

IT Security Education Program

Revised January 28, 2002

University Computing and Information Services
University of North Carolina at Pembroke
Pembroke, NC 28372

1 - Purpose

This program exists to provide network and system users with a continual education regarding security issues. Security begins with a set of policies and procedures that ensure a reliable environment. To be effective, however, security must become a practice which all users adopt. It need not be so restrictive that it interferes with the normal course of work. But it must be robust enough to eliminate as many dangers as possible and manage those which can be negated.

This program will serve to remind users of basic security principles. These are presented to the user whenever an account is established. However, that is the only time many users see or consider them. Thus, they may develop habits over time that compromise the security of the university's network or systems. Reminding users of these principles will help offset this danger.

This program will also serve to inform users of new information related to security. Few users can stay abreast of the changes in computing and newer related fields. This rate of change has produced a tremendous amount of information that must be summarized and conveyed to the user community. Failure to do so will expose the university to additional risks and will create a false perception of security in these new environments.

Finally, this program will serve to keep security considerations at the forefront of the decision-making process within UCIS. To be successful, this program will require the corporation of a large number of staff with disparate duties. This will increase the amount of security information that flows within the department and will be a catalyst to ensure that a secure, stable network environment is maintained.

2 - Scope

This program covers all aspects of network and system use and includes every user of a UNCP system. This includes academic and administrative services, file, print and web servers, network infrastructure devices, legacy systems and workstations. While some systems do not fall under the purview of UCIS, the information presented by the program will hopefully find its way into the considerations of those responsible parties.

3 - Background

Network and system security has traditionally been an important component of the university's operation. However, additional demands are being placed on network services every day. In this environment, the need to ensure security plays an ever-increasingly role in decision-making and operations. A security breach could lead to loss or theft of data, loss of productive use of staff time or even liability in legal proceedings.

4 - Threats

Comprise of security could result in a variety of situations and might eventually lead to litigation. Each of these presents its own unique problems and potential threats to the university.

Many laws or policies require that certain information be kept confidential. Other laws require that other information be made public, but policy prescribes the means by which this information is furnished. Much of this information flows over UNCP's network and is stored on servers and in tape archives. Interception of this data could be accomplished electronically or by the theft or copying of printed materials. This could result in the dissemination of confidential information unlawfully or in dissemination of information outside of the prescribed means.

Likewise, much confidential information is or will be made available to the appropriate parties electronically. Should a user fail to understand that this information is available, he or she might not give security much consideration. Thus, they might share passwords or other codes or simply allow them to read inadvertently. In either case, this would allow others to masquerade as the user and use university resources. This could result in decreased availability of resources for legitimate users. It could bring about a situation in which an innocent user appears guilty of some incident and system logs attest to that guilt. While this might be a situation in which the user is actually responsible for any damages, it behooves the university to support its users and prevent a situation if at all possible.

Another way in which the university could be affected is through the loss or thief of data stored on a server. Should a password be compromised, intentionally or inadvertently, an unauthorized individual might use it to gain access to a system. Alternatively, should a security flaw exist in an operating system or application, an individual might be able to exploit it to gain access. In this case, they might have access to a great deal of information. This would normally be much greater than the amount that could be gained by interception. The individual could steal this information and use it for illegitimate purposes. Even worst, the theft might never be detected. Instead of stealing, they could use their access to delete information, either in a large or small scale. On a large scale, the information could probably be retrieved and the university would only lose a few hours of productive work by its staff. On a small scale, the loss might never be detected and the information could eventually be completely lost in the backup rotation process.

Many classes and other academic activities have come to rely on technology. In some cases, these classes or projects could not be completed without this technology. In a similar vein, many research projects or other activities which faculty undertake to attain tenure or advance in their profession rely on technology. A security comprise could lead to the resource being unavailable

temporarily or permanently. This could result in a number of undesirable situations. Classes might not be able to be completed, projects may go unfinished, students might receive lower or failing grades and faculty might fail to complete a research assignment. Any of these could lead to litigation.

Finally, an outside party might use a breach of security to gain access to a workstation or server. Once this individual has access to that machine, they could use it as a platform to attack other equipment on our network, or even on other networks. This could lead to further security breaches in the former case or to penetration of resources at other institutions in the latter. This technique has been used for years to attack government and military networks and, in one documented case, resulted in a global investigation and the eventual arrest of an individual in Germany. This is perhaps the most chilling threat faced by the university, as the federal government is considering legislation that require higher education institutions to secure their networks or face stiff legal penalties. Even without this law, the threat of major litigation is still a very real possibility.

While these treats are illustrative of the types faced by the university, this is not intended to be a complete list. Instead, its purpose is to highlight a few risks and hopefully instill the reader with a sense of the extent of the impact that network and system security has on the campus. Indeed, given the nature of computing, it is impossible to list all threats faced by the university.

5 - Administration

Administration of this plan will be the responsibility of the Director of University Computing and Information Services and the User Services area within that office. The cooperation of other staff within UCIS will be essential for the programs success. At times, staff of other departments or individuals from other agencies may be asked to participate.

User Services will be responsible for the scheduling, transcription and communication of routine communications. Other staff may be responsible for authoring urgent messages, but User Services will be responsible for their communication. This group will also keep a log and copies of all communications distributed under the plan.

6 - Periodic Communications

The foundation of this plan will be periodic communications from UCIS to the user community. These will typically be short and cover a variety of topics. They will be used to remind users of password guidelines, of access restrictions, and other general security information. They will not be sent so frequently as to be routinely ignored by the community. They will take the form of email messages and short statements placed in other publications.

Communication Method	Frequency
Mass email	Sent to user listserv(s) monthly.
Written publications	Printed in <i>Braves Bulletin</i> each quarter.
	Printed in <i>This Week</i> every six weeks during the fall and spring semesters.
Web publications	Contains all basic information. Other communications will refer to this site.

7 - Intermittent Communications

As has been noted, the rate of change in computing requires that a great deal of information be distilled and adsorbed by users. Some of this information is critical and must be distributed as quickly as possible. Examples include virus warnings and security issues relating to email attachments. Intermittent communications will be used to spread this information.

Communication Method	Frequency
Mass email	Sent to user listserv(s) as needed.
Written publications	Printed in <i>Braves Bulletin</i> for extremely critical issues.
	Printed in <i>This Week</i> for extremely critical issues.
Web publications	Contains all basic information. Other communications will refer to this site.

8 - Summary

The purpose of the *Security Education Program* is provide ongoing education for all users of UNCP network and system resources. It will serve to counter the effects of complacency and lack of knowledge about security issues. It will also serve to inform users of critical information about new threats and help to focus the attention of UCIS staff on security. As the university has grown more and more dependant on network resources, the need to ensure security has become paramount. Without a secure network environment, the university would simply cease to function.