# University Information Security Requirements

Effective Period: 1 August 2005 to 31 July 2008 pending review
Version 0.2f

Richard N. Knowles
University Information Security Officer

Revision History

| | Person | Change Description |
|---|---|---|
| 040919 | Richard Knowles | Initial Draft |
| 041015 | Richard Knowles | Continued work |
| 041105 | Richard Knowles | Continued work and adding requirements |
| 050831 | Richard Knowles | Added requirements for Windows Update Servers and for use of a third system for vendor access behind the firewall |
| 060502 | Richard Knowles | Cleaning up some references, updated some entries and added item on physical security |
| 060505 | William Custer | Revised data valuation categories |
| 060603<br>070118<br>070930<br>071207 | William Custer<br>William Custer<br>William Custer<br>William Custer | Add References to ISO 17799<br>Extend effective period per RK<br>Extend effective period 3 month pending review<br>UISR-A001 UniqueID<br>UISR-D001 Application security review<br>UISR G002 Data passing<br>Appendix - Move Student-ID to Confidential |

Contributors:

Stephen Bradley Miami University Information Security Office
William Custer Miami University Information Security Office
Connie Johnson Miami University Information Security Office

## Table of Contents

## 1. Introduction

This document defines the key aspects of Miami University's Information Security Requirements (UISRs). These requirements are provided to define a security baseline as well as to provide guidance to assist in decision-making as it relates to the protection of University Information Systems and associated controls.

### *A. Assumptions*

There is a need to maintain privacy and integrity of the data and systems existing within Miami University, thereby sheltering Miami from potential monetary loss due to disruption or legal liabilities. All controls described here are "due care" measures and represent the best practices within the information security profession.

### *B. Scope*

UISRs are applicable to all Miami University Information Systems, controls and supporting infrastructure, principally within IT Services however baseline controls can be considered 'best practices' and as such are applicable University-wide.

### *C. Effective Period*

This document is considered a living document and will be updated and expanded as needs require. The effective period for this document is defined on the cover page. The Miami University Information Security Requirements shall be reviewed annually to ensure continued relevance by the University Information Security Office.

### *D. Constraints*

At times the University may choose to waive requirements for operational reasons. Should this be done, an exception shall be granted by the Information Security Office for a defined period of time, at the end of which the requirement will again be in force.

### *E. Responsibilities*

The University Information Security Requirements are defined by Miami University's Office of Information Security which acts as the documents office of principal responsibility.

Compliance with these requirements is mandatory unless otherwise indicated in the individual requirement. Certain requirements may be waived by written consent from the University Information Security office.

### *F. Governing Regulations and Policies*

Many of the security requirements defined below are constraints resulting from federal, state and local legislation. The following is a brief (but not inclusive) list:

- Gramm-Leach-Bliley (GLBA)
- Family Educational Rights and Privacy Act FERPA
- Health Insurance Privacy and Accountability. Act HIPAA

## 2. University Information Security Requirements

### *A. Baseline Requirements*

Baseline requirements are those controls that can be considered "reasonable and expected" and are necessary to provide a minimum-level security for the system, issue or application.

| UISR# | Acronym | Description |
|---|---|---|
| UISR-A001 | Unique User IDs | All Users of Miami University information services except those accessing Unrestricted Data shall be provided with and shall use a unique user ID.<br>**Rationale**: Unique ID usage ensures accountability. ISO 17799 11.2.1; 11.5.2 |
| UISR-A002 | Shared User IDs | The use of shared User ID's is not permitted except in those cases where it is unavoidable due to specific application design constraints.<br>**Rationale**: Non-unique ID usage does not permit direct accountability. ISO 17799 11.2.1a |
| UISR-A003 | Default User IDs | All User IDs provided with systems and applications initially from vendors shall be changed from their defaults<br>**Rationale**: Removing or blocking default accounts prevents unauthorized channels of access. ISO 17799 11.2.3h |
| UISR-A004 | User Authentication | All Users of Miami University information services shall be required to authenticate prior to gaining access to any information system or resource<br>**Rationale**: Security Policy and industry practices. ISO 17799 11.2.1; 11.5.1 |
| UISR-A005 | Password Control | All Users of Miami University information services shall authenticate with a properly structured password which shall be changed periodically as defined in University information security policy.<br>**Rationale**: Security Policy and industry practices. ISO 17799 11.3.1 |
| UISR-A006 | Security Awareness Training | All personnel accessing Miami University information services shall have received Security Awareness Training within the last calendar year.<br>**Rationale**: Periodic training is needed to ensure employee secure practices. ISO 17799 8.2.2 |

### *B. Workstations*

Workstation requirements are those requirements which constrain the deployment, management and use of workstations within Miami University.

| UISR # | Acronym | Description |
|---|---|---|
| **UISR-B001** | Workstation Anti-Virus | All workstations shall be equipped with anti-virus software<br>**Rationale**: Anti-viral software protects against entry by Trojan horses or viruses. ISO 17799 10.4 |
| UISR-B002 | Automated Anti-virus Update | All workstation anti-virus software will be updated automatically<br>**Rationale**: Automated update ensures against lapses in coverage. ISO 17799 10.4.1 |

| | | |
|---|---|---|
| UISR-B003 | Workstation Backup | All workstations shall have the capability of having their data backed up. Users shall take advantage of this capability to the extent they are able.<br>**Rationale**: Data Backup is a best practice. ISO 17799 10.5 |
| UISR-B004 | Hardened Default Workstation | All workstations shall have had their operating systems pre-configured to remove vulnerable services and applications<br>**Rationale**: Hardened workstations are more resistant to external attack. |
| UISR-B005 | Automated patch application | If possible, workstation users shall perform periodic updates through vendor-provided patching mechanisms. (Such as the Windows Update system)<br>**Rationale**: Many system vulnerabilities are exploited shortly after their discovery. Periodic updates reduce the risk from this. |

### *C. Servers*

Server requirements are constraints imposed upon the deployment, management and use of workstations within the University technical environment. These include both those servers which are protected by firewalls, but also those that are exposed to the Internet.

| UISR # | Acronym | Description |
|---|---|---|
| UISR-C001 | Enterprise Hardened Server | All trusted enterprise servers shall be hardened using the agreed-upon hardening procedure<br>**Rationale**: To qualify as a trusted server, all potential vulnerabilities shall be reasonably mitigated. |
| UISR-C002 | Server Anti-virus | All enterprise servers shall be equipped with appropriate levels of anti-virus protection<br>**Rationale**: Anti-viral software protects against entry by Trojan horses or viruses. ISO 17799 10.4 |
| UISR-C003 | Server Backup | All enterprise servers shall have a means by which their critical data can be backed up.<br>**Rationale**: For purposes of good stewardship, any time critical and changing data shall be backed up. ISO 17799 10.5 |
| UISR-C004 | Blocking unused ports and services | All enterprise servers shall have unused network application ports and system services disabled<br>**Rationale**: Unused applications or networking ports represent a vulnerable path of entry into the server. ISO 17799 11.4.1; 11.4.4 |
| UISR-C005 | Data Valuation Limits | All enterprise servers which will be containing confidential or restricted data shall be located within the confines of the administrative firewall<br>**Rationale**: For legal reasons, specific sensitive data necessitates a higher level of control. (See FERPA, GLBA). ISO 17799 11.4.1; 11.4.5; 11.6.2 |
| UISR-C006 | Privileged Accounts | System users accessing privileged accounts (Administrator or root) will be the minimum to adequately support the server.<br>**Rationale**: Excessive levels of access or sharing of privileged passwords can compromise security. ISO 17799 11.2.2 |
| UISR-C007 | Physical Server Protection | All enterprise servers which will be containing confidential or restricted data shall be located within a |

| | | |
|---|---|---|
| | | secured area.<br>**Rationale**: For legal reasons, specific sensitive data necessitates a higher level of control. (See FERPA, GLBA) ISO 17799 9.2.1; 9.2.3 |
| UISR-C008 | Vendor access to servers behind firewalls | Enterprise servers placed behind firewalls cannot be opened up for vendor maintenance. Instead a dedicated intermediate system shall be used which will permit the direct assignment of access as well as to allow logging of the vendors actions while accomplishing the work.<br>**Rationale**: Specially protected servers are protected for a reason. Permitting unrestricted access by a third party thwarts the necessary controls. ISO 17799 6.2 |
| UISR-C009 | Protected server access to windows update services | Windows-based servers require connection to a wide range of Internet IP addresses in order to properly accomplish their periodic software updates via TCP port 80. If permitted, this opens those servers up to potential threats accompanying the use of that port. Firewall protected servers will not be permitted unlimited port 80 access through the firewall. As a result, an alternative method should be utilized which places a secondary server outside the firewall to act as a proxy server and pass-through for update traffic. The Firewall shall be configured to permit connection with this server only. In this manner there will be only a single IP address permitted access. The intermediary server shall be hardened appropriately to ensure it will remain uncompromised.<br>**Rationale:** Positive control of all accesses into protected areas. |

### *D. Applications*

Application requirements define those attributes imposed upon applications, both internally and externally developed that work to protect and control Miami University users and that user's data objects.

| UISR # | Acronym | Description |
|---|---|---|
| UISR-D001 | Application Level Security Review | All applications classified as a High Risk Applications by the ISO or any LDAP Authentication Enabled Application shall have had a documented security review<br>**Rationale**: The University Information Security office is responsible for ensuring IT applications conform to best security practices. ISO 17799 12.0 |
| UISR-D002 | Application Level default account access review | All implementations of third party applications will be reviewed for default accounts which will be disabled if unused<br>**Rationale:** Many applications are distributed with default accounts and passwords in place which could be employed as a route for unauthorized access. ISO 17799 11.2.3h |

### *E. Data Management*

Data management requirements define both the stratification of data elements, but also the controls and protective measures employed to ensure its protection.

| UISR # | Acronym | Description |
|---|---|---|

| | | |
|---|---|---|
| UISR-E001 | Data Valuation | All Users of Miami University information services data shall comply with the restrictions defined in the Data Valuation guidelines contained in Appendix B of this document<br>**Rationale:** Care must be taken to not permit restricted and protected data to be disclosed. ISO 17799 7.2 |
| UISR-E002 | Data-application Security Review | All data-handling applications shall have had a documented security review.<br>**Rationale:** The University Information Security office is responsible for ensuring IT applications conform to best security practices. ISO 17799 12.0 |

### *F. Networking And Network Management*

| UISR # | Acronym | Description |
|---|---|---|
| UISR-F001 | Encrypted Privileged Password Handling | All networking and network management passwords shall be protected by encryption on the wire<br>**Rationale:** Passwords sent "in the clear" are susceptible to sniffing. ISO 17799 11.5.1i |
| UISR-F002 | Encryption Level | All encrypted communications shall utilize no less than 128 bit encryption key protection<br>**Rationale:** The longer the encryption key, the more difficult it is for an attacker to apply brute force attack techniques. ISO 17799 12.3 |
| UISR-F003 | Wiring closet access | All wiring closets shall be secured and their access controlled through the CNOC.<br>**Rationale**: Industry practices. ISO 17799 9.2.1;9.2.3 |

### *G. Web-Based Applications*

| | | |
|---|---|---|
| UISR-G001 | No URL Password Passing | All web based applications shall not permit user authentication information to be passed in the clear through the URL<br>**Rationale:** Unless care is taken with web application design, user authentication information could be passed in the clear through URL calls. ISO 17799 10.8.4; 10.9.2 |
| UISR-G002 | URL Parameter Passing | Care must be used when passing parameters as arguments to a URL. User data must not be accessible as a result of deliberate malformed URL's or reconstructed URLs, unless the data is classified as Unrestricted Data.<br>**Rationale:** Use of parameter passing in URL's could permit a third party to spoof a system to revealing protected information. ISO 17799 10.9.2 |

### *H. Physical Security*

| | | |
|---|---|---|
| UISR-H001 | Protected Areas | All areas in which activities occur that access protected information shall have access control in effect.<br>**Rationale:** Unauthorized access to protected information could occur unless areas in which this work takes place are properly protected. ISO 17799 9.1.2 |

## 3. Appendices

### *Glossary*

**Authentication**: The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

**Availability**: To ensure that the information remains accessible to authorized users.

**Baseline Requirement**: A baseline requirement is a requirement that represents a minimum security requirement from a body of minimum requirements. Baseline requirements are directed at maintaining a minimum level of security.

**Baseline Control**: A baseline control is a minimum security control.

**Confidentiality**: To ensuring that only authorized people have access to information.

**FERPA** – Federal Educational Rights and Privacy Act - http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

**GLBA** – Gramm-Leich-Bliley Act

**Hardened Server**: A hardened server is a server upon which system management actions are performed to close potentially vulnerable openings in it's configuration.

**High Risk Application:** A High Risk Application is one that handles Sensitive-Confidential data in sufficient quantity that if the data is exposed it would cause significant harm to the university either financially or in loss of reputation. Any LDAP Authentication Enabled Application is considered high risk because compromise of it could compromise other such applications. High Risk Applications should undergo a security review by the ISO.

**HIPAA**: Health Insurance Privacy and Accountability. Act - http://www.cms.hhs.gov/hipaa/

**Identification:** Any mechanism to determine the actual identity of an individual. This could be accomplished by direct verification or via automated means.

**Integrity**: To ensure that information has not had unauthorized modifications.

**LDAP Authentication Enabled Application:** An application that calls one of the University LDAP authentication databases for authentication

**Password**: A secret word or phrase that is used to identify a valid user.

**PCI**: Payment Card Industry consortium.

**Restricted Data:** See Data Valuation below

**Sensitive-Confidential Data:** See Data Valuation below

**Server(s):** Computer systems engaged in providing data or services across the network.

**Unrestricted Data:** See Data Valuation below

**User(s)**: Users are identified as all individuals who make use of Miami University information resources

## *Data Valuation*

From "Policy on Data Sensitivity and Stewardship of Electronic Information"
To properly protect data that belongs to Miami University, the following definitions are proposed to act as a basic guide in making determinations.

| Type | Definition |
|---|---|
| **Not Classified** | All information not otherwise identified |
| **Unrestricted Data/ Eligible for public release** | Available to the general public without restriction.<br>Available to employees for normal operational use.<br>+ Public bulletins such as course catalog<br>+ General financial reports<br>+Student directory information (non opt-out)<br>+ Unique ID<br>Non-confidential personnel data |
| **Internal Data** | Information that is generally available within the University but is not classified as open to the general public. By default all University information will have this classification at minimum, however Data Stewards may reclassify it.<br>+ Employee ID |
| **Sensitive-Confidential Data** | Information that the organization and its employees have a legal, regulatory, or social obligation to protect. Intended for use solely within defined groups in the organization.<br><br>Information intended solely for restricted use within the organization and is limited to those with an explicit, predetermined "need to know". Disclosure could result in personal or financial damage to individuals or the organization<br>+ Employee benefit information<br>+ Student non-directory information<br>+ SSN<br>+ Passwords / PINS<br>+ Credit card numbers<br>+ Digitized signatures<br>+ Encryption keys<br>+ Medical Records – Employee, student, research<br>+ Student ID |
| | |

## 4. Index