

Miami University Computing Security Policy (Revised Dec 12, 2007)

Document Outline

- 1.0 Introduction
- 2.0 Network Security
- 3.0 Network/Netware Directory Services (NDS) and Security
- 4.0 UniqueID and Password Security
- 5.0 Security of Computer Applications
- 6.0 Security of Departmental Servers and Applications
- 7.0 Leadership for Security Policy
- Appendix A: Architecture Documents
- Appendix B: Internet Firewalls

1.0 Introduction

1.1 Computer security is generally distinguished from privacy; in addition, security of the infrastructure is generally distinguished from proper use and access control. Miami University policies for proper use, privacy, and access of computer resources, as well as a brief statement about computer security, may be found in the document "Responsible Use of Computing Resources at Miami University". "Responsible Use of Computing at Miami University" is a general document to be read by all consumers of computing resources at Miami University and is published on the university web site.

1.2 This current document titled "Miami University Computing Security Policy" is the basic document on computing security at Miami University. The University acquires, develops, and maintains computers, computer systems and networks. Some of these computing resources such as the central network are managed centrally by IT Services, other resources are managed by the departments, and still other resources (such as departmental servers attached to the central network), are jointly managed by central computing and the departments. This security policy document applies to all University computing resources, whether central or departmental, whether on campus or from remote locations, and to all users of University computing resources, whether affiliated with the University or not.

Responsibility for security of centrally managed computing resources is given in detail in this policy document, security responsibility for other resources is mentioned only in general terms. Examples of centrally managed resources include our central network and administrative systems. Examples of other computing resources include departmental servers. Where security management responsibility is not defined in this document, it is understood that responsibility follows the general lines of management assigned by university administration. For example, security management of most computing resources in the library would be the responsibility of the library, even though there is no explicit mention of this fact in this policy document. To continue the example, the library also uses central computing resources that are in this document, and which are not the responsibility of the library.

2.0 Network Security

2.1 IT Services is responsible for the configuration, management and security of the Miami University Data and Video Network (MUNet) infrastructure. This responsibility includes management of moves, additions, and changes to network topology and for management of the configuration of devices that comprise the network proper. The 'network proper' involves both the physical transport media and the various devices used for routing, switching, transporting network traffic and managing the same.

2.2 IT Services designs a network security architecture that is within industry security norms for the data being secured; that results in maximum network availability and performance consistent with this security policy; and that is cost effective. The network architecture is described in documents listed in Appendix A

and which are available for review by appropriate management including IT Services Security Office and the University Internal Auditor's office.

2.3 The architecture of MUNet employs various switching technologies to reduce the risk of data exposure through 'sniffing'. To accomplish this, IT Services Networking defines the campus-wide network into public and private subnets, consistent with public and private workspace, in a manner that correlates our firewall policy with appropriate workspace. Private work space is defined to a private subnet and public workspace is defined to a public subnet. Administrative offices are defined as private workspace and thus are on private subnets. The result is that our firewall rules generally restrict administrative computing Services to administrative offices in private workspace.

However, since precise definition of private workspace is difficult, since the related firewall rules are not the primary means of securing our administrative servers, and since delivery of network service is of highest importance, ambiguous workspace is defined as private subnet.

2.4 Changes to administrative firewall rules are implemented by IT Services after approval by the Information Security Office in consultation with IT Services Networking regarding the three-way dependence of firewall rules, public/private workspace and public/private subnets. Because of this three-way dependence, IT Services Security Office is consulted by IT Services Networking when it defines public/private workspace. Similarly, IT Services Security Office periodically audits the definition of the campus-wide network for conformity with the intention of firewall policy. Network performance must be balanced with security concerns, when a firewall rule is considered for adoption.

2.5 The internet firewall has significant differences in purpose and scope from the administrative Firewall; hence, changes to its firewall rules, although managed by IT Services Security Office, require a wider investigative process. These procedures are spelled out in the appendices.

2.6 IT Services Security Office promotes communication of changes to either the firewall rules or the definition of the campus-wide network as described above.

2.7 IT Services Networking is responsible for monitoring security issues on the network proper. This monitoring includes keeping the network secure from non-sanctioned modification and the tracing of unauthorized access to servers attached to the network. Networking will act to log activity and provide eavesdropping services under guidelines stated in "Responsible Use of Computing Resources At Miami University" in the section called 'Limits on Security and Privacy'.

2.8 Remote access to network devices is the responsibility of IT Services Networking. IT Services Networking authorizes physical access to network devices. Implementation of physical access to network devices is the responsibility of the Department of Safety, consistent with their other responsibilities and procedures. Even, in physical space that is not totally under control of Networking, Networking judges whether there is a security risk and takes appropriate action.

2.9 It is understood that Networking may make available to outside contractors, consultants, and vendors, secure access to our network. The following guidelines apply to such access: Change the passwords for the electronics to a new value, ensure that snmp community strings are encrypted, all the vendor access, then return the equipment to standard passwords when the vendor is finished.

2.10 Network devices are classified by IT Services Networking according to their importance in the security of the network, with the backbone given the most secure level. This classification is the basis of physical security policy, the basis of periodic audit by IT Services Security Office, and the basis by which Networking distributes device access to its staff. Networking restricts modification to configuration of its most secure devices from student employees.

2.11 Where possible, Networking maintains access to its devices using a username/password scheme implemented on a secure server that logs both access to the devices being configured and the maintenance of the username/password scheme itself.

2.12 Procedures for access to networked devices are reviewed periodically by IT Services Security Office

3.0 Network Directory Services and Security

3.1 Computer network directory service is provided campus-wide to those who wish to receive centrally supported network resources. Network resources include printing, space for personal computer files, file sharing, and access to computer applications. The following policies governing directory service for personal computers apply to current and future technologies, regardless of the vendor, until explicitly revised.

3.2 There is one directory for the entire University and it is managed at its highest level by IT Services. This one directory may be expressed in multiple technologies. IT Services guarantees that local units have local control over their units. At the direction of University administrators, IT Services grants to appointed security managers in various offices outside of IT Services, the management of branches to the directory. Stated another way, University administrators appoint security managers over branches of the directory, and the branches so managed are limited to the domain of that administrator. IT Services has primary responsibility for assuring that the directory branches match administrative domains; and to this end IT Services regularly produces a directory report and publishes the results to administrators and their designated security managers.

3.3 Stewards over branches of the directory will grant to clients, various requested services such as printer and file access that exist in that branch of the directory. The basis of these grants may vary from administrative unit to administrative unit, according to the policy of that unit.

The following example illustrates the above policy: The dean of CAS has hired a network administrator to be steward of the CAS branch of campus-wide directory. IT Services grants the CAS network administrator the ability to give to clients access to the CAS branch of the directory. A client who wishes to view files or print to printers that exist in containers on the CAS branch of the directory would contact the CAS network administrator. The CAS network administrator could not grant access to files or printers on the SBA branch of the directory.

3.4 Although it is technically possible for a University department or office to set up network directory services outside of the one University directory, there is significant loss of network services if one were to do so. Specifically, logins defined to an independent directory could not use the University UniqueID/password, would not have access to dialup modems, would not have access to central management of printing services, and would not have certain library services. Therefore, independent directories are not advised.

4.0 UniqueID and Password Security

4.1 User accounts for central computing Services are generated by an automated account generation process that is designed and managed by IT Services.

4.2 It is policy to reduce the number of UniqueID-password combinations that any individual needs to remember. This policy is intended to eliminate a primary cause of password compromise, which is the practice of writing passwords in a conspicuous place and thus risking discovery.

It follows that the default password scheme for any application is the existing uniform UniqueID-password scheme embodied in our uniform password database.

4.3 However, because the compromise of a unified password will compromise the security of all applications used by it, there may be applications that should not employ the unified password scheme. Also, because individuals may synchronize passwords of disparate accounts that have the same username, and therefore compromise the application; it follows that some applications will not participate in the use of UniqueID. System management accounts generally should not follow the uniform UniqueID-password

scheme.

4.4 All new applications which could compromise our directory services must undergo a security review to assure that the application is appropriately secured, and to assure that the integrity of existing computer systems is not compromised by the integration of a new application into the uniform password scheme or use of UniqueID. This review must trace the path of username/password pair from the client to the password database and document that it takes a secure path. The path may be made secure either through isolation or reliable encryption.

4.5 Accountability for use of computer resources contributes significantly to proper use. Therefore, each computer account should have one person identified as the responsible person or owner, and computerized records relating the computer account to the responsible person shall be kept. Only when there is no reasonable alternative should computer accounts be shared by more than one person, and even then, one person shall be designated as the owner of the account and shall be responsible for its proper use. When shared accounts must be set up, care should be taken to restrict the privileges of the account to those required for its function. It is recognized that there may be appropriate needs for shared accounts, especially in instructional settings.

4.6 Passwords. All users of University Information Services including but not limited faculty, staff, students, must select good passwords and may not share them with others. A good password has the right number and mix of letters, numbers and special characters to avoid being guessed or cracked in an unreasonably short time. The University Information Security Office shall set standards and guidelines for good passwords that are within industry best practice and based on the sensitivity of the information being protected. Password standards and guidelines must be published and reviewed annually for their effectiveness as technology changes.

Passwords should be changed periodically to enhance computer security; however, if password changes are required for those who use the computer system only occasionally, or if passwords are difficult to remember, the user will be tempted to put the password in writing and risk exposure of the password. Therefore, expiration of passwords and prohibition of prior passwords based on history, should be implemented selectively, based on sensitivity of the data being protected.

4.7 Requests for password change must be accompanied by proper identification and a log of changes must be kept. Presentation of the Miami University photo identification in person is the proper way by which password changes requests are made. Alternately, one may print the 'Request for Password Change' form from the web, have it notarized and mailed to the address on the form. IT Services Security Office may authorize specific password resets based on alternate identification.

5.0 Security of Computer Applications

5.1 The University has a variety of administrative databases and software applications, such as the Banner 2000 System, the University Data Warehouse, and legacy systems, and servers on which they run. In addition, these administrative applications have integrated supporting systems such as job scheduling, report distribution, printing Services, source code management, and web service.

5.2 Access (authorization) to use these administrative systems is managed by the departments that have controlling interest in them according to the principles described in "Responsible Use of Computing Resources At Miami University" and documents that derive from it. For example, the University Registrar has a controlling interest in the registration of students and thus grants access to the computing systems that register students.

In many cases, a computer screen may be distributed to the office with controlling interest, so that that office may grant access directly and immediately. In other cases the office with controlling interest may need to grant access indirectly by communicating its wishes to a third party, who then implements the access. But, in either case, access is granted by the office that has the controlling interest.

Authorization, the granting of access, differs from management of the security structures that deliver access.

5.3 IT Services manages the security structures that deliver access to administrative databases and software applications. Management of these security structures includes design, configuration and implementation. Security structures guarantee that only those who are authorized to use an application may do so. For administrative systems, IT Services manages security structures, but authorization is granted by the office that has controlling interest.

5.4 When a new computing system is acquired, IT Services takes leadership in resolving how the application and hence its security is managed, whether centrally or departmentally.

5.5 The University has a variety of servers and applications whose purpose is for instruction. Some of these servers, such as UNIXGEN, are managed by IT Services. The security structures for these servers are designed, configured and managed by IT Services.

5.6 Access (authorization) to use these academic systems is managed by the departments that have controlling interest in them according to the principles described in “Responsible Use of Computing Resources At Miami University”.

6.0 Security of Departmental Servers and Applications

6.1 Departments have servers, which may or may not be connected to the central campus network, and which support departmental applications. It is the responsibility of the departments to appoint managers of both the system software and the applications that run on these servers. These managers will design, manage, and implement both security structures and authorization structures that are consistent with this policy document and with “Responsible Use of Computing Resources At Miami University.”

6.2 When these hosts or applications in 6.1 interact with central security resources, departments still have responsibility to secure these hosts, but they must follow security procedures specified by central computing. For example, the library maintains servers that it is responsible to secure, but because these servers are connected to the central network and/or make use of the LDAP servers, then the Library must follow security procedures specified by central computing.

6.3 Departments may also have resources and applications such as file systems whose servers are managed by central computing. The departments grant authorization to these resources and applications. Where possible, means should be created that distribute to the offices and departments the ability to grant authorizations directly. In some cases, however, it may be necessary for central computing to implement an authorization, even though it is the department that grants access to departmental resource. For example, the comptroller's office determines who may enter accounting transactions in its administrative computer applications, although central computing implements the request, as well as manages the installation, upgrades, data stores and other technical aspects of those applications, and secures the means of authorization.

6.4 Those who manage the technical aspects of a computer system (such as the installation, upgrades, and data stores) must guarantee that distribution of security authorization mechanisms are secured per this document.

6.5 Departments are encouraged to appoint technical representatives to facilitate proper communication between departmental and central computing about security.

6.6 Currently, the central computing includes management of the following resources:

- the campus-wide network
- the Administrative System firewall
- the University intranet and the internet firewall
- the campus-wide network file system

7.0 Leadership for Security Policy

7.1 Leadership for security policy within IT Services resides in the Security Office; assistance is provided by the 'Committee On Security Policies, Procedures, Responsible Use' composed of a working group and a review group, appointed by IT Services management.

Appendix A: IT SERVICES Architecture Documents

1. "Miami University Network Topology" diagram maintained by IT Services Networking
2. Description of Network Security Architecture – Maintined by IT Services Networking
Administrative System Firewall Rules (document extracted periodically from firewall software), plus list of subnets which are allowed to pass through the firewall.
3. Campus Firewall Rules, document extracted periodically from the firewall software.
4. Classification of Computer Systems by Password Database

Policy History

The original version of this document was approved 6/2000 by the University Counsel and President's Office in conjunction with "Responsible Use of Computing Resources at Miami University".
Revisions were approved 12/19/01 by Working Committee on Security Issues and Responsible Use. On 1/17/2002 the document was endorsed by the Committee on Computing and Information Services.
8/16/2003 Appendix B changes Endorsed by Committee on Computing and Information Services
6/01/2005 draft of Appendix B revisions, draft of major revisions to network section begun.
6/05/2005 Minor revision to change MCIS to IT Services and add Security Office.
1/05/2007 Reviewed, network section will need revision for upcoming network redesign.
12/12/2007 Minor revision to 1.1, 2.4, 3.1-3.4, 4.4, Appendix A, Appendix B, revision to 4.6