

**Using Information Technology to
Achieve the Strategic Goals of
Rutgers, The State University of New Jersey**

**Appendix 4: Report of the Business and Enterprise Services
Subcommittee**

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

Committee members

New Brunswick:

DiPaolo, S
Drumheller, J
Knight-Cole, C.
Lige, J.
Martin, A.
Rash, J.
Rose, B.
Stein, T.
Woodward, D.

Newark:
Brancato, P.
Rimal, S.
Torres, A.

Camden:
Gwalthney, D.
Rivera, R.
Ryan, T.

Student Representative:
Fensterheim, D.

OIT Members/Advisors:
Gordon, C.
Mundrane, M.
Williams, D

Executive summary

The sub-committee identified four (4) key areas related to the *Enterprise/Administrative Systems* and six (6) for *Business Services* as follows:

Enterprise/Administrative Systems

- Enterprise and Financial Systems
- Student Systems
- Security Framework
- Identity Management

Chairperson

A. Martin
J. Rash/B. Rose
T. Ryan/Jordan
T. Ryan/Jordan

Business Services

- Voice & Video
- Networking, Desktop Computers, Email, & Calendar

Chairperson

D. Gwalthney
A. Martin

The sub-committee reviewed all the draft reports and developed the following high priority strategic recommendations based on the overall vision and critical success factors outlined in each individual report.

Enterprise/Administrative Systems Recommendations

Recommendation 1: Implementation of an *integrated administrative system* including, student, human resources, procurement, payroll, contracts/grants and other financial systems. Implementation of such a system must provide the University community with the ability to automate manual processes, access and manipulate timely data.

Strategies:

- Rutgers University is faced with a choice between different strategies for the future of its core financial administrative systems. For example, an ERP approach using Oracle or another vendor supplied software to provide integrated administrative systems or the 'Best of Breed Approach'. The Best of Breed Approach employs diverse solutions that can be relatively easily integrated with existing financial systems and new financial administrative systems.
- The University is currently exploring the implementation of the ORACLE General Ledger system but the final implementation time and cost is still being evaluated. When complete, this can be used as a benchmark or estimate for implementation of additional modules.
- For student systems employ a solution that can be integrated with existing systems. Several strategies could be explored such as: a partial ERP, a "Best of Breed" approach for individual units, in-house re-engineering of existing systems along with the development of new applications using current technology, or a combination of the above options.

Recommendation 2: Empower the University community with the necessary tools to facilitate the access to "integrated and near time" data in a quick, easy and timely fashion. Accurate and reliable data should be the basis of a more global view of the University and would provide decision makers with a consistent and dependable means of obtaining information.

Strategies:

- A *data warehouse* that provides user-friendly data access and central repository of all core University data and reporting spanning for student, administrative and financial data.
- Implement *electronic work flows* to expedite transactions in all administrative systems resulting in information readily available to the University community.
- In order to provide *data access in an efficient and secure fashion*, a defined process must be developed to verify a user's identity in a secure yet fluid manner.
- Until the core administrative systems are integrated with near time data, the University must develop university wide solutions that will provide the University community with *supplemental capabilities* to access and manipulate financial, student and administrative near time data.

Business Services Recommendations

Recommendation 1: *Centralized network* is a key strategic resource and a “strategic differentiator” in higher education. Consequently, this institution must continue to *maintain, enhance and evolve the network infrastructure* as new technologies emerge. Over time, more services must be incorporated over the increasingly capable network to allow us to provide a reliable, available, secure, adaptable, fault-tolerant and high-performance data communication network to the University community.

Strategies:

- Ensure our network fully supports the *high-performance* requirements needed for enhanced applications.
- Maintain, implement and enforce formal University-wide *policies and procedures* addressing networking issues.
- Implement *network redundancy* to reduce single points of failure to minimize local network outages.

Recommendation 2: Develop an *integrated communication structure* for voice and video with multiple solutions and defined university wide minimal standards that takes advantage of the existing university infrastructures for voice and video services. Network design and capacity must be included in the planning with an eye toward a much longer term strategy of the integration of data, voice and video.

Strategies:

- Develop *broad voice services standard* for University faculty and staff including minimal features such as: voice mail, auto attendant, call forwarding, caller ID, call transfer, and speaker phone on either hard or soft keys. Additional features suggested are found in the survey in the Appendix.
- Develop an *effective funding model* that includes resources for maintenance and capital investments that meet the current and future directions of voice/video services in the market.
- Develop a *long term IP Telephony solution* (Voice over IP) to be incorporated into the planning for PBX systems that includes considerations for network capacity, Quality of Services, reliability, security, and new applications
- *Centralized clearinghouse* to coordinate and communicate all activities related to video distribution and creation at the university.

Identity Management and Security Framework

Recommendation 1: Provide a cohesive centrally managed *identity management architecture* that supports the evolution of system processes and services. One user; one identity; one infrastructure.

Strategy: Establish a University wide identity management system capable of managing and identifying each individual/entity based upon the wide variety of roles presently utilized at this institution for student, faculty, staff and the rest of the University community. This system must also have a centrally managed infrastructure to authenticate people or servers seeking access to service and/or data.

Recommendation 2: Continue to *maintain the distributed security model* that requires both central computing services and business units to follow the same security framework.

Strategies:

- Provide adequate resources and skilled staff to support the current distributed computing services and data security models.
- Continue to develop, refine and monitor information security policies, procedures and University wide standards for systems and network.
- Develop *disaster recovery and business resumption plans* University wide as well as by unit and/or department.
Maintain a robust and reliable network infrastructure within the University.

Attachment: Enterprise and financial systems

Overview

All University employees are responsible for securing and caring for the University's assets. For those charged with the responsibility of managing financial data, there is a great risk in their ability to secure these assets without a centralized and integrated administrative system. Departmental grants and other external funding sources have grown considerably while departmental staff support and the tools with which they accomplish their goals have remained relatively constant. In addition, most units are currently staffed with generalists who perform a wide range of duties that do not require the skill and level expertise necessary to successfully and efficiently manage the funding at more detail level. With the implementation of an integrated system, the academic and administrative departments will be able to increase efficiency and more appropriately utilize staff. Departments will have the option of hiring targeted financial and HR expertise and will through these new staff, gain a broader sense of how to protect their unit's resources. Focus can be spent on optimizing and increasing these resources rather than how to manage the detail.

Future State

Vision

The University will provide the infrastructure, facilities and services to enable its community to make optimum use of computing facilities by providing an integrated, near-time and user-friendly computing environment where the faculty, staff and students will be empowered. This ability to gain secure and timely access to systems and data in order to make improved decisions will allow the institution to move forward in obtaining, receiving and better utilize resources. Accurate and reliable data should be the basis of a more global view of the University and would provide decision makers with a consistent and dependable means of obtaining information.

Objectives & Strategies

- To promote the establishment or re-engineering of common and outdated streamlined business practices that result in improved services and data integration.
- To meet the unique customer needs across disciplines and campuses.
- To provide integrated financial applications for improved access on reporting and querying to provide more opportunities for the better management of funds.
 - A meaningful data warehouse that provides a central and standardized repository of all core University data and reporting spanning both student and administrative/financial data.
 - Allow departments with appropriate IT staff resources to have direct access to their data.

- In order to provide these mechanisms, much effort will be required in verifying users' identity in a secure, yet fluid manner.
- One or more University wide *supplemental accounting* systems should be considered for users who have a need to supplement the available data warehouse options.
 - To move the University forward in providing business practices utilizing electronic work flows to expedite transactions resulting in information readily available to faculty, students, administrators, staff and alumni.

Critical Success Factors

- **Support from University Leadership**

It goes without saying that support from University leadership to implement our vision of the future state of our enterprise wide financial systems is crucial. The championing of our vision by the leadership will determine the business culture and the financial resources allocated to materialize the successful implementation of this vision both internally and externally. Internally, the University leadership support will facilitate the University providing the infrastructure, facilities and services to enable its community to make optimum use of computing facilities in an integrated, near-time and user friendly computing environment where the faculty, staff and students will be empowered resulting in enhancing our mission of financial transparency. Externally, RU will set the standard of how a large, multi-campus educational institution can benefit all its constituents by University leadership's "support of our academic tradition with superb research facilities, a top-ranked library system, and a sophisticated computer network".
- **Buy-in from University Community**

Above everything else, this needs to be considered collaboration amongst all parties. Since many of the users will be resistant to change the comfortable and knowledgeable way in which they currently manage their day-to-day business it will be imperative to both educate and pay attention to the community at large. The enormous obstacles that come without buy-in could either pressure the administration to provide expensive customizations or create a system where the users chose not to avail themselves of its capabilities. To begin to establish this level of trust, it is essential that we heavily involve and place responsibility with members of the community at every level. It will be a tremendous commitment on the part of the University and will come with great disruption to our daily lives given our limited staff and the need to maintain the level of work necessary to conduct business as usual. We will need to listen to the concerns of all and, in the same process, empower them to become part of the team for this very significant challenge. Thus it is important to show them that within time, the new system will provide them with more accurate and timely information and reporting capabilities.

- **Promote Effective and Value Added Communications**
In order to facilitate open and candid discussions with the University community we must first educate them as to what the process will entail and at the same time provide the assurances that their opinions matter and are a necessary part of implementation. It is necessary to have representation of all parts of the current process as well as several venues for those not able to serve on the various committees to express their concerns. Users need to understand what they will gain from this process so that their participation will be a means to an end rather than just a non-contextual opinion. There are many ways in which we can promote such discussions such as informal committees, formal committees, multiple e-mail list serves, informative web sites and hands-on workshops.
- **Changes in the Core Organizational Culture / Business Processes**
It is essential that the University community take a serious look at the business process with the goal of streamlining this process. We have to be willing to critically assess what our needs are and find ways of meeting those needs with the new system. If we refuse to make needed changes to the process and instead change the system to meet our practices, the cost of implementation will skyrocket and the changes could seriously impede the system causing the implementation to fail. Once the process has been redefined, departments will need to accept responsibility for their actions. Departments must be aware that with empowerment comes responsibility. Individuals with the authority to create or approve transactions must be thoroughly familiar with University policies and procedures and ensure that every transaction they process or approve is in compliance with these policies. The recent publicity and investigations into University practices clearly has demonstrated that any impropriety can have serious consequences to the University.
- **Quality & Comprehensive Training & Education**
In order to insure user acceptance of a new system, users need to become comfortable using the system and have confidence in it. A thorough and comprehensive training program, including “hands on” training and ample user documentation, will provide the users with a high degree of acceptance. For training to be of maximum value, it should occur as close to the “go live” date as possible.
- **Integration of Financial Systems**
A true integration of all financial systems is necessary to eliminate duplication and to ensure that data in one system agrees to data in all systems. If this integration is lacking, it will become extremely difficult to obtain reliable data. As changes are made to account structure and account attributes, it is essential that all systems are capable of accepting and transferring data in the new formats.
- **Timely Transaction Processing in Financial Systems**
Timely transaction processing is one of the most important elements to decrease

the dependency departments have on supplemental systems. If data can be retrieved within a day after it is submitted, departments will have less of a need to reenter this data into their own system. This will save considerable time and effort on the part of departmental staff allowing them to deal with more important issues. Departments are being asked to be responsible for their areas in all-financial aspects. Many of these duties, such as monitoring departmental equipment, suffer now because the staff is so overburdened. The elimination of these extra steps should provide time for departmental administrators to better handle their other responsibilities.

- **Commitment to Provide Secure and Timely Access to Financial Data**
If there is one common consensus among the faculty and staff on the real need of our existing financial systems, it is integration of the many modules in existence. This integration has to be concomitant with vigorous commitment to providing secure and timely access to financial data to the users making financial decisions. This concomitant is a major achievement benefiting the students, faculty and staff. Given the current regulatory environment and the evolving technological improvements, this access has to be an automated process based on our work roles resulting in increased productivity.
- **Web Based, Intuitive and User- Friendly Environment**
Most potential users of a new financial system are already familiar with the Internet and web page navigation. Implementing a system, which takes advantage of these familiarities, will ease the training burden as well as provide the users with a level of comfort.
- **Commitment to Empower Staff**
As part of implementing a new system it is also important to review business processes. It is an excellent time to eliminate non-value added processing steps, such as numerous transaction reviews and approvals. As part of this elimination process, it is critical the users be given both authority and accountability when using the systems to perform their jobs.
- **Commitment to resolve gaps between institutional / campus requirement and application functionality**
One of the largest obstacles facing us will be in the continued desire for departmental supplemental systems and the organization of these vast needs. In some cases these needs will be resolved through changes in our current culture and education, but departments will continue to have legitimate requirements that the system will need to provide. Since modifications to the purchased applications are problematic and costly, we must find a way to provide the necessary information to the majority of users within the system's capabilities. In addition, there will be a great need for staff resources so expenditures on supplemental systems should be avoided. Once a system is provided whereby the necessary information is entered and available at near time, reporting of this information will be the greatest need. Data warehousing must be a University

priority. All administrative systems should be available and have the capability of being merged and manipulated through this data warehousing. The use of attributes and identifiers will need to be closely reviewed to avoid duplication and confusion in attempting to assist in merging this information. Standardized reports should be available for the majority users and automatically available via a relatively user-friendly web site.

- A system should be developed for users who choose to deviate from the available data warehouse options to have the ability to gain access to their data from the backend.
- Identifying what information is considered appropriate will be the first major obstacle. If the information supplied in the data warehouse is inadequate for the majority of users, the need for departmental supplemental systems will not disappear.

Current State

Existing Climate

The University continues to invest resources to maintain and evolve its current mainframe applications. Some of the key enterprise/financial applications have not been upgraded for some time. Their implementation dates range from the Payroll System being implemented in 1973 to the On-Line Purchasing System in 2002.

The majority of these systems are paper based, utilizing manual workflow and resulting in significant duplication of efforts and resources. This attributes to ill-timed data that often leads to poor financial decisions.

In addition to the Financial Data Warehouse (FDW), there are a variety of *supplemental accounting systems* throughout the University. Cook College and the College of Engineering's systems, being two of the largest and both supported by permanent full time IT staff, are also briefly described below.

Financial Data Warehouse:

Currently the most accessible method of acquiring data is the Financial Data Warehouse (FDW). The FDW uses Oracle Discoverer. Although improvements have recently been made to the FDW, the existing reporting tool is not adequately meeting the needs of the current users. Recently the University decided to move forward with the General Ledger (GL) implementation project. Reporting has been viewed as a critical success factor in the GL implementation project, so the FDW must be strategically aligned with this effort. The implementation of the GL module will provide additional reporting capabilities as well as new tools to be evaluated. The vision is to build a comprehensive FDW that allows departments to generate reports and extract data at near time using a user-friendly report-writing tool. As with the current FDW, some standard

queries/reports will be pre-written which will enable users to query and report data without having to create their own reports.

The short-term objectives of the current financial data warehouse include the continuation of the user group to identify new standard reports and modifications to existing reports. An important component of the short-term objective is the ability to generate 'month end' reports. In addition, analysis is currently underway to integrate financial data with procure to pay data to facilitate easier and more accurate reporting.

- Over 300 positions with business titles. Those with administrative titles with business responsibilities >50% is not clear.
- 550 Discoverer users. 275 of those are considered active or current.
- 19 Discoverer reports available.
- 1150 OFIS (read only) users.

YESS - Your Engineering Supplemental System:

The School of Engineering has created an account management system that allows for integrated reporting and management across all types of accounts. Currently, YESS is managed on the account level, and can report from the account to the school levels. The School will soon be releasing a new version of YESS which will allow for sub-accounting along with various other enhancements. Sub-account management and reporting will provide a greater degree of utility towards the management of state and gift funds. The School is also in the process of setting up a pilot program with the Neuroscience Department on Newark Campus. They are still in the initial setup phase so more will be known regarding this as they continue with this process. The School of Engineering shared the following details on the system:

* One central server with Microsoft SQL Server 2000 running on a RAID 10 Disk Array - This server takes care of housing the data and running the queries.

* One secure web server with an ODBC connection to the SQL.

* YESS uses the University's data for all commitments except payroll, fringe, and overhead. Payroll is calculated based on a user's entered amount for a person "to be paid this fiscal year" salary encumbrance (Encumbrance - Paid to date = Remaining Commitment). Fringe and overhead are calculated based on the sum of all commitments.

* Users can enter "projections" for money that will either be expended or budgeted into an account in the future. For instance, Professor X is going to spend around \$5,000 on a new piece of research equipment

sometime this fiscal year , but he will not be entering the PO for some time. The account manager can add an expense projection to ensure that the \$5000 tagged and removed from the available funds.

* YESS is designed around the principles of drilling down and rolling up. For instance, users can begin with summary information for all of their accounts, and simply click their way down through levels of detail until they come to the details of what was on a purchase order.

* Reports that can be generated include: The Extended Budget Responsibility Code Rollup (a summary report based on EBRC); The Account Statements (an object code level report for an account); The Activity Detail Report (a line by line breakdown of the object code activity on an account); The PO Report (a summary of an accounts purchase orders that links the requisition amount to the purchase order amount and the amount paid according to OFIS); The Subtotal Report (a report that shows the compresses the data into user designated subtotals); and The Expense Report (an expense only report that allows the user to specify the date range and level of detail as well as an actual versus ideal burn rate).

FACS - Cook College Supplemental System:

Cook College has set up a supplemental reporting system to enable the college to have real time detail and project accounting for departments. The system was needed due to the mandatory reporting requirements of the Experiment Station to the State of NJ. Additionally it allows for the financial control of all College and Experiment Station financial resources, State and Federal appropriations, grants, contracts, sponsored programs, sundry funds, capital and county funds in real time. Cook College has provided the following details on the system:

- FACS is a FOCUS database system running on the OpenVMS operating system on a HP Alpha/Integrity mainframe.
- Ability to encumber funds in real time for budgetary purposes for all documents regardless of its origin.
- Commitments are entered at the departmental level.
- Actuals are downloaded monthly from the General Ledger. We receive a nightly file from RIAS which contains any payments made through RIAS, which we post for informational purposes until the monthly actuals arrive.
- Provides statistical reports identifying system activity levels throughout the College and Station for management decision-making.
- Provides reports and a reallocation process for Federal, State, Station and departmental projects for any time period desired.
- Account details and balances are accessible at the PI level.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

- Ability to download data in Excel or Word format for further manipulation.
- Ability to report on and review archived fiscal years.
- Provides reports for tracking monies spent on individual vendors.
- Records indirect cost and fringe benefit commitments automatically.

Strengths & Weaknesses of Many Administrative Systems

Strengths:

- The systems have been modified throughout the years and although some of the technology is old, these systems are still working.
- The detail and information is accurate.
- Many of the current reports generated by the system are extremely useful.
- Access via budget responsibility code has worked well for the University's hierarchy.
- Newly developed on-line applications have reduced duplication of effort and supplied timely information (On-line time reports, On-line purchasing, absence reporting, address records forms).

Weaknesses:

- Lack of on-line capabilities.
- Paper processes cause duplication of efforts, errors and ill-timed data.
- Business processes have not been analyzed.
- The current data access method limits us to what can only be done manually through the Discoverer application. While this application is reasonably flexible there are several features missing, none the least of which is the ability to perform automated procedures. With backend data access, we could query the data directly, present it in any form we wish and do it in an automated fashion without any direct user intervention.
- Due to the unavailability of timely data from the financial applications, fiscal management processes are lengthy and labor intensive. This causes poor decision-making and does not allow for planning and forecasting.
- Very little pre and post award integration of data.
- The confusing current account structure does not lend itself to project accounting, generating reports and flexibility for expansion.
- Due to the age and inflexibility of the current system, there is little or no margin for error as it relates to due dates.
- Resources are being spent to create or modify systems in order to accommodate needs or to capture data not readily available in the current system. These databases are spread across departmental "owners" and are not easily integrated.
- There are no procedures in place for departmental requests for electronic access.

Summary of Data Obtained from the Focus Group Questionnaires

The committee sought out information from Business Managers and Administrators with financial responsibilities from major units representing a cross section of the University. The information below is a snapshot of concerns regarding the financial systems. Below please find the results of this survey:

- 85% felt that the University's greatest single IT need is a general ledger system, an HR/Payroll system or a fully integrated administrative system.
- 93% of those questioned felt that the University's greatest administrative need was a general ledger and HR/Payroll system that integrates with the current RIAS system.
- 29% favored a general ledger system and 57% favored an HR and/or Payroll system.
- 88% of those questioned had heard of Discoverer, however, only 44% have used it and all those who have used the system expressed disillusionment with it.
- 82% preferred that the University prioritize the implementation of a University-wide integrated administrative system to a departmental supplemental system.
- 44% are currently spending resources to upgrade or implement a new supplemental system.
- 30% are accessing financial data from the Central Administrative systems through a venue other than Discoverer.
- 64% use Excel or Access for their supplemental systems, but only 33% of those using Excel or Access use Discoverer in conjunction with it.
- The primary reasons for needing a supplemental system were:
 - 13% - University system lacks necessary details
 - 40% - ease of use
 - 07% - eliminates the burden of data entry
 - 40% - more accurate and up-to-date
- 100% of these employees would like the University to find some venue to electronically distribute their monthly detail report.
- 93% agree that faculty and staff computer equipment should be upgraded every two to four years.

Networking, Desktop Computers, E-mail/Calendar (Groupware Product)

E-mail/Calendar (Groupware Product)

Overview: In higher education, centralized network is considered a key strategic resource and a “strategic differentiator”. Consequently, we will continue to maintain, enhance and evolve the network infrastructure as new technologies emerge. We will also strive to anticipate the evolving network technology that will transform the higher education environment.

Critical Success Factors

1. Leadership attitudes.
 - a. The University’s top leaders must consider the network as a highly valued strategic resource.
2. Innovation
 - a. State of the industry infrastructure performance and services.
3. Funding resources
 - a. Appropriate funding is needed to support and maintain University goals.
4. Management
 - a. Software tools
 - i. Vendor or consortium products preferred over homegrown applications.
 - b. Controls
 - i. Maintain controls on access and activities to preserve the overall system and integrity.
 - c. Formal polices and procedures that cover networking issues are comprehensive, consistently enforced.
5. Redundancy and Disaster Recovery
 - a. Implementation of redundancy for all single points of failure wherever practical or possible.
 - b. Continue to develop disaster recovery plans University wide and individually by unit or department.

Strengths and Weaknesses

Strengths

- Most departments have acquired dedicated departmental IT staff to assist them in supporting their needs. In addition, OIT provides fee-based IT support to departments who do not require full time technical staff.
- Most buildings at Rutgers are wired and designed for significant expansion.
- Training, templates for policies, procedures and disaster recovery plans are readily available to departments.

- Much of the network has redundant links. The backbone and routers are managed centrally for well-defined support.
- Security is a positive with regards to centralized control, since standard/comprehensive security features can be applied all across the network. Include centralized firewalls, fire walling at the router level, monitoring, CIRT/IPS group to handle abuse problems.
- Authentication through NetID is the standard for wireless access and each campus has availability in most "common" areas - libraries and campus centers.
- Most administrative staff and faculty members have access to a reliable desktop computer and related devices.
- Certain software is available under University site license agreements at reduced or no charge.
- The current calendar system has the ability for the scheduler to see meeting invitees' availability quickly and easily, thereby cutting down on superfluous communication between schedulers.
- Email accounts are available to all Rutgers faculty, students and staff with access anywhere through a web interface.
- Central spam filtering and virus protection is available on central email servers.

Weaknesses

- The building by building data needed to do long range planning Rutgers' network is not readily available.
- No funding model in place for true ongoing support, maintenance and upgrade of the networking infrastructure.
- Too many departments are without updated/current policies, procedures and disaster recovery plans.
- Platforms not supported with RU site licenses are often too expensive to upgrade.
- Wireless service is sporadic, capacity is not adequate, and therefore cannot be relied upon in some areas of the University.
- Units must provide servers to manage/support users as opposed to a single server/system for a density of buildings.
- Standards are not in place to encourage users to adopt a single office productively software suite, or even operating system, and a basic configuration setting which leads to an increase in IT staff support costs.
- There is a need for more software and network site licenses.

- Domain names in e-mail addresses are not standardized so certain addresses can give the uninitiated user no information or misleading information about the sender.
- NetID's have archaic name restraints that create further lack of standardization.
- The current calendar system is not utilized by enough of the users to take advantage of the efficiencies such a system could provide.

Business Services - Networking

Future State:

Vision

The Rutgers network expansion will continue to progress, increasing in speed and service. Over time, more services will be incorporated over the increasingly capable network to allow us to provide a reliable, available, secure, adaptable, fault-tolerant and high-performance data communication network to faculty, staff and students.

Strategies

- Ensure our network fully supports the high –performance requirements needed for enhanced applications.
- Maintain, implement and enforce formal policies and procedures for networking issues.
- Implement network redundancy for single points of failure.

Current State – Existing Climate:

The RUNet 2000 project has succeeded in bringing a new network to most buildings at the University. The Camden and Newark campuses are almost totally wired and a great deal of progress has been made in providing connectivity to all key buildings in the New Brunswick/Piscataway Area. The core of the network, in particular, is especially robust and is capable of handling a significant amount of expansion.

While there still are a number of buildings that are not connected, the majority of them are either small, remote locations that require a very high marginal cost per additional user or are used for warehousing or farming and therefore do not require a network. In some situations, wireless technology has been employed to reach these users, while in others, standard dialup connections are still used.

Those buildings that have been internally wired are largely RUNet compliant giving them up-to-date voice and data capability and the backbone capacity for further expansion.

Summary of the Network Infrastructure by Building:

**Numbers are based on best information available as of 9/2005*

Survey results on existing climate:

- 15% of those who responded have no departmental IT staff support.
- Only 25% of those who responded have an up to date disaster recovery plan.
- Only 21% of those who responded have up to date internal policies and procedures.
- Server / Network platforms of those who responded:
 - 6% Novell
 - 36% Microsoft
 - 11% Unix/Linux
 - 4% Macintosh
 - 9% Combination of Novell and Unix/Linux
 - 15% Combination of Microsoft and Unix/Linux
 - 15% other than above
 - 4% did not respond

Business Services- Wireless

Future State:

Vision

As newer technologies deliver on the promise of increased coverage with fewer distributed devices, wireless access will eventually expand to cover all areas of the University.

Strategies

The expansion of wireless exists on four fronts: increasing range, capacity, speed and capability.

- Increasing range –Increase the viability and lower the cost of wide area wireless implementation.
- Increasing capacity –Distributed technologies promise to provide both extensibility and load sharing to help alleviate this problem.
- Increasing speed –New standards promise 70-100mb with even higher speeds on the horizon.

Current State – Existing Climate:

Wireless is currently available on all campuses of Rutgers and is being administered by a number of local groups. There are four main types of systems in operation: Bluesocket, LAWN, WEP and MAC Filtering. Attached please find detail descriptions of these types and what is currently available at different locations within Rutgers and other institutions.

There are two current wireless implementations at Rutgers. The first is an authentication based wireless system that is used for roaming wireless access and the second is a more fixed location system that provides network services to otherwise disconnected buildings.

Areas that use authentication based services work well providing network security and basic network access that allows roaming users to read e-mail and browse the web.

While the bandwidth available to these users is limited, it does provide enough access for most common Internet tasks.

Areas using the alternate system have been installed to provide primary network service where is it not otherwise available. Many smaller or remotely located buildings were not included in the wiring for the RUNet2000 project and required some type of connection. Wireless technology provided a quick and cost effective way of getting these buildings uplinked with minimal connectivity. While access speeds are generally limited a 20 MB connection that is shared among building users, the system works well and provides both internet and local server access.

The main problems with both systems are building penetration and interference. While the cost per system for wireless is much lower than wireless networks, their inability to easily propagate a signal through some of the older buildings at the University makes it necessary to install a higher number of access points than would be ideal. This drives up costs because of the additional wiring and hardware that needs to be installed along with the extra support costs associated with the management of the equipment. In

addition, access points that may supplement each other in areas of poor signal propagation may simultaneously interfere with one another in an adjacent area. This requires constant monitoring and modification of access points to provide the most reliable access possible.

Other interference issues exist in small buildings that are in close proximity to non-university buildings. In many smaller buildings that sit adjacent to private housing, cheap access points installed in homes interfere with the units Rutgers has installed. In many cases a small frequency adjustment can help alleviate the problem but, in areas where the signal is particularly strong or multiple wireless sources exist, there is often no solution to the problem.

Survey results on existing climate:

- 81% of those who responded use or maintain wireless in some form or another.

Business Services- Desktop Computers

Future State:

Vision

Rutgers should strive to provide state of the art desktop computing resources for faculty and staff. As systems evolve and work process continues to migrate to computers, the University needs to ensure that every user has access to reliable and able computers. Inadequate desktop resources severely weaken the university's ability conduct business by diminishing productivity and compromising the ability to share and distribute vital information. Creating and encouraging standards for hardware and software will help to mitigate these weaknesses.

Strategies

- Ensure desktop replacement every 5 years and purchase/implement a comparable warranty.
- Ensure software is maintained within its supported lifecycle and stays current with recent patches.
- Implement standardized equipment and software recommendations in order to maintain cost effectiveness.
- The standards must be rigorously maintained to keep up with changes in technology.
- Ensure platforms, connectivity, access, usage, etc. are in compliance with all applicable regulations. This includes but is not limited to, antiviral, firewall software, and spyware removal utilities.
- The University should consider reinstating an annual desktop subsidy program.

Current State – Existing Climate:

The desktop PC is arguably the primary business tool for modern office workers. While almost every desk in every department at Rutgers has a PC on it, the disparity between the “haves” and “have-nots” can be significant. Some departments routinely upgrade their desktop systems, while other departments struggle with antiquated hardware that may be barely adequate. Even though not every user requires state of the art equipment, the lack of consistency throughout the university can cause problems as upgrades are made to university infrastructure and new versions of operating systems, security software, and office productivity software are released.

Survey results on existing climate:

- 43% of student labs are either fully or partially funded by the student computing fee.
- 75% of the labs were either fully or partially supported by departmental staff.
- 55% of the departments took advantage of the computer purchase program (CPP) awarding matching funds to departments to assist them in their equipment purchases.
- 66% of the departments replace their computers within 5 years of purchase. 77% of those are within 1-4 yrs.
- 16% use the OIT Computer Store exclusively, 30% purchase from other vendors and 52% purchase from both external vendors and the OIT Computer Store.
- 45% have never used the Procurement and Contracting Department to assist them in receiving discounts for purchasing equipment in bulk. Only 22% uses Procurement and Contracting regularly for such purchases.

Business Services- E-mail/Calendar

Future State:

Vision

Collaboration systems are one of the most important methods of communication that have arisen out of computer technology. These systems will continue to evolve to provide better service to the user community. This evolution will be marked by the ability to track more detailed information, search it more quickly and efficiently and increase its availability. As individuals become available through an ever-expanding number of mediums, it will be increasingly important to have a mechanism to maintain and manage the identifiers for each connection method as well as manage the communications that are transferred.

Strategies

- The key to providing the expanded capabilities suggested above is centralization.
- Increases in server speed, decreases in disk storage costs and the innovations in web browsers and the Java platform will allow for the central storage and access necessary to make online applications available.
- No application could benefit from widespread connectivity better than a collaboration system.
- Just as e-mail clients moved from the POP protocol to the IMAP protocol, storage of e-mail, contacts and directory information will be moved to central, Internet connected systems that will be accessible through multiple platforms.
- Users will be able to choose any compatible client that supports the requisite collaboration protocols and enjoy access to everything from anywhere.

Current State – Existing Climate - Calendar:

The interface has not reached a point where its Universally accepted so the calendar system is not being used very widely.

As of 7/20/2005, 3988 people have logged into the calendar system through RULink. There are also 320 owned by departments and not dedicated to an individual. This number is misleading because some have logged in and found the calendar to not meet their needs and many do not have a need to regularly update their calendar. The weekly numbers range at about 5-600 users. 1,000 are the University's best guess of active users. The calendar is available to everyone (students, faculty and staff); however, the most likely users are administrators. The total number of faculty and staff at Rutgers exceeds 14,000, however, those in the most likely user pool is only about 1,126 (those employees in the A0, A1, A2 and F1 categories). Based on the above assumptions, it can be deduced that a large portion of our administrators are utilizing the calendar system.

Survey results on existing climate:

- 49% of those who responded use their own calendaring system exclusively; only 15% use it to a great extent.

Current State – Existing Climate – E-mail:

The majority of users at Rutgers do choose to use a central e-mail system either in combination with another e-mail address or as their primary address.

OIT has seven (7) public e-mail systems. There are two (2) on each of the three campuses and RULink. RULink is intended to support departments. As such, it has an administrator interface that lets departments create users and shared mailboxes, maintain mailing lists and aliases, and change quotas. The goal is to give a department

everything that would have with their own system, with as much local control. The largest users are Office of Instructional Technology (OIT-ESS), Facilities, and University Relations. It is most attractive for departments that also want calendaring, since the RULink Outlook support works best if you use both mail and calendar.

OIT also runs a private system for Old Queens, and departmental systems for departments that contract their support to OIT.

RULink has 359 users who actually get mail on the system. Some people in the departments OIT supports have addresses, but forward somewhere else. In addition, a lot of people use RULink to forward "name@rutgers.edu" to their favorite system. In theory there's 50,000 people who could use that service. But obviously not all do. The highest daily use is 8765 distinct addresses so the estimated users are approximately 10,000.

Official e-mail addresses:

- OIT: 71,110 (53,833 of these users are from student systems; 8432 of these users from Camden or Newark have addresses that are non-distinguishable between student or non-student).
- Rutgers: 3962
 - These users have 195 distinct e-mail servers/systems
 - Distinct other systems with more than 1 users 114
 - Distinct other systems with more than 5 users 75
 - Distinct other systems with more than 10 users 60
 - Distinct other systems with more than 50 users 16

Data is derived from the University's address directory record within Human Resources (HR). These are approximations, since there are systems with more than one alias, and some of the systems with just one user are typos. It's based on official email addresses. There is some percentage of users who use the departmental systems but haven't registered their email addresses with HR.

Survey results on existing climate:

- 79% of those who responded use the central University's e-mail system(s); 64% for the majority of their users.

Networking, Desktop Computers, E-mail

Summary of Network Infrastructure

RuNet Compliant	284
Unknown	377
Legacy network	36
Not Connected	16
Wireless/Other	7

NOTE: Detailed report available upon request. Numbers are estimates based on best information available as of 9/2005

Detailed Report on the Current Status of Wireless Networking

Wireless is currently available on all campuses of Rutgers and is being administered by a number of local groups. There are four main types of systems in operation: Bluesocket, LAWN, WEP and MAC Filtering.

Bluesocket – The Bluesocket model employs a gateway device, which is basically a customized Linux appliance. Wireless clients associate with an access point and the Bluesocket, which asks them to authenticate, intercepts their connection. Once authentication is complete, the unit allows general network access. Users authenticate against the NetID database and further access controls are employed to guard against excessive use, viruses and standard vulnerabilities. These devices are also being used in some areas to protect standard wired drops.

LAWN (Local Area Wireless Network)– The LAWN network was developed by the Department of Computer Science. It works in a similar fashion to the Bluesocket in that it requires authentication before allowing access to the general network. However, this solution is less expensive because it does not require the purchase of the custom Bluesocket hardware. There is also some additional flexibility available because the system was developed at Rutgers.

WEP (Wired Equivalent Privacy) – This system is generally used for all miscellaneous installations and building uplink connections. It relies entirely on the security capabilities of the individual access points to restrict access to the network and encrypt the data stream. No authentication is required by the user must know the WEP key before they can use the network.

MAC Filtering – In order to use this system users must register their wireless card's MAC address with the controlling authority so it can be added to the allowed access list for the system. Once the MAC address has been entered, users authenticate using their NetID.

New Brunswick

System: RUWireless

Security: Bluesocket, WEP

Protocol in use: 802.11b

Website: <http://ruwireless.rutgers.edu>

Statistics: <http://ccf.rutgers.edu/~edenlogs/wireless/users> (active user charts)

<http://ruwireless.rutgers.edu/index.php?page=sitestats> (unique user stats)

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

Average Monthly Authentications: 2498

Buildings with full coverage: ASB, ASB Annex I, ASB Annex II, Art Library, Chang Library, Davidson Hall, Hill Center Math Library, School of Engineering*, Graduate School of Education*, Student Activities Center, Institute of Marine and Coastal Sciences, Labor Education Center, Douglass Library, Federation Hall, Janice H. Levin Building*, Kilmer Library, SMLR

Buildings with partial coverage: Busch Campus Center (All common areas), Library of Science and Medicine (All Except Circulation), SERC (Reading Room), Alexander Library (Reading Rooms, Periodical sections, Info Labs, SCC, Lounge and Conference Room), CAC Student Center (All common areas), Cook Campus Center (All common areas), Douglass College Center (Lounges, Dining Areas, Multi-Purpose Room), Livingston Student Center (All common areas)

- The NB wireless staff is currently developing their own technology to improve the performance. They have begun using VPN devices to allow for more efficient management and utilization of the Bluesocket devices and have designed their own access points.
- The biggest obstacle they cite is the lack of an operating budget. They are currently funded through resources acquired by reallocation of existing resources and the maintenance fees they charge for management of non-OIT networks.
- Currently no access has been specifically setup to work in classrooms.
- RUWireless staff handles bandwidth and virus issues through manual monitoring and adjustment of the network. If they notice a user consuming too much bandwidth, they throttle the connection. If they notice activity that is indicative of a virus, they block access for the machine.
- They will be deploying a Top Talkers system shortly.
- NB staff are not planning on upgrading to 802.11G based units because of problems with the protocol working when 802.11B card are in the vicinity. They are looking at 802.11N.
- Access does not extend into the residence halls.

System: LAWN

Security: LAWN

Protocol in use: 802.11b

Website: <http://please.rutgers.edu/show/wireless>

Stats: <http://login.rutgers.edu:8008/mrtg>

Average Monthly Authentications: 2428

Buildings with partial coverage: Core, Hill Center, Psychology

Funding is provided entirely by the Department of Computer Science and includes maintenance of the system.

Available in Hill Center classrooms: 114, 116, 120 and 254.

- Users from an authorized list of companies and institutions can authenticate using their e-mail address if they do not have a NetID. The system authenticates them by connecting to their remote e-mail server.
- They are currently testing 802.11A and 801.11G but have not deployed any of these units yet.
- System allows roaming between access points and buildings.
- They have had some problems with dropped signals and bandwidth but nothing major.
- They register all of their access points in the OIT online form. They are currently the biggest user in New Brunswick.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

System: FAS Wireless

Security: WEP

Protocol in use: 802.11b

Buildings with wireless uplinks: 102 College,

Buildings with full coverage: 84 College, 88 College, 64 College, 31 Mine, 34 Mine, 172 College, 2 Richardson, Old Biological Sciences, 39 Union, 132 George

- The FAS Wireless system is used to provide network access for buildings that either have no fiber uplink, no internal wiring or both.
- Buildings that are listed as only having a wireless uplink are internally wired.
- No classroom or undergraduate student access is available using this system.
- Funded, installed and maintained entirely by FAS

School of Business

Systems: RUWireless, MAC Filtering

Buildings with partial coverage: Ackerson (Conference and Classrooms), MEC (Conference and Classrooms)

Buildings with full coverage: Engelhard

- Extensive usage in the classrooms. Close to 500 registered users. 50% saturation in the classrooms.
- System is used in the classrooms to bring up PowerPoint presentations, takes notes right in PowerPoint rather than running to the labs to print out presentations before class.
- PowerPoint presentations and other materials accessed through wireless are kept in the Blackboard system.
- All full time MBA students are required to have wireless laptops.
- Biggest complaint is the cost of the Bluesocket boxes.
- They aren't planning on upgrading to the newer wireless protocols because they don't propagate as well. They have implemented 801.11G in some areas where propagation isn't an issue and when funding permits.

System is funded using Reinvest in Rutgers and ELF funds, not ICI.

Newark

Systems: Bluesocket, LAWN

Security: Bluesocket, LAWN

Protocol in use: 802.11b

Website: <http://wireless.newark.rutgers.edu>

Average Monthly Authentications: 15156

Buildings with Partial Coverage: DANA (50% of 1st floor & 2nd Floor), Norman Samuels Plaza (Green Area), Roebeson Student Center (Cafeteria, Bene Lounge, Coffee Shop, Multi-Purpose Room), Stonesby (Cafeteria, Green Area), Engelhard (3rd floor), Center for Law & Justice (Lower Level).

- The law school uses both LAWN and Bluesocket systems
- The remainder of the campus uses Bluesocket
- Funding is handled through ELF and ICI but they have not identified any ongoing funding for support or maintenance.
- They are not charging areas outside of RUCS for support services.
- Proposed installing access points in classrooms connected to a switched outlet so professors could easily bring down the wireless network if they didn't want students using it.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

Camden

System: Bluesocket

Security: Bluesocket

Protocol in use: 801.11b

Website: http://www.camden.rutgers.edu/RUCS-Camden/wireless_students.html

Buildings with Partial Coverage: Campus Center (Dining Areas, Foyer, Starbucks, Computer Lab and Raptor's Roost), Armitage Hall (lobby), Courtyard Lawn.

Buildings with full coverage: Camden Library

- Computing Services and the Law School each funded their own Bluesockets.
- Funding obtained mainly through ELF and ICI
- Staffing is an issue. Current staff has taken on wireless management as an additional duty.
- Heaviest usage is in the Campus Center and the Library.

Miscellaneous Notes

- CAT is planning on putting wireless in some classrooms on Douglass Campus.
- Interference is an issue. People have installed their own access points and, in some cases it has caused problems for centrally administered networks. Suggestions for dealing with this issue include: 1) Having a central authority who can mandate AP configuration and/or removal to prevent interference, 2) Proving blanket coverage so there would be no need for users to setup their own.
- Security is an issue for APs that have been installed by miscellaneous users. At present, anyone can setup an unsecured access point and provide roaming, unsecured, unrestricted access to anyone in the vicinity.
- Some areas have requested the ability to have VLANs span buildings so they could more effectively leverage Bluesockets. At present, they have to purchase a Bluesocket per building even if there are only a small number of users in the building. (This problem may have another technological solution through the use of small VPN devices).
- Professors have mixed reactions to the availability of wireless access. In areas where it is available, most are employing a closed lid policy where they ask students to close laptops when they don't want them to be distracted.
- Overall bandwidth numbers are not available since everyone except for DCS is only tracking login, unique user and unique MAC address statistics.
- Rutgers Housing does not have any standard wireless network in place. They allow students to setup their own if they wish but will not support them. Their only recommendations involve using WEP and MAC address restrictions. Users are responsible for anything that happens on their connection.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

University of Maryland

- Users are required to authenticate once per day in order to use the wireless network.
- Four days notice is required for guest access to the network.
- They have networked a number of major buildings and common lawn areas.
- They recommend that students not setup their own wireless networks but it is not prohibited.
- They have a standardized procedure for requesting that a building be added to the wireless network.
- They are not using any type of encryption preferring to rely on users to use secure services.
- They control access to in classroom technology using keycard locks on the AV cabinets that are installed in the classrooms.
- Wireless is available throughout all 38 classroom buildings and is part of the design standard for all future classrooms.
- No statistics available online

Carnegie-Mellon

- All 32 academic and administrative buildings and key outdoor areas have access. (4 million square feet of interior floor space, 1-2 acres of outside space)
- Currently looking into 802.11a but have not deployed it yet.
- No encryption is used to secure the wireless data stream.
- Currently available in 35 residence halls
- They recommend that students not setup their own wireless networks but it is not prohibited.
- 750 Mb per day bandwidth limit is enforced on all users.
- Average usage of about 3,100 users per day.
- Authentication is handled using AuthBridge for wireless connections QuickReg for wired.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

Departmental Survey for Networks, Desktops and E-mail

Participant Profile:

- Camden
 - School of Business
- New Brunswick
 - Bloustein School of Planning
 - CAIP
 - Camden
 - Sociology, Anthropology & Criminal Justice
 - Career Services
 - Center for Children and Families
 - Center for Urban Policy Research
 - College of Engineering
 - Chemical and Biochemical Engineering
 - Electrical and Computer Engineering
 - Engineering Computing Services
 - Cook College
 - Entomology
 - Environmental Science
 - Environmental Sciences
 - Food Science
 - Landscape Architecture
 - Plant Biology and Pathology
 - Eagleton Institute of Politics
 - Faculty of Arts and Sciences
 - Art History
 - Asian Languages and Cultures
 - Division of Life Sciences
 - Economics
 - English
 - FAS Dean's Office
 - Geography
 - Geological Sciences
 - History
 - Language Institute
 - Livingston Dean's Office
 - Mathematics
 - Philosophy
 - Physics & Astronomy
 - Rutgers College
 - Recreation
 - Sociology
 - Study Abroad
 - Graduate School of Applied and Professional Psychology
 - Graduate School of Education
 - HIV Prevention CPSDI
 - Mason Gross
 - Music
 - Theatre
 - National Institute for Early Education Research
 - School of Business
 - Waksman
 - Waksman Institute
- Newark
 - Center for Research in Regulated Industries (RBS)
 - Chemistry
 - College of Nursing
 - Cornwall Center for Metropolitan Studies
 - Economics
- OIT
 - CIT – Camden
 - NBCS
 - NBCS Netops
 - NBCS Operations
 - OIT – Camden
 - OIT ESS TD

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

- Other Administrative Units
 - Athletics - NB
 - Financial Aid – NB
 - Fraternity and Sorority Affairs - NB
 - NJ SSI Grant – NB
 - Public Safety (Parking, RUPD, Emergency Services)
 - Registrar’s Office
 - Risk Management and Insurance - NB
 - Student Affairs – Camden
 - University Relations
 - Unknown – NB
- **Total** **67**
- **Campus**
 - New Brunswick 56
 - Newark 5
 - Camden 6
 - **Total** **67**
- **Number of tenured or tenure track faculty in unit**
 - 10 or fewer faculty 9
 - 11 to 20 faculty 10
 - 21 to 30 faculty 7
 - Over 31 faculty 16
 - Not applicable 25
 - **Total** **67**
- **Does your unit offer a graduate program**
 - No 34
 - Masters only 3
 - PhD or equivalent 30
 - **Total** **67**
- Does your unit have a dedicated IT staff member?**
 - No 10
 - Yes, part time only 12
 - Yes, one full time 20
 - Yes, two full time 8
 - Yes, three or more full time 17
 - **Total** **67**
- **How many student use workstations does your unit support?**
 - None 11
 - 0-10 16
 - 11-30 11
 - 31-75 16
 - 76-200 9
 - over 201 4
 - **Total** **67**

• **What percentage of time and effort does your IT staff spend in supporting these student use computers?**

○ Not applicable	14	
○ None, supported from OIT or other University resource	3	
○ Up to 25%	29	
○ 26 to 50%	12	
○ 51 to 75%	5	
○ 76 to 100%	4	
○ Total		67

• **Were these labs funded from the student computing fee?**

○ No, self funded	31	
○ Yes, partially funded	18	
○ Yes, fully funded	11	
○ Did not answer	7	
○ Total		67

• **Did your unit take advantage of the University's matching program during its existence, also known as the Computer Purchase Program (CPP)?**

○ No	14	
○ Yes, but not to a large extent	20	
○ Yes, to a large extent	17	
○ Not familiar with this program	15	
○ Did not answer	1	
○ Total		67

Does your unit purchase from the OIT Computer Store?

○ No, we buy direct from vendors	20	
○ Yes, sometimes	35	
○ Yes, always	11	
○ Did not answer	1	
○ Total		67

• **Has your unit worked with Procurement and / or various vendors to purchase equipment in bulk and receive a larger discount than would normally be offered?**

○ No, never	30	
○ Yes, but it's rare for us to do this	21	
○ Yes, we do this regularly	15	
○ Did not answer	1	
○ Total		67

• **Does your unit utilize the University's calendar system, also known as the RULink Calendar?**

- No, we have our own calendaring system
33
- Yes, we make it available to our users, but only a few choose to use it
18
- Yes, we use it to a great extent within our unit only
4
- Yes, we use it to a great extent within our unit, and also use it to collaborate and schedule events with units outside of our area
6
- Did not answer
6
- **Total** **67**

• **Does your unit use wireless networking technology?**

- No, we've never had the need for wireless
9
- Not on location, but various users have wireless in their homes
20
- Yes, in areas of our building where traditional Ethernet is not available
27
- Yes, our building(s) Internet access is supplied largely by wireless technology
7
- Did not answer
4
- **Total** **67**

Does your unit utilize one of the various central University e-mail systems (RCI, CRAB, ANDROMEDA, or RULink)?

- No, we have our own internal departmental e-mail systems
10
- No, our users use publicly available e-mail systems (such as Hotmail, Gmail, or other ISPs)
0
- Yes, a small portion of our users use central University e-mail systems
10
- Yes, a majority of our users use central University e-mail systems
43
- Did not answer
4
- **Total** **67**

• **How often does your unit replace PCs for the office staff and administration?**

- | | | |
|--|----|-----------|
| ○ Every 1-2 years | 3 | |
| ○ Every 3-4 years | 31 | |
| ○ Every 5 years or more | 10 | |
| ○ Determined entirely by availability of funds | 21 | |
| ○ Did not answer | 2 | |
| ○ Total | | 67 |

• **Does your unit have a disaster recovery plan?**

- | | | |
|--|----|-----------|
| ○ No | 15 | |
| ○ Not currently, but we are working on one | 9 | |
| ○ Yes, but it needs updating | 24 | |
| ○ Yes, and it is up to date | 17 | |
| ○ Did not answer | 2 | |
| ○ Total | | 67 |

• **Does your unit have written policies and procedures on your current network / server infrastructure and all of its components?**

- | | | |
|--|----|-----------|
| ○ No | 17 | |
| ○ Not currently, but we are working on one | 13 | |
| ○ Yes, but it needs updating | 19 | |
| ○ Yes, and it is up to date | 14 | |
| ○ Did not answer | 4 | |
| ○ Total | | 67 |

Which best describes the server / network platform your unit has chosen to standardize on?

- | | | |
|---|----|-----------|
| ○ Novell | 4 | |
| ○ Microsoft | 24 | |
| ○ Unix/Linux | 7 | |
| ○ Macintosh | 3 | |
| ○ A combination of Novell and Unix/Linux | 6 | |
| ○ A combination of Microsoft and Unix/Linux | 10 | |
| ○ Other | 10 | |
| ○ Did not answer | 3 | |
| ○ Total | | 67 |

- **Do you access any of your unit's data directly from ESS?**
 - No, we've never tried 35
 - Yes, we get this data in "read only" format 10
 - Yes, we access data and routinely import the data into our local databases 9
 - Yes, we access data through Discoverer only 4
 - Did not answer 9
 - **Total 67**

- **Would you have the staffing and resources available to make good use of data from ESS if your unit was granted greater access?**
 - No 28
 - Yes 28
 - Did not answer 11
 - **Total 67**

Strengths and Weaknesses

Networking:

Strengths

- A large percentage of departments have departmental IT staff to assist them in supporting their needs.
- OIT provides fee-based IT support to departments who do not require full time technical staff.
- Most buildings at Rutgers are wired.
- There is some training available for IT staff managing departmental networks.
- There are multiple templates for departments to use for internal policies, procedures and disaster recovery plans.
- RUNet standards exist and are documented.
- Most buildings are RUNet compliant with high-speed voice and data capabilities.
- The backbone was designed and engineered for significant future expansion.
- Additional redundancy has been added to the system to increase stability.
- Network is monitored 24 hours a day.
- Centralized control of network hardware reduces departmental IT workload.
- Expansion of network according to established standards may limit problems caused by using cheap but unreliable ad-hoc solutions.
- The RUNet 2000 project built out the major infrastructure on all three campuses to provide a more consistent and higher speed access to the majority of buildings at Rutgers.
- Following standards, RUNet has continued to expand and attach buildings and inside wiring as funding is provided.
- The network has been running effectively for users with minimal disruption.
- Speeds have been increased regularly over the past few years.
- Much of the network has redundant links.
- Backbone and routers are managed centrally for well-defined support.
- Security is a positive with regards to centralized control, since standard/comprehensive security features can be applied all across the network. Include centralized firewalls, fire walling at the router level, monitoring, CIRT/IPS group to handle abuse problems.

Weaknesses

- Platforms not supported with RU site licenses are often too expensive to upgrade.
- The building-by-building data needed to do long range planning for Rutgers' network is not readily available.
- Too many departments are without updated/current policies, procedures and disaster recovery plans.
- The RUNet was a significant investment for the University and funding for maintenance and life cycle planning may not be adequate.
- Departments without IT staff may not be positioned to take advantage of network capabilities.
- Centralized control of network hardware occasionally limits flexibility/innovation
- Expansion of network according to established standards is expensive due to the requirement for end nodes to provide funding for use of uplinks.
- Central management of the backbone and routers limits the flexibility and capability of departments to add their own firewall and security services.
- Not supporting Voice over IP (VoIP) presently.
- Quality of Service not supported (video, VoIP, etc.).
- No funding model in place for true ongoing support, maintenance and upgrade of the networking infrastructure.
- VPN can be difficult for home users to use.
- For those departments that attempt to run their own networks, security can sometimes take a back seat.

Wireless:

Strengths

- Departments in remote areas may have Internet access for a relatively low price.
- There is a wireless policy that requires registration of all wireless networks.
- Can be deployed quickly
- Allows mobile users to roam rather than being tied to a wired location.
- Individual departments (and, even students in Housing) may install wireless.
- Devices if they follow the published policy.
- Authentication through NetID is the standard for wireless access.

- Recommended solutions exist that are shared across departments.
- Each campus has availability in most "common" areas - libraries and campus centers.

Weaknesses

- Often the wireless signal is weak and access is therefore limited.
- Competition on campuses with heavily occupied non-RU student residences.
- Wireless policy is self managed and networks may not be reported in a timely manner resulting in interference.
- No central coordination of wireless on the campuses.
- Constantly changing standards makes it difficult to keep up with emerging technology
- Support hardware is either prohibitively expensive or too cheaply made to be reliable.
- No university-wide (or, even campus-wide) plans/solutions are in place.
- Each building must be provided with servers to manage/support authentication as opposed to a single server/system for a density of buildings.
- Support is sporadic.
- Security. Not everyone encrypts and some encryption standards are not the strongest (WEP).
- Most dorms/resnet buildings are not wireless...and many students bring in their own wireless lans; which interfere with others; or others jump on their wireless network and steal their bandwidth, causing the owner to go over bandwidth limits and get suspended for 7 days, etc. Can be a mess.
- Consistency of wireless performance fluctuates, and can be affected by factors such as thickness of walls, external or rogue wireless networks, and other wireless devices (e.g. cordless phones and microwaves).
- Wireless security standards are still evolving (WEP, WPA, etc.) and may not have reached maturity.

Desktop Computers:

Strengths

- Almost every administrative staff and faculty member has access to a desktop computer and resources.
- Training is available (Ed Series, CAT, etc).

- Certain software is available under University site license agreements at reduced or no charge.
- Declining price and increasing speed has decreased the need for mainframe computing cycles
- Expansion of networks has allowed for interconnected desktops to facilitate more effective collaboration.
- Most are connected to RUNet with a high-speed network connection.

Weaknesses

- Desktop PCs in use with obsolete and insecure operating systems that comprise University data.
- Some departments do not have the financial resources or choose not to spend adequately on their desktop PCs making their business staff less efficient and requiring more time and resources of the IT staff.
- Due to a lack of centralized IT funding, departments are forced to pay for their IT expenses out of their general operating budget. For smaller departments, this imposes a considerable hardship.
- Standards are not in place to encourage users to adopt a single office productively software suite, or even operating system and basic configuration settings.
- Decentralization of desktop management, including but not limited to application licensing, causes duplicate efforts (wasted resources) across departments
- There is a need for more software site licenses.
- Lack of hardware standardization increases support costs.
- Since software and hardware upgrades at the university are essentially dependent on every department and/or division individually finding and earmarking funds, standardization is unlikely to occur. Even within departments, purchases are often made on a one-at-a-time basis, frustrating any attempts at creating a more standard and thus manageable support infrastructure. More centralized funding and planning might help – e.g, a program where departments (based on number of faculty, students, and staff) were allocated x dollars every x years, to be used only for upgrading computing equipment and software licenses.
- Failure of users to familiarize themselves with the capabilities of the system leads to underutilization of available resources.

- Power struggles between technology users and IT-staff create conflicts over who should and does have ultimate authority and control over computing resources. Rutgers should adopt a policy (or at least strongly encourage a culture) that leaves control of computing resources in the hands of IT experts. Faculty and non-IT staff should be encouraged (required) to log in without administrative rights so that less time is spent “fixing” machines that are broken, hobbled, or otherwise made unusable by users with elevated privileges installing software, legitimate and otherwise, in ad-hoc fashion. This would provide for a more stable and secure computing environment, and would also free up large amounts of time for IT staff to work on design problems instead of being reactive to emergencies.
- Departments must totally provide for their equipment replacement costs, which may lead to non-standard desktop purchases (subsidizing purchases encouraged standardization as witnessed with the PC Purchase Program).
- Departments don't have a life cycle (or, evergreening) plan to regularly upgrade and cycle down equipment.
- Software is not kept current, which eventually leads to security problems, compatibility issues with new applications, and outdated operating systems.
- Backups often not done. Can lose data due to hardware failure or user accidentally erasing files.

E-mail and Calendar:

Strengths

- Ability for the scheduler to see meeting invitees' availability quickly and easily, thereby cutting down on superfluous communication between schedulers.
- Staff members can maintain their privacy while sharing access to their individual calendars.
- Communication is more efficient with meeting attendees also being reminded by an automated e-mail on all meeting invites and cancellations.
- Meetings can be rescheduled easily.
- High degree of departmental autonomy.
- Departmental identity domain names in the e-mail address name are viewed by some as strength since foo@math.rutgers.edu may be identified as being from a Math Department.
- Creation and maintenance of e-mail accounts in departmental e-mail systems can be completed quickly.
- Web based interface allows for access to calendar from any web connected system.

- Ability to sync calendar with common hand-held devices
- Everyone at Rutgers may use NetID@rutgers.edu for email address on the central server – RULink.
- Email accounts available to all Rutgers faculty, students and staff with access anywhere through a web interface.
- a. name@rutgers.edu is available to everyone via RULink.
- Central spam filtering and virus protection available on central email servers.

E-mail and Calendar:

Weaknesses

- Many faculty / staff are not utilizing the electronic calendar. Some are not even aware of its existence.
- When too many attendees are included, it is often necessary to create more than one entry to include all. Departmental e-mail systems lead to redundancy in equipment, software and personnel. Rutgers now maintains over 100 e-mail servers for approximately 14,300 faculty / staff e-mail accounts. Given that the existing central e-mail systems in Camden, Newark and New Brunswick already serve about 10,000 of these accounts, that leaves approximately 97 systems for 4,300 accounts (43 accounts per server on the average).
- Domain names in e-mail addresses are not standardized and hence addresses with names such as foo@Andromeda.rutgers.edu or foo@aesop.rutgers.edu give the uninitiated user no information or misleading information about the sender.
- Net id's have archaic name restraints (e.g., 8 character limit) that create further lack of standardization. (Most organizations follow a naming convention; Rutgers does not.)
- Less common hand-held devices are not supported
- User interface is not as user-friendly as some other systems.
- Lacks automatic synchronization of PDAs, Outlook and other calendar software with RULink.
- Lacks capability for rooms, staff and equipment calendars to be coordinated efficiently.
- Central mail server can't have campus-based email address, ie, NetID@camden.rutgers.edu or NetID@newark.rutgers.edu or NetID@nbp.rutgers.edu.

- A truly integrated desktop email/calendar system not available centrally. Something like an Exchange server giving faculty/staff the ability to use Microsoft Outlook Email and Calendaring in an integrated desktop fashion.
- Some features of calendar are buggy (users think they have been invited to an event when they have merely been informed).

Electronic Access:

Strengths

- Current HR system can be downloaded at the departmental level (Oracle)
- Financial information is available in Discoverer.
- Some departments were able to obtain direct feeds.
- Ability to work with data that is as close to real-time as possible.
- Electronics distribution increases speed and accuracy while decreasing costs and use of consumables (paper, ink, etc).
- Web interfaces exist for standard applications that permit most users to easily obtain information from anywhere.

Weaknesses

- In current system there is no report writing or downloading capabilities for users outside Discoverer. Discoverer is found to be extremely cumbersome.
- The tables are difficult to follow and have an inability to join certain data.

Electronic Access

Weaknesses

- Departmental Activity codes I and II are not on any of the currently reports through University Accounting.
- You cannot link detail of actuals, budgets, and commitments to run on one report.
- It is very difficult to create summary reports with accurate data, especially in the grant account area.
- When summary reports are created it is difficult/impossible to limit the totals by date. (If an account is setup by project year you cannot get summary info for a fiscal year. If an account is set up by fiscal year you can't get summary info for a portion of that year)
- It takes a very long time (sometimes over 15 minutes) to run certain reports and there is no way to schedule that report to run before or after working hours.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

- If you use the line item detail in the P2P views it will often return multiple lines of the same information.
- The current data access method limits us to what can only be done manually through the Discoverer application. While this application is reasonably flexible there are several features missing, not the least of which is the ability to perform automated procedures. With backend data access, we could query the data directly, present it in any form we wish and do it in an automated fashion without any direct user intervention.
- There is a tremendous amount of money spent at the department level on supplemental systems. There are no uniform platforms being used for shadow system as most units have unique characteristics and require a different set or reporting.
- Inadequate facilities to link to or download data from central systems, resulting in redundant data entry and out-dated reports.
- No procedures for departmental requests that have a need for electronic feeds.
- Query tools are limited both in functionality (Oracle and Discoverer) and in accessibility (Student Data Warehouse).
- Databases are spread across departmental "owners" and are not easily integrated.
- If your application doesn't "fit" the written application, you may easily (or financially) be able to adapt to it (ie, WOLP for credit card transactions).
- One widely deployed supplemental system (CBPS) is DOS-based, does not work well with networks or modern printer (USB) printers, and is not standardized across departments.

Voice and video

Voice

Vision:

- To develop an integrated communication structure with multiple solutions and broad voice services standards for faculty and staff.
- Cost effective voice wireless services (cell phones) should be coordinated across all campuses for vendor selection for authorized university members.

Critical Success Factors

- Define an effective funding model that encourages convergence of telephone systems to a university-wide communication structure. The present linkage of telephone charges (surcharges) to fund other areas at the university through the “central clearing account for telephone” places a burden on campuses (and, central administration) interested in moving to a more current telephone system (PBX - Private Branch Exchange). The funding model must include resources for capital improvements. A PBX is the central hardware and software required to provide telephone services.
- Develop an institutional design for a minimal set of current telephone services that all employees will have from their desk. Such services would be included in the basic cost of telephone billing.
- Encourage the implementation of major PBX systems that can cover large geographic areas to maximize coordination in organizations that are not co-located.
- Educate users on basic functions/departmental functions – training is vital.
- Any campus or departmental projects involving PBX purchases must be coordinated as a University project and integrated effectively and efficiently. To accomplish this, a predefined and approved university list of PBX systems should be presented to be sure there are enough selections to make it attractive for a department.
- Voice over IP (VoIP) support must be either included or available as an option for any PBX solutions to provide for future direction with an eye toward longer term potential cost savings. VoIP is the implementation of telephone service over the Internet where one plugs the phone into a data jack.

Strategies to accomplish Vision

- Assess current strategies and models of funding to determine if they will work efficiently and effectively for the future. Develop a funding model that uses existing voice system to provide capital investment as appropriate/needed. For example, the Camden PBX implementation required an \$800,000 investment cost and was completed within a year. The University could use this as a benchmark for future voice implementation as it relates to both cost and timeframe for each individual Campus.
- Develop broad voice services standard for University faculty and staff including minimal features such as: voice mail, auto attendant, call forwarding, caller ID, call transfer, and speaker phone on either hard or soft keys. Additional features suggested are found in the survey in the Appendix.
- Develop a long term IP Telephony solution (Voice over IP) to be incorporated into the planning for PBX systems that includes considerations for network capacity, Quality of Services, reliability, security, and new applications.
- Test and evaluate the positioning and timing for incorporation of VoIP for the large-scale application at Rutgers.
- Network design and capacity must be included in the planning with integration of data, voice and video as a long term strategy for success.

Current State -Existing Climate

Currently, Rutgers works closely with Verizon to supply Centrex service to all of the campuses. To be clear, a Centrex line is merely a PBX (Private Branch Exchange) that resides in a facility owned by Verizon that delivers services to non-digital phones (or, handsets). All adds, moves and changes are handled through a central campus-based office. However, the final conversion of phone numbers, attachment of new lines and activation of the service requires Verizon's action. The monthly billing is performed through a single department (OIT) in NB where the charges are applied for a basic monthly service and the long distance/other billable phone calls. Verizon offers to Rutgers University a variety of services (voice messaging, call attendant, caller ID and the whole range of telephone services) at an additional monthly charge to a department per phone or service contracted.

Camden has installed a Nortel PBX to service the majority of the voice service in Camden for faculty and staff with a small percentage of independent Centrex lines supporting such activities as modems, off campus offices, student housing, and emergency outside phones. Billing for this service will be defined locally by the Provost Office to cover all costs defined including PBX extensions, PBX maintenance, Verizon links and telephone numbers, and data connectivity.

Many offices/departments have decided to not contract for Centrex services, but rather opted to purchase small key systems (10-60 handsets) or PBXs. Other major PBX systems are found in Center for Law and Justice (Newark), ASB, ASB III, Marine Science, Foran Hall, Graduate School of Educations, Civic Square, Hale Centere, Rutgers Athletic Center. Depending upon the range and quantity of services required these systems cost anywhere from a few thousand dollars to tens of thousands. The benefit identified by these departments is the one time cost to gain access to the suite of services offered only on a per monthly charge from Verizon – voice messaging for all office members and automatic call attendant/routing of incoming calls are two of the most popular options.

The Newark campus is in the middle of an evaluation of a PBX for the campus.

Various departments are testing Voice over IP (VOIP) technology for use within their units.

Strengths and weaknesses

Strengths

- Verizon Centrex provides basic dial tone service to the university.
- Additional services are available through Verizon for monthly service charges.
- No additional staff resources required to manage a PBX.
- Departmental costs for basic telephone service are fixed.
- Centrex provides dependable service even when power is lost.
- 911 service identifies a physical location for individual lines.
- Billing by extension is provided to departments.

Weaknesses

- Additional services are billable on a monthly basis. Centrex pricing is based on 'tariff pricing' that Verizon regulates with the State of NJ. Features for central systems are all priced individually, for example voice mail costs approximately \$10/month where as with most phone systems this is included.
- Departments across multiple buildings have difficulty in managing internal phone service (ie, Intercom).
- Voice Service is an area where central funding has not historically been provided to allow for capital improvements.
- Many small key systems and/or PBXs have a limited number of additional services and may require the creation of additional extensions for connection.
- Telephone bills arrive to the department more than 60 days after a month's end.
- Difficult to get wrong charges corrected either at all or in a timely fashion.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

- Many departments still have phone systems that are 30+ years old.
- There's a lack of understanding of the funding model presently in place for telephone charges. Because of the current voice billing structures at the University, departments may be making poor decisions based on 'what it will cost them and what they will save'. This doesn't mean it is cost effective for the University. Current surcharges on the telephone services help to offset the cost of maintenance and repairs. This service will always need to be funded either at the department level or centrally.

Data Gathering

The committee identified specific data gathering needs for the eight key business services as per table below:

Vision	Data Gathering	Current State
Voice: Broad view of voice services for University	Numbers and types of systems (PBX, etc.)	Phone Numbers – 22,000 Phone Sets – 32,000 PBX Systems – 10 Small key systems - 250 Camden campus PBX – 1,200 handsets
	Project cost of university-wide solution vs. individual solutions	\$17.20/line from Centrex PBX Estimates - \$.8M – Camden \$1.5M - Newark \$2.5M - Busch
	Identify special needs	911 Service?

Survey

A short survey was compiled to identify satisfaction with the present services and ideas for future telephone services provided by Rutgers. Ten (10) faculty and twenty eight (28) staff members responded to the survey providing some insight for reference. All three campuses were represented with four from Newark, six from Camden and twenty eight from New Brunswick.

Overall, the following were identified:

- Those still having access to only Centrex service were unhappy either with the limited basic service or the costs associated with the leasing of additional services such as voicemail and auto attendant.
- Those who have moved to key or PBX systems are generally happy with the improved services provided and the departmental cost reductions obtained.

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

- Features generally identified as in use today included voice mail, auto attendant, caller ID, speaker phone, call forwarding, hold, intercom, and vacation messaging.
- Features suggested for improvements included friendlier speed dial, larger voice mailboxes, music on hold, fax to computer email, voice over IP, and different ring styles.
- Many suggested that the university needs a university-wide telephone system.
- It was commented that some would certainly pool resources to gain the improvements from a more modern telephone system.
- There still seemed to be a good percentage of respondents that state that they (department) did not “own” their phones on their desk, but rather had a shared phone or extension.
- One department recently purchased a PBX for their building and found out after installation and put into production that their new 5-digit extensions are not compatible with the existing university applications for listing telephone numbers/extensions. Presently, the data fields are designed for up to 4 digits.

A copy of the survey and the responses are available for review.

Video

Vision

- To develop a university-wide integrated video structure with multiple solutions and broad video services standards for faculty and staff.
- To develop supported videoconferencing protocols capable to encourage present and future access for distant video communications coordinated under an identified office.

Critical Success Factors

- Identify a university-wide office charged with coordinating videoconferencing equipment, policies, and procedures.
- Network expansion and management to provide the “Quality of Service” required for good quality video.
- Development of a valid funding model capable to meet the expansion from new and/or modified services.
- Procedures and equipment must be clearly defined for a quality, user- friendly video service to be
- used in any department.
- Video on demand capability, analog to digital capability and video streaming (even classroom instruction to CATV) must be easily supported by departmental staff.

Strategies to accomplish Vision

- Centralized clearinghouse to coordinate and communicate all activities related to video distribution and creation at the university.
- Investment of resources to understand the current and future directions of video services in the market.
- Network design and capacity must be included in the planning with integration of data, voice and video as a long term strategy for success:

Current State - Existing Climate

The academic and housing video services are contained elsewhere in the report (Distance Learning, stored video to deliver video on demand for instruction, CATV to most residential rooms on all campuses, and a production studio available in New Brunswick to create material for video distribution)

Departments have individually purchased videoconferencing equipment to provide service mostly for their own departmental meetings across campuses.

Live video streaming of special events, such as, the President’s State of the University Address and special lectures/presentations are occurring and the recordings are stored on streaming servers. This capability is available to departments for a fee in New Brunswick, in a single department in Camden, and not at all in Newark.

RUNet 2000 planning document was used to define basic cable TV services to the residential buildings in New Brunswick. The overall definitions of the network design for IP does not preclude the use of video over IP as this technology is developed.

Strengths and weaknesses

Strengths

- Matching equipment (ie, all Polycom) has been used successfully within departments to hold meetings.

Weaknesses

- No coordination or standards maintained to guarantee a successful link between any two units/manufacturers.
 Very limited support for purchase, installation, and ongoing issues.
 Interconnections between various departments must be constantly tested to provide a successful meeting/program.
- No single point of contact exists today for coordinating videoconferencing at Rutgers.

Data Gathering

The committee identified specific data gathering needs for video services as per table below:

Vision	Data Gathering	Current State
Video Services (meetings, training, executive announcements, etc.): Available to everyone Easy to use Quality of service	Who has? Public or private? Space Costs	240 buildings in NB with CATV Conference rooms Portable units Desktop units Bandwidth issues Academic Video Services: http://videoconference.rutgers.edu/ Available Rooms: http://videoconference.rutgers.edu/videoconferencing.jsp#scheduling

Survey

A short survey was compiled to identify satisfaction with the present services and ideas for future video services provided by Rutgers. Ten (10) faculty and twenty eight (28) staff members responded to the survey providing some insight for reference. All three

campuses were represented with four from Newark, six from Camden and twenty eight from New Brunswick.

Overall, the following were identified:

- Videoconferencing is fragmented across the university with those that “know” where it is available and those that “don’t know if it exists”.
- Academic applications were identified by some as probable implementations.
- Key positive features for video communication was the ability to meet at distance sites (whether between campuses or between universities), the avoidance of the travel.

A copy of the survey and the responses are available for review.

RUNet 2000 Planning documentation:

The RUNet 2000 documentation consistent with the project references video from the perspective of a standard cable television distribution system. This was associated with the desire to provide capability for University Relations and the existing Rutgers television service offering. The existing data network models utilized 10/100Mbit full duplex ports and a 2Mbit aggregated internal bandwidth at academic locations so that internal building infrastructure would not be a hindrance to desktop video, among other things. However, video support was not a formal part of the design. The current RUNet standard has not been a hindrance to video use when the published reference model is adhered to.

TD published information pertaining to video can be found at:
<http://www.td.rutgers.edu/documentation/>

The relevant documents are as follows:

- RUNet Video Reference Checklist
- RUNet Video Reference Model
- H.323 Tutorial

As of Sept. 6, 2005, Estimates:

Classrooms with:

	Number	VCR/etc	dvd	data/pc	internet	RUTV count
NB	242	66.1%	47.5%	35.1%	28.9%	3
C	64	95.0%	95%	21.9%	99.0%	0
Nwk	125	39.0%	39%	39.0%	95.0%	0

Student Services Systems

Overview

Most student systems either send data to and/or extract data from the Student Records Database (SRDB), which is an antiquated application rooted in a mainframe environment. Despite the limitations of the SRDB, the University has developed several web-based applications for students in recent years using Oracle as the database architecture (e.g., registration, grade-reporting, transcript requests, term billing, admissions, financial aid). Additionally, individual units have customized their own systems and/or acquired commercially developed systems designed specifically for their business process (e.g., CS Housing, Financier for Financial Aid). Broadly stated, many services are offered to students online through well-designed web-interfaces, but the backbone system that populates student data into these applications, while functional, is antiquated and limited in terms of future enhancements.

The primary strategic objectives are the integration of the many student systems and the availability of real-time or near real-time data. It is unclear whether an enterprise system, homegrown solution using current development and database technology, or “best-of-breed” model is the best choice to realize these strategic objectives. Both the timing of any implementation as well as structural changes to the University currently being considered might significantly alter the calculus as to the best approach. If enhancements to student systems are likely to be delayed several more years, there is little purpose in doing a full assessment / gap analysis at this time since the capabilities of the current systems continue to evolve and new applications are continually developed. In the past, enterprise solutions have been rejected because the complexity of the University’s organizational structure made such solutions either practically unworkable or would require too much customization to be cost-effective. The question is whether structural change at the University might make for an administrative environment more receptive to an enterprise solution. A second-tier strategic objective is an IT organizational model that effectively supports the technology needs of both small and large student services units.

Future State

Vision

The vision for student systems, generally stated, has the following attributes:

- Student services offices will have the ability to provide exceptional service to students, faculty, staff and other constituents facilitated through their systems.
- Integrated student records systems such that update by office A automatically updates data for same student in systems used by offices B and C.
- Flexibility for individual units to continue to develop in-house enhancements to the backbone systems that are responsive to their specific business needs, but

with the guide of common standards developed jointly by departmental and appropriate OIT technical staff.

- Real-time or near real-time updates.
- Supportive of self-service for faculty, staff and students with services available 24/7
- User-friendly Web interfaces to information and the elimination of paper wherever feasible.
- Systems that easily support tiered access privileges to facilitate improved security environment.

Objectives

- Integration of schedule of classes, registration information, course evaluations (SIRS), online course syllabi noting required texts, online bookstore orders, degree audit, catalog, program/major listings, and comparable information on academic department/collegiate Web pages (e.g., course offerings, degree requirements, major/minor requirements).
- Incorporation of frequently requested student services information to MyRutgers via a real-time Integrated Student Services Screen, including pertinent online help.
- Enhanced electronic communication with prospective and current students (e.g., via email or through portals similar to MyRutgers) that can be easily configured and tracked by appropriate staff.
- Payment at any cashiers office or online would be updated into system quickly or near time allowing student to pay off holds and register immediately.
- The ability of any office contacted by a particular student to add notes of the contact that would update into the systems viewed by other offices so that services can be better coordinated across offices (partly achieved in the new degree audit system currently being deployed).
- To help students better plan their academic progress modify the current systems so that departments can build future class schedules on a multi-semester, multi-year basis.
- The capability of listing together all financial transactions for a period of time defined in search parameters (holds, parking charges, credits from refunds/financial aid crossing, etc.).
- Web-based reporting environment that includes reporting across offices as needed (e.g., admissions and registration data, financial aid and admissions data) for trend and previous year's point-in-time analysis, etc. Interactive (e.g., OLAP)

analysis for key performance indicators could assist in handling many standard reporting needs.

- Enhanced web-based functional and technical documentation to facilitate staff training.

Critical Success Factors

- Prioritizing projects such that feasible ones with the greatest impact on advancing Rutgers University are implemented. ITPGC has documented criteria for determining the priorities of IT projects that could prove useful.
- Teamwork and collaboration across student services offices, academic and collegiate offices, OIT, OIRAP, and other relevant offices on joint initiatives.
- Support from academic community, university leadership and OIT for IT initiatives.
- Thorough business process analysis to determine if a business process needs to be improved prior to implementing a correlated IT initiative.
- Analysis and evaluation using readily available survey/research data, and/or appropriate focus groups representative of the audience for a particular IT initiative.
- Enthusiastic staff with a positive attitude toward improvements.

Current State - Existing Climate

Some of the key student services mainframe applications and their implementation dates are as follows:

Student Services Mainframe Applications	Implementation Year
SAR Statement of Accounts	FY 00/01
Cash Register	Not available
Undergraduate & Graduate Admissions	Pre-1990
Course Scheduling System	1990
Financial Aid	1982
Course Scheduling System	1990
Course Registration	1992

All of the current systems are either homegrown or so extensively modified from the original purchased software that they are modified and maintained presently by OIT. Since 1997 the individual service units have been meeting on a monthly basis to share data and processes. This sharing of information has led to the identification of data and service gaps, which have been remedied one by one through OIT or through the unit computing specialists. It is both time-consuming and cumbersome but has been

successful in minimizing the effect of the disparate systems on timely service to students. Additionally, significant cross-training of support and professional staff has occurred between units in order to present a more unified and streamlined service experience to students and their families.

Strengths & Weaknesses

Strengths:

The University had implemented several web-based applications primarily for student services using Oracle as the database architecture since 1997. Each of these services (listed below) has been developed to provide a seamless and integrated online experience for students.

- Admissions Application
- Enrollment Pathway
- Financial Aid Application
- Class Scheduling
- Course registration
- Term Grade Reporting & Submissions
- Transcript Requests
- Statement of Accounts
- Term Bill Payment
- Financial Aid Awards
- Financial Aid Requests for Documentation
- College-to-College Application
- Loan Promissory Notes
- Loan Counseling (Entrance and Exit)
- Online Student Survey to measure service quality
- Expanded use of student email and listservs to improve delivery of important notices.
- My Rutgers Portal
- AP Credit Evaluation Application
- Prospect System
- Document Imaging

In 1999, a document imaging application (ImageNow) was implemented by Undergraduate Admissions, Financial Aid, and Student Accounting Services. In 2004,

Graduate Admissions also deployed ImageNow. This application has significantly improved the processing and organization of paper credentials in these offices and others that utilize this information, as well as the level of service provided to students.

- The systems work effectively and are customized to the Rutgers environment, business rules, and each department's internal processing needs (e.g., NB first-year student scheduling/sectioning system).
- In-house systems are based on relatively current development (e.g., Microsoft tools) and relational database technology (Oracle), allowing student service units to more easily adapt and integrate systems to meet evolving needs and goals.

Weaknesses:

- Lack of integration between student service systems leads to a delay in knowing the precise status of student at any given time.
- Changes or additions to information in one system does not update other systems without manual intervention or programmed batch updates. This constrains efficiency.
- The absence of real-time data or more frequent updates in student accounts / IMS were identified as factors that constrained housing billing and reconciliation and also parking and transportation (student status determines parking privileges)
- Absence of real-time data in student records (IMS/TSO)
- Implementation for changes to central systems is too slow and often too costly.
- End users cannot generate simple extract reports to verify data.
- Limited ability in certain systems for students to access, review and confirm records.
- Lack of online help for some systems creates the need for additional faculty/staff training and in some cases can lead to inaccurate information being conveyed.
- There are 14 different versions of the RU Connection Card – simplification would be facilitated by integration of student systems that would allow the card system to pick up changes in student status affecting privileges accessed via the card.
- Difficulty billing in continuous education programs that are off-cycle from the traditional semester calendar
- Mapping of data and data reconciliation across systems (e.g., NJAS and SRDB) are probably more challenging than they need to be. Systems are unnecessarily complex in some instances (e.g., different naming conventions and codes used for common elements across systems, such as semester codes used in NJAS and SRDB), making integration more challenging.

Strategies:

The student service units have developed various methodologies to accomplish their business needs and provide effective services. The problems ultimately are ones more related to efficiencies than they are to absence of services.

Some departmental units have reallocated staff lines to IT over time, and are in a better position to develop in-house solutions or deploy best-of-breed solutions with minimal assistance required from OIT than other offices. The student service units have discussed having greater IT collaboration among student services offices and possible reorganization of IT staff in order to realize gains from teamwork, more IT skill specialization, interoffice IT staff backups and scaling solutions as appropriate to benefit all student services offices. Special attention would be given to ensure that individual units would have their current IT service level met or exceeded in any IT staff reorganization considered.

Institutions that have achieved the desired integration of student systems appear to have done so through the acquisition of an ERP solution. This has been explored in the past (Banner). The complexity of the institutional structure (three campuses and multiple colleges/schools with varying business rules across colleges/campuses) made this solution unworkable.

Partial ERP implementation in high impact areas could be explored.

In-house re-engineering and new application development with departmental/OIT-developed standards using current technology (development tools/relational databases) is another option. While possibly requiring the use of contracted IT staff, this could prove significantly less costly than an ERP solution and possibly be easier to maintain in the long run.

Employ "Best-of-Breed" solutions that can be relatively easily integrated with existing systems.

Security Framework

Vision

A successful distributed security model must be based on information and how it flows through the University. This will require for both central computing services and business units to follow the same security framework that is layered and replicated in both environments. This security framework will as a minimum meet the following characteristics:

- Data classes (classifying information according to its level of sensitivity)
- Zones and layers (security boundaries between zones and within zones)
- Zones to zone data transfers (data feed or data query across boundary)
- Data transport within zones (moving information within a department)
- Policies (rule set for transferring data across a boundary)

It is the policy 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. Those systems holding critical information will be categorized as a critical host and its configuration must comply with the highest level of care.

Critical Success Factors

- Adequate balance between access and security/privacy.
- Training and security awareness.
- Effective administration of security practices/standards/guidelines.
- Departmental Policy/Plans as they relate to information technology and security.
- Business Continuity Plans and Data backup/recovery strategies for each unit.
- Increase Information Security & Privacy Assurance: Enhanced security of assets, intellectual data and personal data.
- 100% Regulatory Compliance: Compliance with state regulations, FERPA, HIPAA, GLBA and other.
- Collaboration and continuous communication between OIT and the business units with clearly defined levels of authority.

Strategy

The University places a high level of trust in its members to properly secure university assets that are under their control. It is incumbent upon all faculty, students, contractors, consultants and visitors to be familiar with and comply with these policies. Minimum practices that will be followed include:

- Maintain current patch levels.
- Configure systems carefully to maximize security.
- Use token-based authentication for access to systems with critical data.
- Limit access to services to those who have a business need.
- Segregate or distribute services to different hosts to limit vectors of attack.
- Log all successful and unsuccessful access.
- Utilize a hardware firewall if appropriate (Federal Regulations may require it).
- Use encryption to transmit confidential data and for data storage.
- Use integrity checking tools.
- Properly dispose of data and data storage devices.
- Report suspected or actual system security breaches to management.
- Baseline metrics to be developed and communicated to all units.

Continue to support the distributed security model (draft) as presented by OIT on email dated August 17, 2005. Refer to the Appendix for a copy of the model.

- The responsibility for applying the appropriate level of security will continue to lie with the department management and the unit computing staff.
- Both central computing and the business unit will follow the security framework detailed on this model.

Information protection is a shared responsibility between central services and business units. In order for this model to successfully function the University must:

- Provide adequate resources and skilled staff to support the current distributed computing services and data security models.
- Continue to provide a robust and reliable network infrastructure within the University.
- Local collection of central authentication credentials should be deprecated where practical.

- Continue to develop and refine information security policies that comply with and reinforce federal, state and university regulations. Ensure students, faculty and staff are presented with the information security policy.
- Educate and Train Users:
 - Train end-users on their rights, on how fair-use is defined, and their role in safeguarding the assets.
 - Provide refresher courses and training to users.
 - Provide a mechanism for customers to verify the legitimacy of a Rutgers' host.

Current State

The University computing services environment is highly distributed between OIT and departments. As such, the information protection strategy reflects a shared responsibility between central services and business units. There are a wide variety of systems, databases, and applications connected to RUNet that create, store, and transmit "non-public" and public information. Therefore, information protection at Rutgers University is a shared responsibility between central services and distributed business units. The greater the sensitivity of the information, the greater the impact if exposed, thus the greater the due care in protecting that information.

To determine the level of protection necessary, data was assigned to one of the following categories:

- Confidential: Access to information is on a "need to know" basis only.
- Internal Use Only: Access is restricted to use by employees for Official Business
- Public: Information is suitable for public dissemination.

The arbiters of security on the network are the Data Custodians and are charged with enforcing security controls commensurate with these categories. Data Users are responsible for following appropriate business practices, working within the areas for which they have authorization and reporting and suspected for actual violations of policies.

The following set of security approaches are used by both central and business units, but not on a consistent basis within all units:

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

Security Technology	Central	Departments	Notes
SSL for credit card transactions	Consistent	Not consistent	All credit card transactions should require SSL and use of WOLP
Data backup	Yes	Not consistent	Needs to be a requirement for all departments or units
Network firewall	Yes	Not consistent	Not necessary for all departments. Each department needs to conduct a risk assessment to determine need
Enterprise directory	LDAP pilot	Not consistent	Current LDAP and PDB have data definition/consistency issues. Departments should be able to leverage University directory
VPN	Yes	Not consistent	Departments can leverage the University VPN
Intrusion Detection	Limited	Limited	Not necessary for all depts
Intrusion prevention	No	No	
Encryption	Limited	Not consistent	Should be requirement for all services that are available outside of the department.
Content Monitoring	No	Unk	Considered to be against University Policy
Standards for application and system development	Yes	Unk	
Electronic signature	Limited	Limited	
Tokens	Yes	Limited	Use is application dependent
Anti-spoofing software	Yes	N/A	
Secure Shell	Yes	Not consistent	Telnet and FTP services eliminated from central servers

ITSP Appendix 4: Business and Enterprise Services Subcommittee
Public Draft 1: February 15, 2006

Formal Policies	Central	Departments	Notes
Acceptable Use	Yes	N/A	Departments do not need to recreate a University AUP
Access Control	Yes	Not consistent	NetID/SecureID/Safeword; Ability of departments to leverage NetID limited by skill set or application
Network Security	Yes	Not consistent	
Data Security	Yes	Not consistent	
Physical Security	Yes	Not consistent	
Privacy Policy	Yes	Not consistent	
Remote access policy	Yes	Not consistent	Allowed through VPN and Modems and through the use of remote control software installed on individual workstations.
Anti-virus policy	Yes	Not consistent	Ex VP letter Sept 2003 regarding patching & AV
Desktop/Server admin policy	Yes	Not consistent	EX VP letter
Incident Handling	Yes	Not consistent	

Strengths and Weaknesses

Strengths:

Access:

- Access to the institutions data bases are controlled through permissions granted by the custodians.
- Centralized authentication permits single password for multiple applications.
- Multiple methods of accessing central authentication servers allow use on multiple platforms.
- Availability of VPN gives users secure access to local services from offsite locations.
- Centralized account management simplifies access control with respect to account creation/removal.
- One-time token password cards are available for high security applications.
- Distributed management and control delegated to local business units.

Procedures:

- Central systems that house the institutional data bases follow well-documented security and access procedures.
- Central data systems (mainframe and warehouses) are backed up regularly with a full disaster recovery plan (including an off-site facility) maintained.

Weaknesses:

Access:

- Access to data is sometimes very difficult to obtain from custodians due to limits of the access controls to the data bases.
- Distributed use of central authentication systems provides multiple administrators access to usernames and passwords.
- Distributed use of central authentication system increases the number of possible vulnerable points at which usernames and passwords could be compromised.
- High cost and inconvenience of token cards has limited their acceptance and implementation.
- It is not possible to differentiate between legitimate and illegitimate Rutgers sites that ask for Net IDs for authentication.
- Access to infrastructure through locally managed wireless access points or network drops not centrally restricted.

Procedures:

- Departments maintaining individual data bases of confidential information may or may not have a complete and effective security plan.

Baseline Metrics:

- No institutional requirement for departments to have a disaster recovery plan.
- No institutional plan for Business Resumption.
- No standards presented for the university to follow for minimal security for systems, data and network traffic.

Attachment: Distributed Security Model Draft

<http://rusecure.rutgers.edu/compliance/dsm.htm>

Introduction : The “Standards for University Operations Handbook” states that the University places a high level of trust in you, its faculty and staff, and requires that university assets under your control be protected and properly safeguarded from loss and misuse. This highly distributed operations model applies equally to both business operations and computing operations at the University. Everyone at the University has a role in protecting the confidentiality, integrity and availability of our information and as such, the information protection security model is distributed equally between central operations and business units.

Scope : This policy applies to all University staff, faculty, students, contractors, consultants, and visitors. All users of university information are expected to be familiar with and comply with this policy.

Model Description : The University’s technology environment is highly distributed and complex. There are a wide variety of systems, databases, and applications connected to RUNet that create, store, and transmit “non-public” and public information. Therefore, information protection at Rutgers University is a shared responsibility between central services and distributed business units. The greater the sensitivity of the information, the greater the impact if exposed, thus the greater the due care in protecting that information. (See Information Classification Definition and Critical Host Definition for more detail.)

Implementation: A successful distributed security model must be based on information and how it flows through the University. This will require both central computing services and distributed business units to follow the same security framework that is layered and replicated in both environments. This security framework will as a minimum meet the following characteristics:

- Data classes (classifying information according to its level of sensitivity)
- Zones and layers (security boundaries between zones and within zones)
- Zones to zone data transfers (i.e., FTP feed or data query across a boundary)
- Data transport within zones (moving information within a department)
- Policies (rule set for transferring data across a boundary)

Originator : Office of Information Technology

Policy Effective date : TBD

Attachment: Critical Host Definitions

<http://rusecure.rutgers.edu/compliance/chd.htm>

Introduction: The university has the responsibility to implement and maintain a high standard of security to avoid the disclosure of confidential and restricted information. The increase of incidents of identity theft and the passage of tougher security standards at the state and federal level place a greater responsibility on anyone holding confidential or restricted information. To meet this responsibility, the university calls upon each person who uses or manages access to confidential and restricted information to apply the appropriate levels of due care. (Due care ensures that a minimal level of protection is in place in accordance with the best practice in the industry.)

Scope: This document applies to all University staff, faculty, students, contractors, consultants, and visitors who access RUNet facilities and “non-public” information for the purpose of supporting the University mission. All are expected to be familiar with and comply with the terms of this document.

Definition statement: It is the responsibility of the University community to protect Critical Hosts from compromise. A Critical Host is any server or desktop connected to RUNet that creates, stores, or transmits confidential or restricted information about people or information about another business unit outside its administrative control. A Critical Host, if compromised, could disclose information to unauthorized parties and significantly harm the University. (Refer to Information Classification Policy for more details.)

Implementation: Due to the university’s distributed computing environment, the responsibility for applying the appropriate level of security lies with department management and the unit computing staff. The university has an expectation that all unit computing staff will exhibit “due care” in the administration of computing systems. Due care will be followed for all University hosts regardless of the type of information accessed, but practices will not be limited to :

- Installing and maintaining anti-virus software
- Keeping operating systems current and patched
- Installing host-based firewalls
- Creating user accounts using complex/strong passwords
- Disabling password caching

The following practices will be followed for all critical hosts but are not limited to the following:

- Remove unnecessary services
- Properly configure systems carefully to enhance their security
- Use token-based authentication for system access and encrypt passwords
- Limit access to services to those who have a business need
- Segregate or distribute services to different hosts to limit attack vectors
- Log all successful and unsuccessful access
- Utilize a network-based firewall if appropriate (some Federal Regulations require it)
- Use encryption to transmit confidential data and for data storage
- Use integrity checking tools
- Properly dispose of data and data storage devices

Due care includes the reporting of suspected or actual system security breaches or compromises to management, the data owner, and abuse@rutgers.edu along with immediate action to mitigate the risk of continued exposure of confidential and restricted information.

Attachment: Information Classification and Responsibilities

<http://rusecure.rutgers.edu/compliance/icd.htm>

Introduction: The University is committed to the open sharing of information in pursuit of its core objectives of research, education and outreach. Also, the University recognizes that certain information must be selectively disclosed in order to meet externally mandated compliance requirements and to accomplish our routine business functions.

Scope: This document applies to all University staff, faculty, students, contractors, consultants, and visitors who access RUNet facilities and non-public information for the purpose of supporting the University mission. All are expected to be familiar with and comply with the terms of this document.

Definition statement: 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.

The University's information is defined as any information within its purview, including student record data, personnel data, financial data (budget and payroll), student life data, departmental administrative data, police records and legal files, and all other data that pertains to, or supports the administration of the University. In addition, this document applies to any other information that the University may own but which is governed by laws and regulations to which the University is held accountable. This document covers all information regardless of storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, and CD-ROM) and regardless of form (e.g., text, graphic, video, and voice).

Implementation : Implementation: University information will be assigned one of the following categories:

Confidential Use: This information is usually described as 'non-public information' about people and under the purview of a Data Owner. Examples include student or employee identifiable information (i.e., name, SSN, birth date, home address, etc.), medical records, legal records, student records, police records, and credit card information. The Data Owner grants access to this information to Data User, however Data Users are not allowed to disseminate this information outside their administrative control. Unauthorized release or loss of this information could reasonably be expected to cause legal and/ or financial consequences.

Restricted Use: This is information that business units may decide to share with other units outside their administrative control for the purpose of collaboration. This information is not information that meets the requirements of 'non-pubic' information. Examples include data created by the department, research data, and project data. Loss of this information could cause harm to the University's image or reputation, but would not necessarily violate existing laws or regulations.

Internal Use: This information is available to anyone within Rutgers University community. Access to this information is restricted to use by employees only for the conduct of university business. Examples include student telephone and address lists, budgets, recruitment plans, strategic plans, network diagrams, etc.

Public Use: This information is suitable for public dissemination and is accessible to anyone in the world. Examples include public web pages, course listings, press releases, marketing brochures, etc.

Identity Management

Vision

Provide a cohesive centrally managed identity management architecture that supports the evolution of system processes and services. One user; one identity; one infrastructure.

Identity Management is defined by Free Encyclopedia Wikipedia as *“an integrated system of business processes, policies and technologies that enable organizations to facilitate and control their users’ access to critical online applications and resources while protecting confidential personal information from unauthorized users.”* It is important that this system integrates both technology and business processes.

A cohesive centrally managed identity management system is much needed at Rutgers University and any type of environment where information is a prized and a high-value asset. Additional challenges that we should consider as we explore the identity management model are:

- Increasing number of on-line services and information offered to faculty, staff, students and to the general public.
- The need to balance access with protection of confidential information from unauthorized users
- Advances in technology
- Mobility of users
- The credentials at Rutgers University might be used for access to shared learning resources, research infrastructure, licensed information, etc.

Critical Success Factors

A successful identity management strategy needs to encompass attributes with scope for both private and public use and possess qualities that have mutability, permanence, uniqueness, and pervasiveness. In order for this system to be successfully implemented, we would need:

- A defined business process for managing profiles for the people, system and services provided by the University.
- Integration of technology with business processes and policies
- Consistency of data classification
- Centrally managed infrastructure to authenticate people or servers seeking access to a service as a resource offered to all units

- Operational efficiency and flexibility:
 - Meet business needs for rapid account creation, use and termination.
 - Be flexible enough to address future needs.
 - Ability to manage users in a variety of roles across the University, users outside the University and user access to content, application and services
 - Access to the right information at the right time will improve productivity and decision making
- Increase information security & privacy assurance: Enhanced security of assets, intellectual data and personal data
- 2. Regulatory Compliance: Compliance with state regulations, FERPA, HIPAA, GLBA and other

Strategy

- Establish a University wide identity management system capable of managing and identifying each individual /entity based upon the wide of roles presently utilized at this institution for student, faculty, staff, alumni, retirees, etc. This system must also support the evolution of system processes and services such as:
 - Authentication – This is the act of proving that you are the subject of a particular credential.
 - Authorization – This process determines if authenticated individuals have access to a particular applications, services and/or data.

Current State- Existing Climate

The NetID is a university-wide identification that is used to login to computer applications and services throughout the university. In order to obtain a NetID the user must be validated in one of the following roles:

- Student
- Staff
- Faculty
- Guest

The validation process occurs through an administrative procedure performed by the registrar's office for students or a business unit for staff, faculty, and guest. The student's data is recorded in the Student Records database and the staff, and faculty data are

recorded in the payroll record database system. Selected data from both of these databases are merged into the People Records Database or PDB.

For Guest accounts, the department creates a record directly into the PDB. When the user creates their NetID, the application checks the PDB to validate the user's role.

Strengths and Weaknesses

Strengths

Current system works, but is very complex and requires the merging of different databases.

Weaknesses

- Central identity is not authoritative but is derived from other data set that are not designed or intended to manage identity.
- The data classification is not consistent across databases.
- Current system has developed over time and no longer meets the needs of the university.
- Lost productivity and inefficient administrative processes: Current system requires the involvement of too many groups to work.
- Hampered ability to extend applications to other classes of users such as visiting faculty and external institutions.