Information Technology Systems Security Overview

Information Technology uses a number of accepted and industry standard methodologies to provide system security at The College of New Jersey. In general, the following approaches are used:

- Require passwords for all internal data systems
- Enforce password requirements on all systems
- Require logins for all public-access systems
- Limit user account access
- Educate users on the importance of password security
- Maintain system user population
- Employ firewall technology to restrict access
- System isolation
- Monitor general system function
- Review information availability

A number of internal data systems are employed at The College of New Jersey. Such systems maintain student records, financial information, employee information, user email and other private internal information. These systems are vital to the functions of The College in addition to containing sensitive information. Information Technology recognizes that no system will be 100% secure due to user error and hardware or software deficiencies; however, Information Technology is always at work to better the security of the systems.

Require passwords for all internal data systems
> All internal data systems at The College have at least one level of password access. Some systems require passwords at multiple levels.

Enforce password requirements on all systems
> Systems with sensitive information have internal mechanisms to enforce password requirements. Such requirements include password expiration, prevention of password reuse, and password selection rules.

Require logins for all public-access systems
> Public-access computers at The College of New Jersey require a personal user login and password in order to gain access. This helps to prevent entirely-anonymous access to the campus network. In cases where persons not affiliated with The College require access, departmentally-administered accounts are used to provide access.

Limit user account access
> Where possible, user accounts are provided with only as much security level access as necessary. These restrictions are typically implemented through the application package itself.

Educate users on the importance of password security
> Users are made aware of the importance of password security when they receive their system user accounts. Issues such as password-sharing and password maintenance are discussed.

Maintain system user population
> Information Technology maintains contact with the department of Human Resources to determine when staff have left The College. Departed staff accounts will be secured and/or deleted to prevent their use later. Student accounts are also removed once it is determined that they are no longer registered for classes.

Employ firewall technology to restrict access
> The College uses firewall technology to restrict access to campus systems via the Internet. With this technology certain systems are designated as general access for campus users and affiliates.

All other systems are either prevented from being accessed or are permitted access only after authentication with one of the accessible systems.

System Isolation

Certain systems at The College of New Jersey contain information or handle operations that do not require general user access. These systems are isolated from general use on the network, either by disconnecting them or protecting them via access restriction technologies (firewalls).

Monitor general system function

Information Technology recognizes that even with technology in place to help prevent security breaches, no facility is perfect. With that in mind, system administrators monitor system function in general. Abnormal operations are typically noted and the causes investigated. The administrators are familiar with how the systems should be operating and are capable of noticing parameters out of nominal ranges.

Review information availability

Information Technology is constantly reviewing industry-standard security information. Such information provides alerts for upcoming security threats, information about new security technology, and ideas for new directions to head with the current security schema at the College.