements will be written and approved.
- A time frame will have to be defined.
- An estimate for the programming costs will be obtained to determine the financial feasibility of the project.
- Equipment for the project will be identified and if necessary, purchased.
- Support staff for the project will be identified; either in-house or hired externally.
- A project budget will be finalized and a funding source will be found.
- Once funding is identified, permissions will have to be established with the appropriate data custodian to access registration records. Note: The application must comply with all security recommendations for handling sensitive data, both in the architecture of the applications and in the physical security of the hardware.
- A regularly scheduled feed of those records will then be established with the administrative computing area.
- A rollout plan will have to be written to implement the new service
- An evaluation mechanism will have to be put in place to survey the results of the project and monitor improvements.

Time Frame

The target implementation date for this project is Fall '06. Proposed timeframes are as follows:

Planning	2 months	May/ June 05	Identifying the project goal, defining scope and the initial meetings with the resource group to establish feasibility and obtain an estimate.
Funding Proposal ^a	6 weeks	July/mid Aug. 05	With the estimate in hand, a funding request will be written linking the value of the project to the departmental goals and the overall mission of the university. Substantive support documentation i.e. examples of similar projects having positive impact at other institutions, will be included in the packet.
Application Development	4 months	mid Aug/ mid Dec. 05	The programming estimate will include the time element for each step in the application development and include a contingency for identified risk factors. Each function will be clearly described and agreed to by both parties to avoid scope creep. Regular review meetings will be scheduled in advance to set the timeframe.
Equipment	4 weeks	mid Nov/ mid Dec. 05	Required equipment will be configured and ordered within this period. Delivery dates will be monitored. Upon arrival, the equipment will be installed and tested.
Pilot Test	2 weeks	late Dec. 05	The application will be piloted by a small test group to identify any potential production problems prior to going live.
Communications Plan ^b	3 weeks	Jan. 06	The Communications Plan is a key document in rolling out a new service. It will identify who needs to be communicated with and when and how it will happen.
Training ^c	2 weeks	Jan / Feb 06	The optimal training situation will be determined.. If it requires hands-on training, arrangements for the use of a training lab will be made.
Implementation ^d	1 week	Feb. 06	If all the preparation was accomplished successfully, we expect that the actual implementation will be executed easily. However, since problems can occur, we will also create a roll back plan.
Feedback/ Survey ^e	2 weeks	ongoing	We will need to develop a mechanism to evaluate the success of the project. This will be done via an online survey instrument.

Attachment sections 2a–e show examples of plans in the identified areas.

Attachment 2a: Project Budget

Expenses	One Time	On-Going
Application development-programming	\$7,498	
Pilot phase	\$200	
Hardware (per attached quote)	\$2,500	
Server hosting		\$1700
Software (per attached quote)	\$400	\$200
Support staff	\$1,000	
Training	\$300	
Maintenance		\$500
Total	\$11,898	\$2,400

Attachment 2b: Communications Plan

Internal Project Communications

- All correspondence will be copied to the project manager, project team members, and consultants.
- Status reports will be sent to the department chair and IT committee members.

- All interactions will be done in email (lists will be created). Status reports will be drafted following meetings and posted on a website with links sent in email to the list.
- Interactions among team members will occur as necessary; the team will meet formally every two weeks.

External Communications

- Students will receive information about the project through web announcements and printed materials placed on departmental bulletin boards.
- Faculty will receive information at faculty meetings and through email announcements from the chair.

Attachment 2c: Training/Support/Documentation

A determination will be made as to the extent of the training requirements for all users of the application. Every effort will be made to ease the transition for the users. Training will be scheduled at their convenience. For the first few weeks of implementation, a dedicated help contact will be identified.

Where extensive training is required, we will develop a customized training program designed with the participation/input from the key participants. Documentation will be clear, concise, and written in terminology geared to the intended audience. It will answer questions like:

- What is going to happen?
- How will this happen?
- How long will this take?
- What will this mean to me?
- What are the benefits to me?

Attachment 2d: Implementation Process

If all steps in the project requirements have carefully been followed, the actual implementation should proceed smoothly. In planning the implementation, careful attention should be paid to the following:

- Scheduling – be sure to check all university calendars to insure that there will be no conflicts with any other events happening, i.e., network maintenance periods.
- If possible, schedule an overlap period when both the new and the old systems are available.
- Have all the necessary technical staff available for the cutover.
- Develop a roll back plan in case of an unexpected failure.
- Communicate status reports with all participants.
- After a smooth implementation, celebrate your project team's success.

Attachment 2e: Evaluation

Upon completion of the implementation process, an evaluation should take place. Research should identify benchmarks and metrics initiated to quantify results. If possible, several forms of data gathering should be utilized to obtain the most thorough picture. Satisfaction surveys, performance data and process improvement measures will provide mappings to goals and objectives with

associated costs. The evaluation statistics will either validate the investment or help to identify problem areas to improve.

Sample Evaluation

Sample follow-up email to student user

You have recently used the new online course exemption service and we would like to know if you would be willing to fill out a 5 minute survey telling us about your experience. In our efforts to improve student services, we need your feedback to grade how we are progressing with the improvement projects that have been implemented. Follow the link below and you will be eligible for a \$25 gift certificate to the university bookstore. Thank you for your assistance

1. Have you ever obtained a course exemption in the old manual process?

Yes___

No___

2. If yes, how would you describe that experience?

Satisfactory___

Unsatisfactory___

3. How would you describe the new online process?

Satisfactory___

Unsatisfactory___

4. Were the instructions clear and easy to follow?

Yes___

No___

5. Would you suggest a change to the new process?

Yes___

No___

6. If yes, please describe_____

7. Any comments?_____

In addition to the survey for students, feedback from the faculty and staff utilizing the application will also be required to obtain a complete picture of the success of the new service. The mechanism for this smaller group can be direct polling via phone or email.

ATTACHMENT 3: PROJECT PLAN TO ADDRESS IMMEDIATE SECURITY ISSUES

With the results of the audits in hand, the committee believed that some actions needed to take place immediately. With approval of and funding from our department chair and dean, the following activities will occur concurrently with other departmental IT planning.

- Regular testing of UPSs – UPSs will be tested monthly on the 1st.
- Provisions to continue operations in the event central services (RIAS) software is not available - A team will be created to develop a plan for business continuity in the event of central services downtime.
- WAN failure department functionality – Staff will have sufficient software to support short term network problems. OIT will provide a long-term solution.
- Staff duties and standards – Security duties and responsibilities will be designated in job descriptions and standards evaluated at regular intervals (quarterly).
- Funding – A sincere effort will be made to provide for additional security measures and personnel. Initially, 1% of the budget will be devoted to security purchases.
- Unauthorized users – Staff will be provided with a workshop on Security Awareness and Social Engineering to make them aware of security practices.
- Remote access authorization not known – The systems administrator will do a survey of alternative methods for remote access including modems, VPN, wireless, network connections and PDAs.
- Procedure for disposing of confidential and sensitive material on hard drives, tapes, floppy disks, CDs, etc. – The system administrator will provide process and documentation by 12/05 with the help of part-time students.
- Regular dates to test to verify backup capabilities – Back-up capabilities will be tested in June and January
- Policies. The IT staff member will write and implement policies, standards, and processes for passwords, account removal, elimination of chat clients, and trusted workstation security.

In addition, the following security precautions will be taken on individual workstations:

- Remote desktop and remote assistance will be turned off on XP machines .
- All workstations will be set up to implement a password-protected screensaver with a 5 minute maximum time.
- All workstations will have the latest service packs installed including software firewalls.
- Antivirus software will be installed on all workstations and set for auto updates.

Appendix 2: OIT Support Resources

Campus-Specific Resources

	Camden	Newark	New Brunswick/Piscataway
Website	http://computing.camden.rutgers.edu	http://ncs.newark.rutgers.edu	http://www.nbcs.rutgers.edu
Help Desk	856/225-6274 help@camden.rutgers.edu	973/353-5083 help@newark.rutgers.edu	732/445-HELP (4357) help@rci.rutgers.edu
Computer repair	856/225-6274 help@camden.rutgers.edu	973/353-5086 cs-net@newark.rutgers.edu	732/445-5000 computer_repair@email.rutgers.edu
NetID creation, user support	856/225-6274 help@camden.rutgers.edu	973/353-5083 help@newark.rutgers.edu	732/445-HELP http://rci.rutgers.edu
Departmental consulting and server support	856/225-6274 help@camden.rutgers.edu	973/353-5086 cs-net@newark.rutgers.edu	Solaris, Linux, Unix 732/445-5748 oss@nbcs.rutgers.edu , http://oss.rutgers.edu Windows, Novell Netware, MacOS and general consulting 732/445-6950 contactus@mssg.rutgers.edu
Telephone services	856/225-1766	973/353-5342	732/445-2769
OIT Training	856/225-6274 http://edseries.camden.rutgers.edu	973/353-5083 http://edseries.newark.rutgers.edu/	732/445-HELP (4357) http://edseries.rutgers.edu
Wireless networking	help@camden.rutgers.edu	help@newark.rutgers.edu	ruwireless@rutgers.edu

University-wide Resources

Website	http://oit.rutgers.edu
Overview for systems administrators	http://techdir.rutgers.edu
Computer store	732/932-5800 computer_store@email.rutgers.edu
Mainframe access (OFIS, SAR, Registration, etc.), SecurID Card, web applications	732/445-4638 help@acs.rutgers.edu
RUNet connectivity: network maintenance, new network allocation, new construction, renovations, moves, adds, changes, wiring, DNS, modems, voice, video	732/445-0327 noc@rutgers.edu
Oracle site license	732/445-3836 help@acs.rutgers.edu
RIAS/Procure to Pay accounts	732/445-8288 help@acs.rutgers.edu
Software site licenses	732/445-6950 software@mssg.rutgers.edu
University telephone office	732/445-2769 telephone@rutgers.edu

Security

Abuse	732/445-8011 or -2293 after normal business hours, abuse@rutgers.edu
Departmental security planning	732/445-8011, rusecure@rci.rutgers.edu
Kerberos services	732/445-8011, kerberos_support@email.rutgers.edu
LDAP services	ldap-support@rutgers.edu
RADIUS services	732/445-0327, radius_support@email.rutgers.edu
Safeword (Enigma cards)	732/445-8011, safeword_support@email.rutgers.edu
Security training	732/445-8011, rusecure@rci.rutgers.edu
University scanning	732/445-8011, http://infoprotect.rutgers.edu/ruscan

Meetings

Apple meeting	first Wednesday of each month at 12:00 pm, Busch Student Center
Camden UCS meeting	four times per year, contact 856/225-6152
Networking admin meeting	second Tuesday in January and July, Busch Student Center
Newark Information Technology Forum	second Wednesday of each month at 2:00 pm http://nitf.newark.rutgers.edu
OIT technology meeting	first Wednesday of each month at 1:30 pm, Busch Student Center
UNIX meeting	first Tuesday of each month at 1:30 pm, Busch Student Center

Mailing Lists

Administrative contacts for computing and software collection development	it_admin_liaisons@email.rutgers.edu
Computer store specials	computer_specials@email.rutgers.edu
Discussions about networking	network_admin@email.rutgers.edu
Discussion among webmasters and developers	web_developers@email.rutgers.edu
Faculty contacts for computing and software collection development	it_faculty_liaisons@email.rutgers.edu
Forum for all video issues	video_admins@email.rutgers.edu
Forum for high performance computing	hpc_admin@email.rutgers.edu
General announcements for departmental computing staff	all_dcscs_announce@email.rutgers.edu
Linux issues	linux_admin@email.rutgers.edu
Macintosh and related LAN issues	apple_admins@email.rutgers.edu
Network disruption announcements	net_people@email.rutgers.edu
Novell Netware issues	netware_admins@email.rutgers.edu
Novice web developer issues	web_managers@email.rutgers.edu
Official announcements for webmasters and developers	web_announce@email.rutgers.edu
PC and network OS issues	pc_lan_admins@email.rutgers.edu
Security announcements from vendors	security_alerts@email.rutgers.edu
Security issues	security_admins@email.rutgers.edu
Technical contacts for computing and software collection development	it_computing_liaisons@email.rutgers.edu
Unix issues	unix_admin@email.rutgers.edu

To subscribe to a mailing list, send mail to listserv@email.rutgers.edu. The message should contain a single line, of the form, subscribe LIST FIRST LAST, where LIST is the name of the mailing list and FIRST LAST is your name. The address from which your message comes will be added to the mailing list.

Appendix 3: OIT Services at Rutgers

ISSUE	OIT CORE SERVICE	UNIT RESPONSIBILITY	ADDITIONAL INFORMATION (\$ = MAY INVOLVE A FEE)
Networking:			
Backbone and network access	Operates Internet, I2 connections, University firewall, virtual private network (VPN), network address translation (NAT) service, dialups, campus backbone and building interconnectivity.	May operate VPN, NAT, dialups. Must follow University Acceptable Use Policy and networking policies, controlling access to authorized persons only, maintaining appropriate logs, and ensuring proper operation of the network.	noc@rutgers.edu 732/445-0327
Network addresses and DNS service	Has overall responsibility for IP addresses and DNS. Provides tools for units to manage DNS data themselves.	Responsible for keeping data about their systems current, and keeping contacts current for networks and systems.	noc@rutgers.edu 732/445-0327
Wiring within buildings, including adds, moves, and changes	Provides infrastructure design development, data electronics design, and project management services for the telecommunications component of new construction projects.	Wiring upgrades to an existing facility are funded by units or renovation budget. Wiring is performed by OIT or OIT contractor. Must follow University Telecommunications Design Standards and update documentation.	noc@rutgers.edu 732/445-0327 \$
Voice services	Acts as liaison between customer and vendor. Consults with units in design/procurement.	Responsible for funding telephones and other voice services. Works with OIT in design/procurement.	Camden: 856/225-1766 Newark: 973/353-5342 NB/P: 732/445-2769 \$
RU-tv cable television	RU-tv joint venture between OIT and University Relations in NB/P.	Responsible for funding video installations.	732/932-RUTV (7888) \$
Switches and other network equipment	Manages switches owned or installed by OIT. Provides policy and standards.	Responsible for LAN design requirements, equipment purchases, and operation of non-OIT equipment. May share responsibility for equipment (see: http://www.td.rutgers.edu/documentation/Policies/Switch_Access_Policy/)	Some OIT Campus Computing Divisions can manage unit-based networking equipment for a fee. Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-6950 \$
Wireless networks	RUWireless is wireless infrastructure for units in Camden and NB/P campuses. RN Wireless is infrastructure for units on Newark campus.	Responsible for funding wireless in their buildings, following standards, coordinating with other units in vicinity about overlap.	Camden: 856/225-6274 Newark: 973/353-5086 NB/P: installations@ruwireless.rutgers.edu \$

ISSUE	OIT CORE SERVICE	UNIT RESPONSIBILITY	ADDITIONAL INFORMATION (\$ = MAY INVOLVE A FEE)
Computer systems and common computer services			
Developing a unit-based IT plan	Provides planning assistance/consulting for developing IT plans. Also includes assistance in using IT for instruction and research.	Responsible for IT planning, implementing services within unit.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-6950 Instructional and research planning: http://oirt.rutgers.edu \$
Systems administration	Provides no cost telephone services to help units including 2 nd level and emergency support for unit staff.	Responsible for administering all local systems including account security, software updates, backups, disaster planning, etc. AUP and Standards for Management documents describe requirements for security, privacy, logging, and handling incidents.	Camden: 856/225-6274 Newark: 973/353-5086 NB/P, for UNIX/Linux systems: 732/445-5748 NB/P, for other systems: 732/445-6950 \$
Unit-based computing labs	Provides consulting for development of unit-based computing labs.	Responsible for arranging all aspects of support for unit-based labs. Some funding may be available from student fees. Allocation is handled at the campus level.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: feedback@computerlabs.rutgers.edu \$
Email systems for use by units	OIT email servers available to all faculty, staff, students. Provide support for email needs for units.	Units that run their own mail servers must make sure that they handle security issues such as not relaying spam and protecting against viruses.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-5748
Mailing lists	Systems for lists where readers join, or an owner creates members. Lists can be automatically generated from administrative data and class membership.	Units should review policies about bulk email. There are legal, policy, and technical issues.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-5748
File storage	Provides file storage on central systems. Provides consulting for storage/backup for unit-based systems.	Units that run file servers should be aware that Microsoft file sharing protocols have a history of security problems. Critical to review security-related settings and keep software up to date.	Backups of user/unit-based systems may be charged based upon resource availability. Camden: 856/225-6274 Newark: 973/353-5083 NB/P, for central systems: 732/445-5748 NB/P, for unit-based systems: 732/445-6950 \$

ISSUE	OIT CORE SERVICE	UNIT RESPONSIBILITY	ADDITIONAL INFORMATION (\$ = MAY INVOLVE A FEE)
Web hosting	<p>Provides central web hosting for individuals and units.</p> <p>Provides consulting, hosting, and design services for units.</p>	Units are responsible for finding the best and most secure way to host web services, following all relevant university guidelines.	<p>Camden: 856/225-6274 Newark: 973/353-5083 NB/P: for central systems: 732/445-5748 NB/P, for unit-based systems: 732/445-6950</p> <p>\$</p>
Calendar service	<p>Provides consulting on setup and use of RULink, the university-wide calendar service.</p> <p>Provides consulting and hosting for unit-based services.</p>	<p>Units that use the OIT service and that want resources such as conference room in the system must assign someone to maintain information about them.</p> <p>Units are responsible for finding the best and most secure way to host calendar services.</p>	<p>Camden: 856/225-6274 Newark: 973/353-5083 NB/P, for RULink: 732/445-HELP (4357) NB/P, for unit-based systems: 732/445-6950</p>
Streaming video services	Campus computing divisions in Camden and Newark, and the Department of Continuous Education and Outreach (DCEO) provide access to streaming video servers.	Units are responsible for finding the best and most secure way to host streaming video services.	<p>Camden: 856/225-6274 Newark: 973/353-5083 NB/P (DCEO): 732/445-1907</p> <p>All campuses-NJEDge.Net: 973/596-5490</p>
Applications	Provides consultation to units at an early stage on any projects that will use university data, which would benefit from integration with OIT applications, or which use technology that may have wider application within the university.	Units developing applications should consult with OIT at an early stage on any projects that will use university data, which would benefit from integration with OIT applications, or that use technology that may have wider application within the university. Should also coordinate authentication with OIT, and follow best security practices.	<p>Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-6950</p>
Software	<p>Tracks use of major software packages to determine the best way to purchase and license software. OIT aggregates demand and offers site licenses and discounts to units.</p> <p>Public software mirror, training, limited help desk support, software in public labs. Site license for McAfee antivirus software.</p>	Responsible for providing software for their systems, making sure it is properly licensed, and that all staff understand responsibilities for intellectual property. Also responsible for keeping up to date on security and other updates.	<p>732/445-6950 http://software.rutgers.edu</p> <p>\$</p>

ISSUE	OIT CORE SERVICE	UNIT RESPONSIBILITY	ADDITIONAL INFORMATION (\$ = MAY INVOLVE A FEE)
Hardware sales	Rutgers Computer Store provides negotiated prices for common systems.	Responsible for purchasing, installing, and configuring computers in accordance with university policies.	Camden: 856/225-6274 Newark: 973/353-5086 NB/P: 732/932-5800, http://computer-store.rutgers.edu \$
Computer repair	Provides warranty and fee-based service for computers, printers, and peripherals.	Responsible for maintenance of equipment, to the extent not covered by warranties.	Camden: 856/225-6274 Newark: 973/353-5086 NB/P: 732/445-5000
Security			
Security planning	Offers template for developing security plan and many technical resources. Provides unit-based consulting.	Responsible for security of local systems and networks. Security plan required as per 9/23/03 EVP memo.	732/445-8011 rusecure@rci.rutgers.edu
University firewall	Operates university firewall, which protects the university network from many types of attack from the Internet.	NA	732/445-0327 noc@rutgers.edu
University Virtual Private Network (VPN)	Consults with units on using Virtual Private Network to access services such as Windows file sharing that are protected by the firewall from outside Rutgers.	Units may make use of the VPN (http://oit.rutgers.edu/vpn) to access services such as Windows file sharing that are protected by the firewall from outside Rutgers.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-HELP (4357)
Authentication services	Can give units access to central authentication services via Kerberos, RADIUS, LDAP, and Safeword.	Responsible for controlling access to unit-based systems, implementing password policies as appropriate, and setting and enforcing policies needed to maintain password quality and prevent inappropriate sharing.	732/445-8011 radius_support@email.rutgers.edu ldap-support@rutgers.edu kerberos_support@email.rutgers.edu safeword_support@email.rutgers.edu
Vulnerability scanning for system-based security flaws	Provides tools for unit self-scanning. Conducts targeted vulnerability scanning based on threat.	Expected to deal with significant vulnerabilities exposed by scans. Units with firewalls or particularly sensitive data may need to do their own scans.	732/445-8011 ruscan@rutgers.edu
Antivirus protection	Provides central management for virus scanning for central and unit-based systems. McAfee virus protection software available at no cost.	Responsible to make sure that systems are protected.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P, for central mgmt: 732/445-5748 NB/P, for unit-based systems: 732/445-6950 http://oit.rutgers.edu/rads

ISSUE	OIT CORE SERVICE	UNIT RESPONSIBILITY	ADDITIONAL INFORMATION (\$ = MAY INVOLVE A FEE)
Spam management	Provides central management for spam filtering for central and unit-based email systems. Free and reduced cost spam management software available for units.	Users define actions taken as part of the spam management functionality	Camden: 856/225-6274 Newark: 973/353-5083 NB/P, for central mgmt: 732/445-5748 NB/P, for unit-based systems: 732/445-6950 http://software.rutgers.edu \$
Incident handling	Processes complaints of abuse and security breaches from systems inside Rutgers. Reports are forwarded to the administrators of the systems where the problem occurred.	Staff are expected to deal with abuse and other attacks coming from their systems in a timely fashion. Often means significant changes to software or configurations to improve security.	732/445-8011 abuse@rutgers.edu
Unit-based firewalls	Recommends approaches for implementing firewalls. Consults with units on requirements and implementation.	Units should consider a network-level firewall or host-based firewall software. It is the responsibility of units to assess security needs and implement firewalls where necessary.	Camden, 856/225-6274 Newark, 973/353-5086 NB/P, 732/445-6950 \$
Information and Training			
Help desks	Primary support for all OIT services.	NA	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-HELP (4357)
Documentation and online information	Available on OIT websites and public locations such as labs.	NA	http://techdir.rutgers.edu
Orientations	Participation in all relevant orientation programs.	Units should contact OIT about programs for prospective students and new students, and should include OIT presentations and materials in programs.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: 732/445-HELP (4357)
IT certification training	Mandatory training for all new IT staff at Rutgers	Units should ensure that all new IT staff attend IT certification training.	University Human Resources: 732/932-3020
IT support meetings	Conducts regular meetings on all campuses for IT support staff focusing on key technology areas.	IT staff should participate in activities that are relevant to their job functions. Units should provide release time for IT staff to attend these meetings.	See Appendix 2
IT staff mailing lists	Facilitates mailing lists for staff involved in support of most key technology areas.	IT staff should register for mailing lists that are relevant to their job functions.	See Appendix 2.

ISSUE	OIT CORE SERVICE	UNIT RESPONSIBILITY	ADDITIONAL INFORMATION (\$ = MAY INVOLVE A FEE)
IT training courses	Training is done by OIT, the Division of Continuous Education and Outreach (DCEO), the Libraries (RUL), University Human Resources (UHR), the Office of Instructional Design and Technology (Camden), the Office of Academic Technology (Newark), and the Center for Advancement of Teaching (NB/P).	Other units that provide IT training should contact Human Resources to be added to the list.	OIT: http://oit.rutgers.edu/training DCEO: http://ce1766.rutgers.edu RUL: http://www.libraries.rutgers.edu/rul/lib_instruct/lib_instruct.shtml UHR: http://uhr.rutgers.edu/profdev Camden: http://idt.camden.rutgers.edu/training.htm Newark: http://oat.newark.rutgers.edu NB/P: http://cat.rutgers.edu/workshops
Application services			
Core applications	Provides services that support entire university including administration of students from the time they are prospective students through graduation, administration of faculty and staff, university financial management, and auxiliary services.	NA	http://www.acs.rutgers.edu/ (Select Link: Core Services)
Faculty/staff applications	Provides access to web-based applications such as the absence reporting system, and address directory update.	Requires NetID.	http://www.acs.rutgers.edu/ (Select Link: Faculty/Staff)
Prospective student applications	Provides access to web-based applications such as the undergraduate application.	Requires NetID.	http://www.acs.rutgers.edu/ (Select Link: Prospective Students)
Student applications	Provides access to web-based applications such as registration, schedule of classes.	Requires NetID.	http://www.acs.rutgers.edu/ (Select Link: Current Students)
Web Online Payments (WOLP)	Provides units with the ability to accept credit cards via an online web application.	Units are required to develop an online storefront that integrates with the WOLP module.	732/445-4646 \$
Data feeds	Provides data extracts for unit-based activities.	Units are required to define data requirements and ensure a secure infrastructure for data delivery.	http://www.acs.rutgers.edu/ (Select Link: Access)

ISSUE	OIT CORE SERVICE	UNIT RESPONSIBILITY	ADDITIONAL INFORMATION (\$ = MAY INVOLVE A FEE)
Instruction and Research			
Computing labs	Labs are available on all campuses for students, faculty, and staff.	Faculty are asked to request new software for placement on lab systems as early as possible. It can take up to 90 days to install.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: http://www.nbcs.rutgers.edu/ccf/main
Instructional computing labs	Facilities can be reserved for hands-on use in class. Facilities are also available for units to conduct their own hands-on training.	Responsible for arranging all aspects of support for unit-based labs.	Camden: 856/225-6274 Newark: 973/353-5083 NB/P: http://www.nbcs.rutgers.edu/ccf/main
Enhanced/smart classrooms	Enhanced/smart classrooms contain equipment and network connections that can be used for multimedia instruction.	Faculty who wish to reserve an enhanced/smart classroom should contact http://scheduling.rutgers.edu	Camden: http://smartclassrooms.camden.rutgers.edu/ Newark: http://oat.newark.rutgers.edu/smartclassinfo.html NB/P: http://cat.rutgers.edu
Online collaboration tools	Sakai is a tool for collaboration, providing discussion groups, mailing lists, and list archives.	NA	http://sakai.rutgers.edu
Web-based instructional systems	WebCT in Camden and NB/P, with the Office of Instructional Design and Technology and the Center for Advancement of Teaching, and Blackboard in Newark, with the Office of Academic Technology. Sakai in pilot stage. eCourse available for fully online courses and eCompanion for hybrid courses through DCEO.	NA	NA
Facilities for research use	Provides shared resources, such as Unix-based time-sharing systems, and a system for large-scale statistical work. Tracks commonly used research technologies and can make recommendations for implementing unit-based facilities.	NA	NA

Glossary

Acceptable Use Policy (AUP)	Rutgers policy for use of computing systems.
Data custodian	An individual who takes responsibility for the security and confidentiality of any sensitive data.
Disaster recovery	A plan for duplicating computer operations after a catastrophe occurs, such as a fire or earthquake. It includes routine off-site backup as well as a procedure for activating vital information systems in a new location.
Domain name system (DNS)	A database of addresses of Internet sites.
Firewall	A method of preventing unauthorized access to or from a particular network; firewalls can be implemented in both hardware and software, or both.
Internet2	A collaborative effort by more than 130 U.S. research universities, a number of federal agencies, and many leading computer and telecommunication companies to accelerate the next generation of Internet technology. Rutgers is the only public university in the state of New Jersey that is a member of this group.
Internet Protocol (IP)	The address of a computer on a TCP/IP (Transmission Control Protocol/Internet Protocol) network. IP addresses are written as four groups of up to three digits (e.g., 169.237.104.18).
Kerberos	A program that will reject a password it considers too common or too easy to guess. Its purpose is to encourage choosing passwords which cannot be easily guessed by someone meaning to do you or your computer files harm
Lightweight Directory Access Protocol (LDAP)	A set of protocols for accessing information directories
Linux	A very popular version of the Unix operating system that runs on a variety of hardware platforms.
Modem	A device which modulates and demodulates signals on a carrier frequency and allows the interface of digital terminals with analog carrier systems
NetID	In order to use any central computing facilities at Rutgers, you need to create a username and password. The same username is used for a variety of academic and administrative services, including modems and web pages such as course registration and checking on financial aid status. The username is your NetID.
Online Financial Information System (OFIS)	OFIS permits online access to financial accounting and budget data to authorized users throughout the university.
Patches	Updates that “fix” an inherent flaw in programs that you have on your computer, or flaws in an operating system.
Radius	Provides authentication for the University modems, RIAS, and web servers. It is available for use by any system at Rutgers that needs to verify the identity of potential users.
RULink	University wide calendar system
Rutgers Antivirus Delivery System (RADS)	RADS keeps antivirus software on systems up-to-date and ensures virus scanning policies are set to keep systems secure and virus-free.
Rutgers Integrated Administrative System (RIAS)	The Rutgers online purchasing system.

Safeword	The Safeword authentication service provides strong authentication to validate the identity of a token holder. All users of the service are individually registered with the system and the resulting security is by far the strongest of any service available at Rutgers. This technology is used to secure access to various systems and services run by OIT and may be utilized by groups within Rutgers if desired.
Sakai	A higher education community project to develop and support a new collaboration and learning environment. The Sakai system is a potential alternative to course management software such as Blackboard and WebCT and is intended to facilitate collaboration in research, administration, and service, as well as in courses.
Student and Exchange Visitor Information System (SEVIS)	A tracking system, fully implemented by the United States Citizenship and Immigration Services that requires universities across the United States to report information about F, J and M non-immigrant categories.
Site license	A license that gives permission to use a software package on more than one system. Site licenses are a means of providing a bulk rate to schools that want to use software on many computers.
Secure shell software (SSH)	SSH software provides secure logon for Windows and Unix clients and servers. SSH replaces telnet, ftp and other remote logon utilities with an encrypted alternative.
Secure Sockets Layer (SSL)	The leading security protocol on the Internet. SSL is widely used to validate the identity of a Web site and to create an encrypted connection for sending credit card and other personal data.
Subnets	A division of a network into an interconnected, but independent, segment, or domain, in order to improve performance and security. Because traffic is often the heaviest within a department, and Ethernet is the common network technology, the subnet limits the number of nodes (clients, servers) that have to compete for available bandwidth to a confined geographic area. A subnet also allows multiple users to access the Internet with the same subnet address.
Switch	An electronic device that opens or closes circuits, changes operating parameters or selects paths either on a space or time division basis.
Virtual Private Network (VPN)	Technology used to allow access to resources that are restricted to members of the Rutgers community.
Vulnerability scanning	Security measure the campus has implemented to help protect the campus computer network and individual computers from viruses and other threats. A key component of this measure is the Vulnerability Self Scan, which allows individuals to scan their computers and access instructions for fixing any problems found.

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Office of Information Technology
Rutgers, The State University of New Jersey
96 Davidson Road
Piscataway, NJ 08854-8031
<http://oit.rutgers.edu/unitguide.pdf>

RU-0506-0029/2M

Printed on Recycled Paper 