THE UNIVERSITY OF TEXAS MEDICAL BRANCH

INFORMATION RESOURCE SECURITY PROGRAM

Published February 1, 2008
Authority

This document has been developed by the UTMB Office of Information Security (OIS) in furtherance of its statutory responsibilities under the Texas Administrative Code 202.71

The OIS is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all UTMB Information resources. The information contained in this document is consistent with the requirements as set fourth by the Texas Administrative Code 202, Subchapter C and the University of Texas System Policy UTS-165. It is not to be taken to contradict standards and guidelines made mandatory and binding by UT System, the State of Texas or the Federal Government.

This guideline has been prepared for use by all personnel of UTMB. It may also be used by other components within the University of Texas System and is not subject to copyright. (Attribution would be appreciated by the UTMB OIS.)

This document has been reviewed and the underlying Institutional Information resource Security Program is approved for use by The President of The University of Texas Medical Branch at Galveston.

David L. Callender, MD
UTMB President
Table of Contents

Authority ........................................................................................................... i
Table of Contents ........................................................................................... ii
Executive Summary ......................................................................................... vi
Organizational Structure ............................................................................... vii

1.0 Introduction ............................................................................................... 1
1.1 Purpose and Scope ..................................................................................... 1
1.2 Audience .................................................................................................. 1

2.0 Roles and Responsibilities ......................................................................... 2
2.1 UTMB President ....................................................................................... 2
2.2 Information Resource Manager ................................................................. 2
2.3 Department Head and Principle Investigator ............................................. 2
2.4 Director of IT Operations .......................................................................... 2
2.5 Information Security Administrator .......................................................... 2
2.6 Information Security Officer ...................................................................... 2
2.7 Institutional Compliance and Internal Audit ............................................. 3
2.8 Owner ...................................................................................................... 3
2.9 Owner of Mission Critical Information Resources .................................... 3
2.10 End-User ................................................................................................. 3
2.11 Vendor .................................................................................................... 4

3.0 Policies and Practice Standards ................................................................. 5
3.1 Policy Requirements .................................................................................. 5
3.2 Policy Development .................................................................................. 5
3.3 Policy Exceptions ..................................................................................... 6

4.0 Network Design ......................................................................................... 7
4.1 Minimum Requirements ........................................................................... 7

5.0 Privacy .................................................................................................... 8
5.1 System Warning Banner .......................................................................... 8

6.0 Acceptable Use of Information Resources ................................................. 9
6.1 Acceptable Use Requirements .................................................................. 9
6.2 Incidental Use .......................................................................................... 10

7.0 Email Use ................................................................................................ 11
7.1 Acceptable Use of Email .......................................................................... 11
7.2 Incidental Use of Email ........................................................................... 12

8.0 Internet Usage .......................................................................................... 13
8.1 Acceptable Use of the Internet ................................................................. 13
8.2 Incidental Use of the Internet ................................................................. 13
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.0 Network Access</td>
<td>36</td>
</tr>
<tr>
<td>21.1 Network Access Implications</td>
<td>36</td>
</tr>
<tr>
<td>21.2 Network Access Practice Standard</td>
<td>36</td>
</tr>
<tr>
<td>22.0 Wireless Access</td>
<td>38</td>
</tr>
<tr>
<td>22.1 Wireless Access Implications</td>
<td>38</td>
</tr>
<tr>
<td>22.2 Wireless Access Practice Standard</td>
<td>38</td>
</tr>
<tr>
<td>23.0 Change Management</td>
<td>40</td>
</tr>
<tr>
<td>23.1 Change Management Implication</td>
<td>40</td>
</tr>
<tr>
<td>23.2 Change Management Practice Standard</td>
<td>40</td>
</tr>
<tr>
<td>24.0 Backup and Data Recovery</td>
<td>42</td>
</tr>
<tr>
<td>24.1 Backup and Data Recovery Implications</td>
<td>42</td>
</tr>
<tr>
<td>24.2 Backup and Data Recovery Practice Standard</td>
<td>42</td>
</tr>
<tr>
<td>25.0 Reporting of Lost Information Resources and Data</td>
<td>43</td>
</tr>
<tr>
<td>25.1 Reporting of Lost Information Resources and Data Implications</td>
<td>43</td>
</tr>
<tr>
<td>25.2 Reporting of Lost Information Resources and Data Practice Standard</td>
<td>43</td>
</tr>
<tr>
<td>26.0 Portable Computing</td>
<td>45</td>
</tr>
<tr>
<td>26.1 Portable Computing Implications</td>
<td>45</td>
</tr>
<tr>
<td>26.2 Portable Computing Practice Standard</td>
<td>45</td>
</tr>
<tr>
<td>27.0 Remote Access</td>
<td>47</td>
</tr>
<tr>
<td>27.1 Remote Access Implications</td>
<td>47</td>
</tr>
<tr>
<td>27.2 Remote Access Practice Standard</td>
<td>47</td>
</tr>
<tr>
<td>28.0 Encryption</td>
<td>49</td>
</tr>
<tr>
<td>28.1 Encryption Implication</td>
<td>49</td>
</tr>
<tr>
<td>28.2 Encryption Standard</td>
<td>49</td>
</tr>
<tr>
<td>29.0 Data Classification</td>
<td>51</td>
</tr>
<tr>
<td>29.1 Data Classification Categories</td>
<td>51</td>
</tr>
<tr>
<td>29.2 Data Reclassification</td>
<td>53</td>
</tr>
<tr>
<td>30.0 Security Training and Awareness</td>
<td>54</td>
</tr>
<tr>
<td>30.1 Training and Awareness Responsibilities</td>
<td>54</td>
</tr>
<tr>
<td>30.2 End-user Training</td>
<td>54</td>
</tr>
<tr>
<td>30.3 Information Security Administrator and Program Developer Training</td>
<td>55</td>
</tr>
<tr>
<td>30.4 Information Security Awareness</td>
<td>55</td>
</tr>
<tr>
<td>31.0 Information Security Councils, Groups and Meetings</td>
<td>56</td>
</tr>
<tr>
<td>31.1 Information Services Security Leadership Council</td>
<td>56</td>
</tr>
<tr>
<td>31.2 Information Security Administrators Council</td>
<td>56</td>
</tr>
<tr>
<td>31.3 Incident After Action Meetings</td>
<td>57</td>
</tr>
</tbody>
</table>
32.0 Media Sanitization
32.1 Sale Transfer and Disposal of Information Resources
32.2 Record Keeping
32.3 Media Sanitization Matrix

APPENDIXES

a) Security Practice Bulletins
b) References
c) Definitions
d) Acronyms
e) Document Revision History
Executive Summary

Information Security (InfoSec) has emerged as the predominant challenge of the information age. The “ever present” world wide domain of the Internet, high speed data transfer, large capacity portable storage devices coupled with the demand for unfettered access to confidential, sensitive and proprietary data has made information security a challenge to manage.

Vision

• Create and maintain an enterprise-wide information resource security program to protect institutional data, which is highly sensitive and often confidential, while not obstructing the business needs of UTMB.
• That any compromise, degradation or disruption of the operation of critical UTMB information resources be rare, brief, limited in effect, manageable, and minimally detrimental to the integrity of UTMB services and mission.
• To continuously enhance the quality, efficiency, and effectiveness of this function.

Goal

To strike a reasonable balance among competing needs and influences for information security, productivity, end-user convenience, and cost-effectiveness; all based upon prudent business judgment and an overall understanding of the risks and consequences of unauthorized disclosure, alteration, destruction, or the disrupted or degraded access of critical information systems and the data that they manage.

In response to this defined vision and goal, the President of The University of Texas at Galveston, under the authority of Texas Administrative Code, Rule §202.71 has appointed and empowered the Information Security Officer (ISO) to maintain oversight and control of the enterprise information security program.

The ISO is charged with the development of policies, procedures and practices. The ISO will maintain an up-to-date information security program and monitor the effectiveness of defined security controls. He/She will also ensure that the confidentiality and integrity of all information resources (IR) and will submit a report, at least annually to the IRM as to the status and effectiveness of information resources security controls.

Conclusion

As long as there is the ability to profit from stolen information, threats to our information resources will remain constant and the means to compromise them will continue to evolve. As tactics get more sophisticated, the users and caretakers of our information resources must remain vigilant, informed and trained to protect our assets from new and emerging threats.

This document is intended to provide guidance to the Information Security Officer and other members of the UTMB community so that a comprehensive Information Resource Security program can be established, maintained and matured, thereby minimizing our risk of loss, unauthorized disclosure or theft of one of our most valuable asset, information.
Information Security Organizational Structure

UTMB uses a matrix managed approach to administer its information resource security program. Instead of having a centralized information services (IS) security department, enterprise responsibilities are spread across several department within IS. This approach allows UTMB to leverage talent within specific department where a dedicated security resource is not required to support a specific security process. An example would be the enterprise spam filtering solution. While spam filtering is considered a security function, the filter itself is a component of the email gateway sitting on a Linux platform, it only make sense for the email administrator to support the entire platform since all the components are tightly integrated.

The matrix managed approach also protects from collusion, where as the Director of Operations is responsible for the operational aspect of security, the Information Security Officer is responsible for program oversight.

Information Security Organizational Chart

[Diagram showing the organizational structure with roles and responsibilities]

- Compliance Reporting Only
- Security Council, Compliance Reporting, Planning
1.0 Introduction
Providing sound IT security within the university is essential to protecting information assets, safeguarding the integrity of institutional processes, and ensuring compliance with state and federal regulations. One challenging characteristic of higher education is a culture that values relatively uncontrolled and timely access to information and the free and continuous scholarly exchange of ideas. This culture requires that a secure environment carefully balance the extremes of leaving institutional and faculty information assets unprotected in a misplaced spirit of “academic freedom”, and choking off critical pathways of scholarly exchange by overly restricting access to these assets.

Other differences regarding information security in higher education…

- Mission diversity (teaching, research, healthcare delivery, business functions, etc.)
- User diversity (faculty, staff, students, contractors, volunteers, temporaries, agents, affiliates, business associates, and other 3rd parties)

Additionally, healthcare is one business that must have the best information protection available, lives may depend on it. For this reason, the most important assets we protect are patients and the privacy of their personal medical data.

Therefore, UTMB must ensure the privacy and security of it’s IR: the IT infrastructure, information systems, the files, records and data elements instrumental to delivering quality medical care, education, and on-going research.

1.1 Purpose and Scope
It is the policy of the state of Texas that information resources residing in the various agencies of State government are strategic and vital assets belonging to the people of Texas. Assets of UTMB must be available and protected commensurate with their value and must be administered in accordance with federal and state law and UTMB’s policies and practice standards.

This document provides requirements and guidelines to establish, maintain and manage a comprehensive security program that will protect the confidentiality, integrity, and availability of sensitive and confidential information contained within the confines of UTMB’s information Resources.

This document is also intended to serve as the foundation for UTMB’s information resource security program, while providing the Information Security Officer with the necessary authority to enforce policies, practice standards, and/or procedures that have been approved and published in accordance with current Practice Standards.

1.2 Audience
This document is primarily written for the Information Security Officer, Security Managers, Information Security Administrators and Security Analysts. It targets individuals who are familiar with the basic concepts of information security controls, concepts and processes.
2.0 Roles and Responsibilities

2.1 UTMB President
1. Ensures the compliance with the Information Security program.
2. Budgets sufficient resources to fund ongoing and continuous information security remediation, implementation and compliance activities that reduce compliance risk to an acceptably low level.
3. Approves the Institutional Information Security Program, or designate someone to provide this approval.
4. Ensures that appropriate corrective and disciplinary action is taken in the event of non-compliance.
5. Designates an individual other than the Information Resource Manager to serve as the Information Security Officer (ISO) who shall serve in the capacity as required by state law and with authority for that entire Entity.

2.2 Information Resources Manager (IRM):
1. Manages UTMB’s information resources.
2. Provides coordination of UTMB’s information activities, and ensure greater visibility of such activities within and between UT Components and other state agencies.
3. Implements Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of UTMB, including both centralized and decentralized systems.

2.2 Department Head and Principal Investigator
1. Complies with all IR security standards as it relates to Non-Research and Research Data respectively under their control including when holding subcontracts for projects in which the prime award is at another institution or agency.

2.3 Director of IT Operations
1. Manages information resource accounts in accordance with the institution’s information security policies, standards, and/or procedures.
2. Approves the installation of all network hardware connected to the local-area network
4. Requires compliance from all individuals who manage Information Systems or applications.

2.4 Information Security Administrator
1. Implements and complies with all information technology policies and practice standards relating to assigned systems.
2. Performs an annual information security risk assessment for Mission Critical Information Resources.
3. Reports general computing and security incidents to the ISO.
4. Assists, as member of the ISA Work Group, the ISO in developing, implementing, and monitoring the Information Security Program.
5. Establishes reporting guidance, metrics, and timelines so the ISO can monitor the effectiveness of security strategies in both the centralized and decentralized operations.
6. Reports at least annually to the ISO about the status and effectiveness of information resources security controls.

2.5 **Owner of Mission Critical Information Resources**
   1. Designates an individual to serve as an Information Security Administrator (ISA) to implement information security policies and procedures and for reporting incidents to the ISO.
   2. Performs an annual information security risk assessment.

2.6 **Information Security Officer**
   1. Provides information security for all centrally maintained and all distributed systems and computer equipment.
   3. Conducts and documents an information security risk assessment annually in accordance with 1 TAC 202.72 that identifies Mission Critical Information Resources in the central and all decentralized areas.
   4. Ensures an annual information security risk assessment is performed by each Owner of Mission Critical Information Resources.
   5. Requires each Owner of Mission Critical Information Resources to designate an Information Security Administrator (ISA).
   6. Establishes an Institutional Information Security Working Group composed of ISAs and holds meetings at least quarterly.
   7. Documents and maintains an up to date Institutional Information Resource Security Program.
   8. Establishes reporting guidance, metrics, and timelines and monitors the effectiveness of security strategies in both central and decentralized operations.
   9. Communicates instances of non-compliance to appropriate administrative officers for corrective, restorative and/or disciplinary action.
   10. Reports quarterly to the U. T. System CISO the current status of the information security risk assessment and Information Security Program, including any significant incidents, situations of non-compliance, barriers to program execution, and planned remedies.

2.7 **Institutional Compliance and Internal Audit**
   Provide high-level monitoring of the Information Security Compliance Program through inspections and verifications of reported information and periodic audits respectively.

2.8 **Owner**
   1. Grants access to the Information System under his/her responsibility.
   2. Classifies Digital Data based on Data sensitivity and risk.
   3. Backs up Data under his/her responsibility in accordance with risk management decisions and secures back up media.

2.9 **End-user**
   1. Complies with UTMB approved Policies and Practice Standards.
   2. Formally acknowledges and abides by the institution’s acceptable use policies.

2.10 **Vendor**
1. Complies with all applicable UTMB rules, policies, practice standards and agreements, and adheres to Federal and State laws to which UTMB must adhere.

2. Represents, warrants and certifies it will hold all UTMB Sensitive Data in the strictest confidence.
3.0 Policies and Practice Standards

The foundation of UTMB’s information resource security program is a comprehensive set of policies and practice standards that are designed to provide guidance to all personnel who are authorized to develop, maintain and access information resources.

The compliance with these published standards are mandatory and as such, will adequately secure information resources from unauthorized access, data manipulation, disclosure and theft of sensitive and confidential information.

3.1 Policy Requirements

Texas Administrative Code (TAC) Rule §202.75 and The University of Texas System Policy 165 (UTS-165) either requires or recommends, but does not limit, the following policies or practice standards be developed, approved and published by all institution of higher education:

1. Acceptable Use--Defines scope, behavior, and practices; compliance monitoring pertaining to users of information resources.
2. Account Management--Establishes the rules for administration of user accounts.
3. Administrator/Special Access--Establishes rules for the creation, use, monitoring, control, and removal of accounts with special access privileges.
5. Change Management--Establishes the process for controlling modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against improper modification before, during, and after system implementation.
6. Email--Establishes prudent and acceptable practices regarding the use of email for the sending, receiving, or storing of electronic mail. Ensures compliance with applicable statutes, regulations, and mandates. The policy shall prohibit sending an individual's name and restricted personal information unless the data is encrypted.
7. Incident Management--Describes the requirements for dealing with computer security incidents including prevention, detection, response, and remediation.
8. Internet/Intranet Use--Establishes prudent and acceptable practices regarding the use of the Internet and Intranet.
9. Intrusion Detection--Establishes requirements for auditing, logging, and monitoring to detect attempts to bypass the security mechanisms of information resources.
10. Network Access--Establishes the rules for the access and use of the network infrastructure.
11. Network Configuration--Establishes the rules for the maintenance, expansion, and use of the network infrastructure.
12. Password/Authentication--Establishes the rules for the creation, use, distribution, safeguarding, termination, and recovery of user authentication mechanisms.
13. Physical Access--Establishes the rules for the granting, control, monitoring, and removal of physical access to information resources.
15. Privacy--Methodologies used to establish the limits and expectations regarding privacy for the users of information resources.
16. Security Monitoring--Defines a process that ensures information resources security controls are in place, are effective, and are not being bypassed.
17. Security Awareness and Training--Establishes the requirements to ensure each user of information resources receives adequate training on computer security issues.
18. Platform Hardening--Establishes the requirements for installing and maintaining the integrity of a platform in a secure fashion.
19. Authorized Software--Establishes the rules for software use on information resources.
20. System Development and Acquisition--Describes the security and business continuity requirements in the systems development and acquisition life cycle.
21. Vendor Access--Establishes the rules for vendor access to information resources, support services (Air Conditioning, Universal Power Supply, Power Distribution Unit, fire suppression, etc.), and vendor responsibilities for protection of information.
22. Malicious Code--Describes the requirements for prevention, detection, response, and recovery from the effects of malicious code (including but not limited to viruses, worms, Trojan Horses, and unauthorized code used to circumvent safeguards.)
23. Wireless Access--Establishes the requirements and security restrictions for installing or providing access to the institution of higher education information resources systems.

3.2 Policy Development
Working with members of the ISA working group, Information Services Leadership (ISL) and the Computer Services Advisory Group (CSAG), the ISO will develop, review, gain approval from the IRM and publish all required policies and practice standards.

3.3 Policy Exceptions
An owner of information resources may request, in writing, an exception to a published policy or practice standards. All requests will be carefully analyzed by the ISO and approved/disapproved based on its business justification and associated risk.

Prior to the approval of non-standard requests or requests that may pose significant risks to UTMB, the ISO will seek advice from the IRM. At the discretion of the IRM, requests may be escalated to the Office of Institutional Compliance or Legal Affair for further review and recommendations.

Policy exception request forms are located at http://cirt.utmb.edu.
4.0 Network Design
Working with the Director of IT Operation, ISL and the ISA working group, The ISO will ensure that the data network is designed and configured in such a way that will minimize external and internal threats to all information resources owned and/or maintained by UTMB.

4.1 Minimum Requirements
Perimeter security controls shall be established, maintained, controlled and monitored. These controls will include, but are not limited to the following:

1. DMZ (Demilitarized Zone)--The DMZ is the network area created between the public Internet and internal private network(s). This neutral zone is usually delineated by some combination of routers, firewalls, and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (email) servers, and DNS servers.

2. Firewall--A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both and are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets. They can also regulate traffic between networks within the same institution of higher education.

3. Intrusion Detection System--Hardware and/or software which is installed on a network and compares network traffic and host log entries to the known and likely methods of attackers. Suspicious activities trigger administrator alarms and other configurable responses.

4. Router--A device or, in some cases, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks to which it is connected. A router is located at any gateway where one network meets another.

5. Compliance Monitoring System--Hardware and/or software which is installed on a network to monitor data traffic destined to a public network for evidence of sensitive or confidential data being transmitted in an unsecured manner.

6. Email Gateway Anti-Virus--Hardware and/or software which is installed at the email gateway and will automatically detect, tag, delete or quarantine email that may be infected with a Virus, Worm or Trojan.

7. Email Gateway Anti-Spam--Hardware and/or software which is installed at the email gateway and will automatically detect, tag, delete or quarantine unsolicited email.

8. Network Access Control--Hardware and/or software which is installed on the network that restricts the availability of network resources to endpoint devices that do not comply with a defined security policy.
5.0 Privacy
Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code, Title 1, Part 10, Chapter §202 (Information Security Standards), Information Resource Standards and in the University of Texas System, UTS 165 - Information Resources Use and Security Policy.

5.1 System Warning Banner
1. To ensure that users of information resources are aware of UTMB’s privacy policy, all UTMB owned and managed information systems will display the following warning banner at all user interfaces

You have accessed an Information System that is the property of or licensed to The University of Texas Medical Branch at Galveston (UTMB). This system has been made available for authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to legal prosecution.

For the integrity of the system and to comply with state and federal mandates, policy and practice standards govern its use. These polices and practice standards are available for review at http://www.utmb.edu/policy/is/listing.htm. By accessing this information resource you acknowledge that you understand, and shall comply with the requirements as they are outlined in the referenced policies and practice standards.

Be advised, all activity on this system may be monitored and recorded by systems support personnel. Pursuant to the Texas Administrative Code (Title I, Part 10, § 202.76), anyone using this or any other UTMB information system expressly consents to such monitoring and is advised that if such monitoring reveals criminal or other inappropriate activity, system administrators may provide the evidence of such monitoring to UTMB management as well as law enforcement officials.
6.0 Acceptable Use of Information Resources

The UTMB information resources infrastructure is an integrated network of computer resources which exists to support essential UTMB services and missions. As such, UTMB has the responsibility to maintain and mediate the use of this shared and finite resource to ensure its ongoing availability to the entire user community. Users are thus expected to exercise reasonable care in their use of this shared resource.

1. Specifically included in this responsibility are:

   a) The observance of Federal, State, and Local laws and regulations governing the use of computing and network resources.
   b) The observance of all established policies and practice standards of UTMB.
   c) The exercise of reasonable care to ensure that their use of these shared resources does not adversely impact availability of these same resources to other users.
   d) the exercise of reasonable care to ensure the security of UTMB information resources.

2. As a user, it is also important to be aware that:

   a) no security mechanism is impregnable.
   b) no security mechanism can protect against the improper behavior of authorized users.
   c) Hence, all personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Failure to implement and comply with appropriate controls can lead to institutional financial penalties, which can lead to loss of public trust, competitive advantage, and ultimately, jobs.

6.1 Acceptable Use Requirements

1. Users must report any weaknesses in UTMB computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management or the UTMB Computer Incident Response Team at (409) 772-3838.

2. Users shall not attempt to access any data or programs contained on UTMB systems for which they do not have authorization or explicit consent.

3. Users shall not divulge dialup or dial-back modem phone numbers to anyone.

4. Users shall not use non-standard software without initially contacting IS and receiving IRM approval unless it is on the UTMB standard software list. (Note: A reference listing of approved software is published at http://www.utmb.edu/isbusops/softwarestandards.aspx

5. Users shall not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of IR; deprive an authorized UTMB user access to a UTMB resource; obtain extra resources beyond those allocated; circumvent UTMB computer security measures.

6. Users shall not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, UTMB users shall not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on UTMB IR.

7. UTMB IR may not be used for personal benefit.
8. Users shall not intentionally access, create, store or transmit material which UTMB may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the UTMB official processes for dealing with academic ethical issues).

9. Users shall not otherwise engage in acts against the aims and purposes of UTMB as specified in its governing documents or applicable rules, regulations, and procedures.

6.2 Incidental Use
As a convenience to the UTMB user community, incidental use of IR is permitted. The following restrictions apply:

1. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, etc., is restricted to UTMB approved users; it does not extend to family members or other acquaintances.

2. Incidental use must not result in direct costs to UTMB.

3. Incidental use must not interfere with the normal performance of an employee’s work duties.

4. No files or documents may be sent or received that may cause legal action against, or embarrassment to, UTMB.

5. Storage of personal email messages, voice messages, files and documents within UTMB’s IR should be nominal.

6. Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code, Title1, Part 10, Chapter §202 (Information Security Standards), Information Resource Standards and in the University of Texas System, UTS 165 - Information Resources Use and Security Policy.
7.0 Email Use
1. Under the provisions of the Information Resources Management Act, information resources are strategic assets of the State of Texas that must be managed as valuable state resources.

This chapter establishes:
   a) compliance with applicable statutes, regulations, and mandates regarding the management of information resources, specifically electronic mail (email).
   b) prudent and acceptable practices regarding the use of email.
   c) education for individuals who may use email with respect to their responsibilities associated with such use.

2. UTMB provides email capability for legitimate business use in the course of assigned duties for the purpose of enhancing productivity and maintaining effective communications in support of the missions of UTMB.

7.1 Acceptable Use of Email
1. The following activities are prohibited:
   a) Do not send email that may be interpreted as intimidating or harassing by the recipient.
   b) Do not use email for conducting a personal business.
   c) Do not use email for purposes of political lobbying or campaigning.
   d) Do not violate copyright laws by inappropriately distributing protected works.
   e) Do not pose as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.

2. The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
   a) Do not send or forward chain letters.
   b) Do not send unsolicited messages to large groups except as required to conduct university business.
   c) Do not send excessively large messages.
   d) Do not send or forward email that is likely to contain computer viruses.
   e) Prohibited activities identified in this section are not all inclusive. UTMB electronic mail must never be used in a manner that violates federal law, state law, U.T. System policy, UTMB policy, or UTMB practice standards.

7.2 Email Incidental Use
As a convenience to employees, incidental use of electronic mail is allowed. The following restrictions apply:

1. Incidental personal use of UTMB provided electronic mail is restricted to UTMB employees; it does not extend to family members or friends.
2. Incidental use must not result in direct costs to UTMB.
3. Incidental use must not interfere with the normal performance of an employee’s work duties.
4. No personal messages should be sent or saved that may cause embarrassment to UTMB.

5. No personal messages should be sent, read, or saved that have high likelihood to expose University computer systems to computer viruses or other harmful programs.

6. Storage of personal email messages, attachments, or files within UTMB’s electronic mail system(s) should be nominal.

7. Employees should remove themselves from any personal mail lists that send messages containing content incompatible with this policy.

8. Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code, Title 1, Part 10, Chapter §202 (Information Security Standards), Information Resource Standards and in the University of Texas System, UTS 165 - Information Resources Use and Security Policy.
8.0 Internet Usage
All personnel are responsible for managing their use of the Internet and are accountable for their actions relating to IR security.

8.1 Acceptable Use of the Internet
1. Software for browsing the Internet is provided to authorized users for business and research use only.
2. All software used to access the Internet must be part of the UTMB standard software suite or approved by the ISO. This software must incorporate all vendor provided security patches.
3. All files downloaded from the Internet must be scanned for viruses using the approved IS distributed software suite and current virus detection software.
4. All sites accessed must comply with the UTMB Acceptable Use Policies and Practice Standards.
5. All user activity on UTMB IR assets is subject to logging and review.
6. Content on all UTMB Web sites must comply with the UTMB Acceptable Use Policies and Practice Standards.
7. No offensive or harassing material may be made available via UTMB Web sites.
8. No personal commercial advertising may be made available via UTMB Web sites.
9. UTMB Internet access may not be used for personal gain or non-UTMB personal solicitations.
10. No UTMB data will be made available via UTMB Web sites without ensuring that the material is available to only authorized individuals or groups.
11. Posting sensitive or confidential data to external, third-party websites must use Secure Socket Layer (SSL) protocols or other approved, secured transmission methods to protect the data in transit.
12. Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

8.2 Incidental Use of the Internet
1. Incidental personal use of Internet access is restricted to UTMB approved users; it does not extend to family members or other acquaintances.
2. Incidental use must not result in direct costs to UTMB.
3. Incidental use must not interfere with the normal performance of an employee’s work duties.
4. No files or documents may be sent or received that may cause legal liability for, or embarrassment to, UTMB.
5. Storage of personal files and documents within UTMB’s IR should be nominal.
6. Electronic files created, sent, received, or stored on IR owned, leased, administered, or otherwise under the custody and control of UTMB are not private and may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code, Title 1, Part 10, Chapter §202 (Information Security Standards), Information Resource Standards and in the University of Texas System, UTS 165 - Information Resources Use and Security Policy.
9.0 Software Compliance with Copyright Laws
It is the policy of UTMB that no faculty, staff, or student use any UTMB facility, equipment or property to copy software from one source to another, except as expressly permitted by the Copyright Act or the applicable software license agreement.

9.1 Liability
Seemingly innocent copying can subject the alleged infringer and UTMB to both civil and criminal liability unless such copying is consistent with relevant license agreements, copies are being made for contingency planning purposes, or with the permission of the author/owner.

9.2 Procedures
Software provided through UTMB for use by faculty, staff and students, may only be used on computing equipment as specified in the applicable software license agreement between UTMB and the software licensor.

9.3 Advisory Resource
The Information Services (IS) Department may be contacted as an advisory resource for information concerning software copyright compliance.
10.0 Security Monitoring
Security Monitoring is a method used to confirm that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of:

1. Automated intrusion detection system logs
2. Firewall logs
3. User account logs
4. Network scanning logs
5. Application logs
6. Data backup recovery logs
7. Help Desk logs
8. Other logs, error files, and audit trails.

We use system, security and audit logs to record and examine system activity in an attempt to recognize questionable access activity, assess security programs, and respond to potential system weaknesses.

One of the benefits of security monitoring is the early identification of suspicious activity or new security vulnerabilities. This early identification can help to block the potentially harmful data traffic or identify vulnerability before harm can be done or at least minimize the impact. Other benefits include Audit Compliance, Service Level Monitoring, Performance Measuring, Limiting Liability, and Capacity Planning.

10.1 Automated Tools
Automated tools will provide notification of detected wrongdoing and potential vulnerability exploitation. These tools will be deployed to monitor:

1. Internet traffic
2. Electronic mail traffic
3. LAN traffic, protocols and devices connected to the network
4. Operating system security parameters

10.2 Security Log Inspection
The following files will be checked for signs of wrongdoing and vulnerability exploitation:

1. Automated intrusion detection system logs
2. Firewall logs
3. User account logs
4. Network scanning logs
5. System logs
6. Application logs
7. Data backup and recovery logs
8. Help Desk trouble tickets
9. Telecommunications activity
10. Network printer and fax logs

11. The following checks will be performed at least quarterly:
a) Compliance with password practice standards
b) Unauthorized network devices
c) Unauthorized personal web servers
d) Unauthorized modem use
e) Unsecured sharing of devices
f) Unsecured platform/application configurations
g) Operating system and software licenses

12. For audit purposes, logs will be archived for a minimum of 90 days.
13. Any security issues discovered will be reported to the ISO for follow-up investigation.
14. For every significant information systems security risk, management must make a specific decision about the degree to which UTMB will assume that risk, adjust controls to minimize the risk, or mitigate the risk.
15. Examples of events to log:

   a) Every addition, modification, deletion or viewing of patient information by User ID
   b) User access violations
   c) System changes
   d) Override transactions
   e) All activities/events that violate established security standards or configurations
   f) Any attempt to deactivate, modify, or delete logging capabilities or the logs themselves
   g) Changes to security privileges/profiles
   h) Changes to security configurations
11.0 Intrusion Detection/Prevention

Intrusion detection/Prevention plays an important role in implementing and enforcing an organizational security policy. As information systems grow in complexity, effective security systems must evolve. With the increase in the number of vulnerability points introduced by the use of distributed systems, some type of assurance is needed that the systems and network are secure. Intrusion detection/prevention systems can provide part of that assurance.

Intrusion detection/prevention provides two important functions in protecting information resources:

1. Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
2. Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

11.1 Intrusion Detection/Prevention Implications

1. To allow UTMB to promptly respond to information attacks, perimeter security will include intrusion detection capabilities.
2. Whenever a systems administrator has good reason to believe that information resources have been compromised, the involved computer(s) must be immediately removed from the network.
3. All security incidents must be properly and promptly reported.

11.2 Intrusion Detection/Prevention Practice Standard

Users reporting any anomalies in system performance and signs of wrongdoing should be directed to the Information Security Officer (ISO) at ext. 23838, the Computer Incident Response Team (CIRT) at ext. 23838, the IS Help Desk at ext. 25200, or to the UTMB Compliance Hotline at (800) 898-7679.

1. All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported in accordance with chapter 15 of this manual.
2. Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems as defined by UTMB Information Services.
3. Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
4. Audit logging of any firewalls and other network perimeter access control system must be enabled.
5. Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.
6. System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.
7. Audit logs for servers and hosts on the internal, protected network shall be reviewed by the system administrator on a weekly basis. The system administrator will furnish any audit logs as requested by the ISO.
8. Network/host-based intrusion tools will be checked on a routine basis by the system administrator.
9. All trouble reports received by system administration personnel should be reviewed for symptoms that might indicate intrusive activity.
12.0 Malware Detection
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents. This chapter describes the requirements for dealing with computer virus, worm, back door, and Trojan Horse prevention, detection and cleanup.

12.1 Malware Implications
1. To prevent infection by computer viruses, all users must employ virus detection capabilities which must be continuously enabled.
2. Virus detection capabilities must be kept current.
3. All suspected or confirmed virus infestations must be properly and promptly reported.

12.2 Malware Detection/Configuration Practice Standard
1. All workstations connected to the UTMB network must use the UTMB IS approved virus protection software and configuration. Additionally, this applies to users connecting to the UTMB network from home computers.
2. The virus protection software must not be disabled.
3. The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
4. The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
5. Each file server attached to the UTMB network must utilize UTMB IS approved virus protection software and configuration to detect and clean viruses that may infect file shares.
6. Each email gateway must utilize UTMB IS approved email protection software and must adhere to the IS rules for the configuration and use of this software.
7. Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Computer Incident Response Team (CIRT) at ext. 23838.
**13.0 Network Configuration**

The UTMB network infrastructure is a vital information asset provided as a central utility for all users of UTMB Information Resources. It is important that the infrastructure, which includes cabling and the associated active equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

This Chapter establishes the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of UTMB information.

**13.1 Network Configuration Implication**

1. The UTMB network infrastructure must be configured such that it can prevent and/or detect attempts to connect unauthorized computer devices.
2. Configuration and set-up parameters on all hosts and workstations attached to the UTMB network must comply with UTMB IR Security policies and practice standards.

**13.2 Network Configuration Practice Standard**

1. Users must not extend or re-transmit network services in any way. This means users must not install a router, switch, hub, or wireless access point to the UTMB network without UTMB IS Network and Security Services approval.
2. Users must not install network hardware or software that provides network services without UTMB IS Network and Security Services approval.
3. Users are not permitted to alter network hardware in any way.
4. UTMB Information Services owns and is responsible for the UTMB network infrastructure and will continue to manage further developments and enhancements to this infrastructure.
5. To provide a consistent UTMB network infrastructure capable of exploiting new networking developments, all cabling must be installed by UTMB IS Network and Security Services or an approved contractor.
6. All network connected equipment must be configured to a specification approved by UTMB IS Network and Security Services.
7. All hardware connected to the UTMB network is subject to UTMB IS Network and Security Services standards for management and monitoring.
8. Changes to the configuration of active network management devices must not be made without the approval of UTMB IS Network and Security Services.
9. The UTMB network infrastructure supports a well-defined set of approved networking protocols (primarily TCP/IP and IPX, with some AppleTalk). Any use of non-sanctioned protocols must be approved by UTMB IS Network and Security Services. The networking addresses for the supported protocols are allocated, registered and managed centrally by UTMB IS.
10. All connections of the campus network infrastructure to external third party networks are the responsibility of UTMB IS Network and Security Services, including connection to external telephone networks.
11. UTMB IS firewalls must be configured and maintained as per the UTMB IR Firewall Management procedures.
12. The use of departmental firewalls is not permitted without the written authorization from the UTMB IRM.
14.0 Platform Hardening
Platforms are defined as any electronic device capable of storing, processing or transmitting digital data. These devices are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the platforms are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

This chapter describes the requirements for installing a new platform or upgrading an existing platform in a secure fashion and maintaining the security integrity of the platform and application software to ensure that information systems equipment continues to operate as it should, thus supporting UTMB in achieving its mission.

14.1 Platform Hardening Implications
1. Before connecting to the UTMB network, all platforms must be preauthorized by appropriate management (i.e., accreditation).
2. New platforms connected to the data network and existing systems that are upgraded must have the preventative maintenance performed before the platforms are put into production. This includes such issues as removing default passwords, adding vendor patches, and removal of application software that may be included in a default installation, but is not necessary or wanted as part of the system's operational capacity.
3. To remain connected to the UTMB network, all platforms must comply with applicable baseline IR security policies and practice standards (i.e., certification).
4. Information must be protected in a manner commensurate with its confidentiality, sensitivity, value, and criticality.

14.2 Platform Hardening Practice Standard
1. A platform must not be connected to the UTMB network until it is in a UTMB IS accredited secure state and the network connection is approved by UTMB IS.
2. Security patches must be implemented within the timeframe specified from UTMB IS.
3. After a reasonable delay for the stabilization of the new release, UTMB must use the most recent version in order to take advantage of recent security improvements.
4. The Platform Hardening Procedure provides the detailed information required to harden a platform and must be implemented for UTMB IS accreditation. Some of the general steps included in the Platform Hardening Procedure include:
   a) Installing the operating system from an IS approved source
   b) Applying vendor supplied patches
   c) Removing unnecessary software, system services, and drivers
   d) Setting security parameters, file protections and enabling audit logging
   e) Disabling or changing the password of default accounts
5. UTMB IS will monitor information security vulnerability advisories issued by trusted organizations such as SANS or CERT.
6. UTMB IS will monitor security issues, both internal to UTMB and externally, and will centrally manage the release of security patches on behalf of UTMB.
7. UTMB IS will test security patches against IS core resources before release where practical.
8. UTMB IS may make hardware resources available for testing security patches in the case of special applications.

9. The platform must run appropriately licensed versions of the operating system and software.

10. Platforms must run only necessary services. After it has been determined what services are needed, all unnecessary services should be shut down.

11. The platform must have all default account passwords changed and after determining what default accounts are required, have all other default accounts disabled.

12. The platform may not function as a relay for SMTP or other means of relaying non-UTMB related email.

13. The platform must comply with all other IR Security policy and practice standards.

14. Servers must authenticate all users to ensure authorized access to the resource.
15.0 Incident Management
The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and the early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

This chapter describes the requirements for dealing with computer security incidents. Security incidents include, but are not restricted to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources (IR) as outlined in the Acceptable Use of Information Resources, Email Use, and the Internet Use.

15.1 Incident Management Implications
1. UTMB must organize and maintain an incident response team that will provide accelerated problem notification, damage control, and problem correction services in the event of computer related security incidents such as virus infestations, hacker break-ins, and the like.
2. To ensure a quick, effective, and orderly response to incidents, the incident response team will define procedures for handling incidents.
3. All suspected or known security incidents must be properly and promptly reported.
4. All known vulnerabilities, in addition to all suspected or known violations, must be communicated in an expeditious and confidential manner.

15.2 Incident Management Practice Standard
1. Should a virus incident occur with a user utilizing a non-standard virus detection package, that user will be disconnected from the network until such problem has been resolved. The user may also find that their connection status will be given low priority during the resolution of the incident.
2. UTMB CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.
3. Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate Incident Management procedures must be followed.
4. The ISO is responsible for notifying the IRM and the CIRT and initiating the appropriate incident management action including restoration as defined in the Incident Management Procedures.
5. The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation.
6. The appropriate technical resources from the CIRT are responsible for ensuring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
7. The ISO, working with the IRM, will determine if a widespread UTMB communication is required, the content of the communication, and how best to distribute the communication.
8. The appropriate technical resources from the CIRT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
9. The ISO is responsible for initiating and completing the incident investigation with assistance from the CIRT.

10. The UTMB ISO is responsible for reporting the incident to the:

   a) IRM
   b) System Owner
   c) Department of Information Resources as outlined in Texas Administrative Code, 1 TAC §§202 (Information Security Standards)
   d) University Police, local, state or federal law officials as required by applicable statutes and/or regulations
   e) Legal Affairs
   f) Internal Audit

11. The ISO is responsible for coordinating communications with outside organizations and law enforcement.

12. In the case where law enforcement is not involved, the ISO will recommend disciplinary actions to the IRM.

13. In the case where law enforcement is involved, the ISO will act as the liaison between law enforcement and UTMB.

14. Any attempt to interfere with, prevent, obstruct, retaliate, or dissuade the reporting of a suspected or known security problem, violation, or vulnerability is strictly prohibited and cause for disciplinary action.

15. Whenever evidence clearly indicates that UTMB has been victimized by a computer or communications crime, a thorough investigation must be performed. This investigation must provide sufficient information so that management can take steps to ensure that: (1) such incidents are not likely to take place again, and (2) effective security measures have been reestablished.

16. Whenever unauthorized system access is suspected or known to be occurring, UTMB personnel must take immediate action to terminate the access.

17. Information describing all reported security incidents must be retained for a period of three (3) years.

18. An annual analysis of reported security incidents must be prepared by the ISO for trend analysis.

19. A stern cease and desist message must be sent to the source of all attacks mounted against UTMB whenever the source or intermediate relay points can be identified.
16.0 Password Management
User authentication is a means to control who has access to an automated Information Resource system. Access gained by a non-authorized entity can cause loss of information confidentiality, integrity and availability that may result in loss of revenue, liability, loss of trust, or embarrassment to UTMB.

Three factors, or a combination of these factors, can be used to authenticate a user.

Examples are:
1. Something you know – password, personal identification number (PIN)
2. Something you have – token (i.e., SmartCard)
3. Something you are – biometrics (fingerprint, iris scan, voice recognition)
4. A combination of factors – token (i.e., SmartCard) and a PIN

This chapter establishes the rules for the creation, distribution, safeguarding, termination, and reclamation of UTMB user authentication mechanisms and to identify the measures that users are expected to take in ensuring the security of their account and UTMB IR.

16.1 Implications
1. Computer and communications system access control must be achieved via passwords that are unique to each individual user in compliance with UTMB security management policies and practice standards.
2. All users must have their identity verified with a User ID and a secret password (or by other means which provide equal or greater security) prior to being permitted to use UTMB computers connected to its network.
3. Users are responsible for all activity performed with their personal User ID. Similarly, users are prohibited from performing any activity with ID’s belonging to other users.
4. Passwords are the first level of protection from a would-be intruder. Once into the system, a knowledgeable user could do considerable damage. Thus, as a member of the user community, it is the responsibility of all users to choose a good password.

16.2 Password Practice Standard
1. User account passwords must not be disclosed to anyone. UTMB IS and its agents will not ask for user account passwords.
2. Users cannot circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software without the approval of the UTMB ISO. A procedure must be available to change the passwords.
3. IS Help Desk password change procedures must include the following:
   a) authenticate the user to the Help Desk before changing password
   b) change to a strong password
   c) the user must change password at first login
4. All passwords, including initial passwords, must be constructed and implemented according to the following UTMB IR rules:
   a) it must be routinely changed (every 60 days for normative use, every 30 days for administrative and special access privileges)
b) it must adhere to a minimum length of six characters
c) it must be a combination of alpha and numeric characters
d) it must not be anything easily identified with the account owner such as: user name, social security number, nickname, relative’s names, birth date
e) it must not be recurring passwords created by combining a set of characters that do not change with a set of characters that predictably change (i.e., May2002, Jun2002, Jul2002, etc.)
f) it must not be dictionary words, acronyms, or common character sequences (i.e., 123456, qwerty, zxcvbn, etc.)
g) a password history must be kept to prevent the frequent reuse of a password (minimally contains the last 8 passwords for each User ID)
h) after four (4) unsuccessful attempts to enter a password, the involved User ID must be suspended until reset by an appropriate party with administrator privileges

5. The display and printing of passwords must be suppressed such that unauthorized parties will not be able to observe or subsequently recover them.
6. Stored passwords must be encrypted.
7. Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with UTMB.
8. If the security of a password is in doubt, the password must be changed immediately.
9. System administrators must not circumvent the Password Management Practice Standard for the sake of ease of use.
10. In the event passwords are found or discovered, the following steps must be taken:
   a) take control of the passwords and protect them
   b) report the discovery to the UTMB IS Help Desk
   c) transfer the passwords to an authorized person as directed by the UTMB ISO

11. Developers are prohibited from building or deploying ‘backdoor’ User ID’s or passwords which have special privileges and circumvent normal system access.
12. All vendor supplied/default passwords must be changed before any computer or communications system is connected to the UTMB network.
17.0 Account Management

Computer accounts are the means used to grant access to UTMB Information Resources (IR). These accounts establish accountability for IR usage. This means that creating, controlling and monitoring all computer accounts is extremely important to an overall security program. This chapter establishes the rules for the creation, monitoring, control, and removal of user accounts.

17.1 Account Management Implications

1. The computer and communications system privileges of all users, systems, and programs must be restricted based upon the concept of ‘minimum necessary’ use (i.e., users receive only those access privileges minimally required to perform their assigned job duties).
2. User ID’s may be granted to specific users only when approved in advance by the trusted requestor within the business area. Prior to being granted to users, application system privileges must be authorized by the involved owner.
3. Computer and communications system privileges must be granted only by a clear chain of authority delegation.
4. The computers and computer accounts given to users are to assist them in the performance of their jobs. Users should not have an expectation of privacy in anything they create, store, send, or receive.

17.2 Account Management Practice Standard

1. All accounts created must have an associated request and approval that is appropriate for the UTMB system or service.
2. All users must sign the UTMB Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
3. All accounts must be uniquely identifiable using the assigned user name.
4. No two people may ever have the same User ID throughout the lifetime of the system (i.e., User ID’s are not to be reused).
5. All default passwords for accounts must be constructed in accordance with the UTMB Password Management Practice Standard.
6. All accounts must have a password expiration that complies with the UTMB Password Management Practice Standard.
7. All new user accounts that have not been accessed within 30 days will be disabled.
8. All user accounts utilized by UTMB employees and students that have not been accessed within 60 days (due to inactivity) will be disabled. (Note: The inactivity period for non-UTMB personnel is 60 days).
9. All disabled accounts will be permanently deleted after 30 days of revocation.
10. System Administrators:
   a) Are responsible for removing the accounts of individuals who change roles within UTMB or are separated from their relationship with UTMB.
   b) Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.
   c) Must have a process for periodically reviewing existing accounts for validity
   d) Are subject to independent audit review.
   e) Must provide a list of accounts for the systems they administer when requested by authorized UTMB management.
   f) Must cooperate with authorized UTMB management investigating security incidents.
11. Owners:
   a) Are responsible for developing transition plans for departmental data.
   b) Are responsible for timely notification to appropriate parties when staff leaves department.

12. Trusted Requestors:
   a) Are responsible for requesting revocation of all accounts for personnel transferring from their department or terminating employment at UTMB at the time of separation.
   b) Are responsible for assessing the separating employee’s non-shared drives and removing departmental information prior to employee separation.
   c) Are responsible for requesting minimum necessary access for employees within their department that enables them to perform their job functions.

13. Vendor and special access accounts must be reassessed at least quarterly.
18.0 Special Access
Technical support staff, security administrators, system administrators, and others may have special access account privilege requirements as compared to typical or normative users. The fact that these administrative and special access accounts have a higher level of access means that granting, controlling, and monitoring these accounts is extremely important to an overall security program. This chapter establishes the rules for the creation, use, monitoring, control, and removal of accounts with special access privilege.

18.1 Special Access Implications
1. All multi-user computer and network systems must support a special type of User ID which has broadly-defined system privileges. This User ID enables access to authorized individuals and processes of systems; therefore, these privileges must be restricted and granted only to those directly responsible for system management and/or security.
2. The extent of access privileges granted or used should not exceed that which is necessary to accomplish a specific business objective.

18.2 Special Access Practice Standard
1. Systems must be administratively supported and maintained by personnel that are properly trained and technically competent.
2. All users must sign the UTMB Information Resources Security Acknowledgement and Nondisclosure Agreement before access is given to an account.
3. Each individual who uses special access accounts must refrain from abuse of privilege and must only conduct investigations under the direction of the ISO.
4. Each individual who uses special access accounts must use the account privilege most appropriate with work being performed (i.e., user account vs. administrator account).
5. Each account used for special access must meet the UTMB Password Management Practice Standard.
6. UTMB departments must submit to CIRT a list of administrative contacts for their systems that are connected to the UTMB network and must provide updates as contact changes occur.
7. The password for a shared special access account must change when an individual with the password leaves the department or UTMB, or upon a change in the vendor personnel assigned to the UTMB contract. The account must also be re-evaluated as to whether it should remain a shared account or not. (Shared accounts must be kept to an absolute minimum.)
8. In the case where a system has only one administrator, a password escrow procedure must be in place so that someone other than the administrator can gain access to the administrator account in an emergency situation.
9. When special access accounts are needed for audit, software development, software installation or other defined need, they:
   a) Must be authorized by the system owner, IRM, or ISO.
   b) Must be created with a specific expiration date.
   c) Must be removed when work is complete.
10. All privileged commands issued in association with special access must be traceable to specific individuals via the use of comprehensive logs.
19.0 Vendor Access

Vendors play an important role in the support of hardware, software, management and operations for customers. Vendors can remotely view, copy and modify data; correct software and operating systems problems; monitor and fine tune system performance; monitor hardware performance and errors; modify environmental systems; and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to UTMB.

This chapter establishes the rules for vendor access to UTMB Information Resources (IR) and facilities support services (air conditioning, uninterruptible power supply, power-distribution units, fire suppression, etc.), vendor responsibilities, and protection of UTMB information.

19.1 Vendor Access Implications

1. All third party access to UTMB internal computer systems which are not clearly public must be approved in advance by the IRM or their designee. (They should be treated very carefully on a case-by-case basis.)
2. In-bound dial-up or Internet privileges must not be given to third party vendors unless the relevant system manager determines that these vendors have legitimate business need for such access. These privileges must be enabled for specific individuals and only for the time period required to accomplish approved tasks.
3. As a condition of gaining access to UTMB’s computer network, every third party must secure its own connected systems in a manner consistent with UTMB’s requirements.

19.2 Vendor Access Practice Standard

1. Vendors must comply with all applicable UTMB policies, practice standards, and agreements, including, but not limited to:
   a) Safety Policies
   b) Privacy Policies
   c) Security Policies
   d) Auditing Policies
   e) Software Licensing Policies
   f) Acceptable Use Policies
   g) Email Use and Internet Use Policies
   h) IR Security Management Practice Standards
2. Vendor agreements and contracts must specify:
   a) the UTMB information the vendor should have access to
   b) how UTMB information is to be protected by the vendor
   c) acceptable methods for the return, destruction or disposal of UTMB information in the vendor’s possession at the end of the contract
   d) the vendor must only use UTMB information and IR for the purpose of the business agreement
   e) any other UTMB information acquired by the vendor in the course of the contract cannot be used for the vendor’s own purposes or divulged to others
3. Each vendor must provide UTMB with a list of all employees working on the contract. The list must be updated and provided to UTMB within 24 hours of staff changes pertinent to physical or logical access concerns.

4. Each on-site vendor employee must acquire a UTMB identification badge that will be displayed at all times while on UTMB premises. The badge must be returned to UTMB when the employee leaves the contract or at the end of the contract.

5. Each vendor employee with access to UTMB confidential and/or sensitive information must be approved to access that information compliant with applicable IR Security Management Practice Standards.

6. Vendor personnel must report all security incidents directly to the Computer Incident Response Team (CIRT) at (409) 772-3838 or cirt@utmb.edu.

7. If vendor management is involved in UTMB incident management, the details must be specified in the contract.

8. Vendor must follow all applicable UTMB change management processes and procedures.

9. Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate UTMB management.

10. All vendor maintenance equipment on the UTMB network that connects to the outside world via the network, telephone line or leased line and all UTMB IR vendor accounts will remain disabled except when in use for authorized maintenance.

11. Vendor access must be uniquely identifiable, and password management must comply with the UTMB Password Management Practice Standard and Special Access Practice Standard. Vendor’s major work activities must be entered into a log and made available to UTMB management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, and deliverables.

12. Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and/or destroyed within 24 hours.

13. Upon termination of contract or at the request of UTMB, the vendor will destroy all UTMB information and provide written certification of that destruction within 24 hours.

14. Upon termination of contract or at the request of UTMB, the vendor must surrender all UTMB identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized UTMB management.

15. Vendors are required to comply with all Federal, State and other regulatory auditing requirements, including the auditing of the vendor’s work.

16. All software used by the vendor in providing service to UTMB must be properly inventoried and licensed.
20.0 Network Access
The UTMB network infrastructure is provided as a central utility for all users of UTMB Information Resources. It is important that the infrastructure, which includes cabling and the associated ‘active equipment’, continues to develop with sufficient flexibility to meet UTMB demands while remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

This chapter establishes the rules for the access and use of the network infrastructure. This includes issues of documentation and change control, as well as those of connectivity to other networks such as the Internet and extranets. These rules are necessary to preserve the integrity, availability, and confidentiality of UTMB information.

20.1 Network Access Implications
1. Configurations and set-up parameters on all hosts attached to the UTMB network must comply with UTMB IR Security Management Practice Standards.
2. Prior to being permitted to use computers connected to the UTMB network, all users must have their identity verified with a User ID and secret password (or by other means which provide equal or greater security) and are accountable for activities associated with such use.
3. UTMB reserves the right to audit the security measures in effect on these connected systems without prior warning.
4. UTMB reserves the right to immediately terminate network connections with systems not meeting such requirements.

20.2 Network Access Practice Standard
1. Users are permitted to use only those network addresses issued to them by UTMB IS.
2. All remote access to UTMB will be either through an approved modem pool or via an Internet Service Provider (ISP) using UTMB approved protocols.
3. Devices attached to the UTMB data network cannot have a modem.
4. Users must not extend or re-transmit network services (i.e., DNS, DHCP, dynamic routing, etc.) in any way. This means users must not install a router, switch, hub, or wireless access point to the UTMB network without UTMB IS Data Network approval or assistance.
5. Users are not permitted to alter network hardware or software that provides network services without UTMB IS Data Network approval.
6. Computer systems requiring network connectivity that are not owned or supported by UTMB must conform to UTMB IS Data Network Standards and IR Security Management Practice Standards.
7. Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, UTMB users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the UTMB network infrastructure.
8. All network components, including data closets, wiring and fiber, routers, switches, concentrators, and hubs, must be protected from unauthorized access.
9. Firewalls and other enterprise network security measures must be implemented to provide appropriate network security.
10. Multiple simultaneous on-line sessions are not permitted (i.e., one User ID equals one log-in session).
11. Computer Systems requiring network connectivity must use the following approved System Identification/Logon Banner: “The information system you are using is the property of or licensed to UTMB. For the integrity of the system and to comply with state and federal mandates, policy and practice standards govern its use. Please understand that there is no privacy in your use of this digital information system. For security and other reasons related to UTMB operations, activities on these systems are monitored and may be recorded by systems support personnel. Anyone using a UTMB information system consents to such monitoring. Pursuant to the Texas Administrative Code (Title I, Part 10, § 202.7), all UTMB information systems are solely for the use of authorized users. UTMB management or the appropriate law enforcement agency may be advised and be provided evidence of any individual using a UTMB information system without authority, in an unauthorized manner, for inappropriate activity, or to violate the law. Prior to accessing this information system you should be thoroughly familiar with UTMB’s policies and practice standards, accessible at http://cirt.utmb.edu/policies/policies.php. By using this information system, you acknowledge that you understand these issues and will comply with these policies.”

12. Connection to the UTMB network implies acceptance of the terms and conditions set forth in applicable IR Security Policies and Practice Standards.
21.0 Physical Access
Technical support staff, security administrators, system administrators and others may have Information Resource (IR) physical access requirements as part of their function. The granting, controlling and monitoring of the physical access to IR and IR facilities is extremely important to an overall security program. This chapter establishes rules for the physical securing of IR facilities and hardware.

21.1 Physical Access Implications
1. All mission critical computer and communications systems shall be physically located within the protected confines of a secured information resources facility.
2. Access to mission critical IR facilities shall be physically restricted, managed, and documented.
3. Workstations should be used in a manner that maximizes the security of the information contained therein, especially in high traffic areas.
4. Reviews of physical security measures for information resources shall be routinely conducted.

21.2 Physical Access Practice Standard
1. Access to IR facilities must be granted only to UTMB support personnel whose job responsibilities require access to that facility.
2. The process for granting access to IR facilities must include the approval of the manager responsible for the facility.
3. Requests for access must come from the applicable UTMB data/system owner.
4. Support personnel must not permit unknown or unauthorized persons to pass through doors, gates, and other entrances to restricted areas at the same time when authorized persons go through these entrances. (Where access is card controlled, each individual must use their own card to gain entry.)
5. All IR facilities that allow access to visitors will track visitor access with a sign in/out log.
6. Visitors must be escorted in access controlled areas of IR facilities.
7. Card access records and visitor logs for mission critical IR facilities must be kept a period of one year for review and audit purposes and must minimally contain sign-in date, time in, time out, UTMB badge number or company name, reason for visit (maintenance performed if applicable), printed name, signature, and accountable party who authorized entry.
8. The manager responsible for the IR facility must review physical access rights, access records and visitor logs for the facility on a periodic basis and remove access for individuals who no longer require access.
9. When an individual changes roles or separates from UTMB, all physical security access codes known by the individual must be deactivated or changed (i.e., the password entered on a cipher lock to get into the IR facility must be changed) and all access rights must be immediately disabled.
10. All individuals granted physical access to IR facilities shall abide by the recommended requirements outlined within this practice standard and shall not bypass or circumvent prescribed security measures.
11. Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.
12. All multi-user computer and communications equipment must be located in locked rooms to prevent tampering and unauthorized use.
13. If there has been no activity on a computer terminal, workstation, or microcomputer (PC) for ten (10) minutes, the system must automatically terminate the session or invoke a password enabled screensaver. Authentication to re-establish the session must occur after lockout due to idle time.

14. If the computer system to which they are connected, or which they are currently using, contains sensitive information or can be used to access other information resources on the UTMB network, users must not leave their microcomputer (PC), workstation, or terminal unattended without first logging-out or invoking a password enabled screensaver, unless physical access is otherwise assured (e.g., a locked private office).

15. All computer/magnetic storage media (i.e., hard disk, floppy disk, optical disk, magnetic tape/cartridge, etc.) containing sensitive information must be physically secured when not in use.

16. Prior to disposal or transfer of ownership, all stored data must be destroyed or permanently removed from any computer/magnetic storage media (i.e., hard disk, floppy disk, optical disk, magnetic tape/cartridge, etc.).

17. Information resources assigned to UTMB from another agency shall be protected in accordance with the conditions imposed by the providing agency. Conversely, information resources assigned from UTMB to another agency shall be protected in accordance with the conditions imposed by UTMB.

18. All physical security measures must comply with applicable statutes, standards, and regulations.
22.0 Wireless Access
Information Services (IS) is responsible for providing UTMB with a secure and reliable network infrastructure. With the anticipated proliferation of wireless technology and the potential likelihood of vulnerability and interoperability issues, it is essential that wireless services be coordinated to ensure an acceptable level of security and service for the institution.

This chapter outlines how wireless technologies are to be planned, deployed, managed, and monitored. In addition, this practice standard prohibits attachment or access to the UTMB network via unauthorized or non-compliant wireless communications mechanisms.

22.1 Wireless Access Implications
To ensure overall network integrity and security, only wireless equipment and services that meet this criteria and supporting IR Security Management Practice Standards are approved for connectivity to the UTMB network.

To ensure network reliability, IS Network and Security Services (NSS) will manage shared use of the wireless network that is consistent with shared use of the wired network.

As with any other UTMB IR, wireless services and equipment are subject to periodic audits and security reviews.

Pursuant to pertinent policy and practice standards, IS will, at its discretion, disable any unauthorized or non-compliant wireless equipment and services that it discovers on the UTMB network.

22.2 Wireless Access Practice Standard
1. Wireless services and equipment will be standardized and must conform to the 802.1x security model for authentication, encryption, and key management.
2. IS NSS will identify non-compliant wireless services and disable the equipment. (IS NSS will initially attempt to accomplish this via informing and involving appropriate administration within the business function; however, depending upon the circumstances and the perceived risk, the Information Resources Manager may determine that this action needs to be taken without that cognizance.)
3. Wireless services and standards will be centrally managed by IS; all related inquiries and issues should be directed to the IS Help Desk at extension 25200.
4. To prevent unauthorized access and easy viewing of data on the internal network, each wireless deployment must enable dynamic Wired Equivalent Privacy (WEP) and the creation of a per-user, per-session WEP key tied to the network logon (i.e., User IDs and passwords via UTMB-USERS-M).
5. All communications on the internal UTMB wireless network will be encrypted; however, users should assume that wireless services in remote locations such as hotels, conference centers, airports, cafes, and at home are not necessarily encrypted; and such remote access requires the use of a Virtual Private Network.
6. The SSID (service set identifier) for the access point (AP) hardware will be established, registered, configured, and maintained by IS NSS so that it precludes
default values. Broadcasting of the internal SSID by the AP must also be disabled. Furthermore, IS NSS will disable the AP from responding to probe-response requests.

7. Wireless APs must maintain a hardware address and physical location that is registered with, approved and maintained by IS NSS.

8. Users must not set up AP hardware in ad-hoc or stand-alone mode and communicate with each other without traversing an IS authorized AP.

9. Users must not extend their own privileges or use of the wireless device for any purpose (e.g., users must not set up workstations and laptops with wireless hardware to act as an AP and advertise wireless services).

10. Procedures for guest wireless access (i.e., a secondary wireless network providing temporary Internet access only) will be managed by IS NSS.

11. The NSS team will routinely scan the network to identify unauthorized devices. (As with any other IR connected to the UTMB network, this equipment is subject to removal from the network.)

12. Perimeter scans will be conducted periodically by the NSS team to determine the extent of radio frequency (RF) broadcast and contain emission within physical boundaries.

13. Physical security of wireless equipment must be maintained to provide adequate protection from theft or compromise (preferably APs are installed out of sight).

14. Wireless equipment and services are subject to the same policies and practice standards that govern all IR at UTMB including, but not limited to, anti-virus software, platform hardening, authentication mechanisms, timeouts, and encryption.

15. Security requirements must be addressed in all phases of the acquisition process and system management lifecycle.
23.0 Change Management
The Information Resources (IR) infrastructure at UTMB is continuously expanding and becoming more complex. As the interdependency between the users and IR infrastructure grows, the need for a strong change management process is essential.

From time to time each IR element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable IR infrastructure.

This chapter outlines how to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of IR.

23.1 Change Management Practice Standard
1. Every significant change to UTMB multi-user, production IR including operating systems, computing hardware, networks, and applications is subject to this Change Management Practice Standard.
2. All multi-user computer and communications systems used for production processing at UTMB must employ a formal change management procedure which is used to ensure that only authorized changes are made. The change management procedure must be used for all significant changes to software, hardware, communications networks, and related procedures. The change management procedure must also be used for changes made by third parties (i.e., vendors) and for changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms).
3. The change management procedure must address:
   a) Formally identifying, classifying, prioritizing and requesting changes.
   b) Identifying and deploying emergency changes.
   c) Assessing potential impacts of changes.
   d) Authorizing changes and exceptions.
   e) Testing changes.
   f) Change implementation and back-out planning.
   g) Documenting and tracking changes.
4. A formal change request must be submitted for all significant changes, both scheduled and unscheduled.
5. Each change, scheduled or unscheduled, must be reviewed by the system owner or assigned agent(s).
6. Each scheduled and unscheduled change request must receive formal approval before proceeding with the change.
7. All changes must be properly communicated to affected parties prior to change implementation to ensure that implementation reasonably minimizes potential business disruptions.
8. A change management log must be maintained for all changes. The log must contain, but is not limited to:

   a) Date of submission and date of change
   b) Owner and custodian contact information
   c) Nature of the change and potential impact of the change
   d) Indication of success or failure

9. All new or modified programs must be tested and approved by the appropriate user and either Information Services supervisors (if the program is centrally managed) or departmental supervisors (if the program is managed by a department or school).

10. All new or modified programs will be tested in a separate test environment (either logically or physically separate) where possible. Exceptions should be documented in the change request.

11. Copies of production data shall not be used for testing unless the data has been declassified or unless all persons involved in testing are authorized by the data owner to access the production data.

12. Approval documentation associated with each change must be retained for a period of three years to maintain necessary audit trails. Testing documentation, including test plans and test results supporting each change, must be retained for a period of one year.

13. All UTMB information systems must comply with an IR change management process that meets the standards as outlined above.
24.0 Backup and Data Recovery
Electronic backups are a business requirement to enable the recovery of data and applications in the event of natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

This Chapter establishes the rules for the backup and storage of electronic UTMB information.

24.1 Backup and Data Recovery Implications
1. All critical information and software resident on UTMB IR must be periodically backed-up with sufficient frequency to support documented contingency plans.
2. Mission critical data shall be backed up on a scheduled basis and stored offsite in a secure, environmentally safe, locked facility accessible only to authorized personnel.

24.2 Backup and Data Recovery Practice Standard
1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the owner.
2. Operational arrangements must be made to ensure that more than one person can access a computer and its associated backup files.
3. The backup and recovery process for each system must be documented and reviewed by April of each year (prior to hurricane season) by the owner.
4. Physical and administrative controls employed at offsite backup storage locations must meet or exceed access requirements of the original system, thus ensuring the confidentiality, integrity, and availability of the information stored.
5. A course of action must be implemented to verify the processing success of the UTMB electronic information backup. At the completion of each scheduled backup, logs must be checked and verified to ensure successful data backup has occurred.
6. Backups must be tested periodically to validate recoverability, based upon documented risk management decisions.
7. Signature cards held by the offsite backup storage vendor(s) or contractor(s) for access to UTMB backup media must be reviewed annually or when an authorized individual leaves UTMB.
8. Procedures between UTMB and the offsite backup storage vendor(s) or contractor(s) must be reviewed at least annually.
25.0 Reporting of Lost Information Resources and Data

IR devices with huge amounts of storage capacity are common today and are becoming increasingly popular with members of the UTMB community. This technology allows individuals to transport large amounts of data efficiently and gives them the ability to work from remote locations where connections to the UTMB network are not always available.

While this technology has great advantages, it also poses significant risks. In recent years, numerous reports of lost or stolen computing/storage devices containing confidential data have generated public concern.

While the loss of some computing equipment may have significant value, it does not compare to the potential cost associated with lost or stolen confidential and sensitive data which has not been properly reported. Failure to report the loss of controlled data could result in huge fines, embarrassment and loss of creditability to UTMB, far out weighing the monetary cost of a piece of equipment.

This chapter establishes procedures for reporting the loss of IR devices which may or may not contain confidential data.

25.1 Reporting of Lost Information Resources and Data Implications

Immediately report any lost/stolen information resources (laptops, PDA’s, removable media, etc.) to departmental management and to the UTMB Information Security Officer (ISO). The Information Security Officer will assist in determining if any UTMB sensitive or confidential may have been compromised. In addition, if the IR was to believed to have been stolen, the incident will have to be reported to the University Police.

25.2 Reporting of Lost Information Resources and Data Practice Standard

1. UTMB Employees, Staff and Faculty
   a) The loss or theft of removable media i.e., floppies, CD-ROMs DVDs, etc, containing sensitive/confidential information will be reported to the Information Security Officer.
   b) The unknown loss or suspected theft of UTMB-owned data that has been classified as confidential or sensitive will be reported to the Information Security Officer.
   c) Reports of IR equipment and/or data loss or theft will be submitted to the UTMB Computer Incident Response Team (UTMB-CIRT) utilizing the Lost/Stolen IR form that is located off the main menu of the UTMB-CIRT website. (http://cirt.utmb.edu) or by calling 409-772-3838.

2. UTMB Police
   a) Within 24 hours of being reported, the UTMB police will forward a copy of the police report involving the theft of IR related devices to the Information Security Officer.

3. UTMB Information Security Officer (ISO)
   a) Upon notification of a lost or stolen IR device which may contain sensitive/confidential data, the ISO will immediately notify the Information Resource Manager (IRM).
b) Upon notification of lost or stolen sensitive/confidential data, the ISO will activate the Computer Incident Response Team and initiate an investigation in an attempt to determine the type of data which may have been compromised, the means in which it was compromised, the extent of the compromise and its potential impact to UTMB.

c) The investigation will be concluded with the convening of an after-action meeting and a formal fact finding report being submitted to the IRM.

d) The confirmed loss or theft of any unencrypted device containing confidential or personally identifiable information will be immediately reported to the UTMB Office of Institutional Compliance, UT System Office of Institutional Compliance and the Texas Department of Information Resources.
26.0 Portable Computing
A portable computing device is any easily transportable device that is capable of storing and/or processing data. They include, but are not limited to: notebook computers, handheld computers, PDAs, pagers, smart phones, digital multimedia players and portable storage media (USB drives, flash drives, CD/CDR/DVD/Blueray disks etc.). Portable devices are becoming powerful and affordable. Their small size, functionality, and ease of use make them very desirable to personnel who need to be mobile while addressing the business of UTMB. However, the portability offered by these devices increases the security exposure to sensitive and confidential data exponentially.

This chapter establishes rules for the use of portable devices and their connection to the network. These rules are necessary to preserve the integrity, availability, and confidentiality of UTMB information.

26.1 Portable Computing Implications
1. Regarding Information Security, the user is expected to have a heightened awareness and take appropriate precautions while using portable devices to access UTMB IR.
2. Before connecting to the UTMB network, all computing devices must be preauthorized by appropriate management (i.e., accreditation).
3. To remain connected to the UTMB network, all platforms must comply with applicable baseline IR security policies and practice standards (i.e., certification).

26.2 Portable Computing Practice Standard
1. Only UTMB approved portable computing devices may be used to access UTMB Information Resources.
2. Portable computing devices must be password protected.
3. Sensitive UTMB data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive UTMB data must be encrypted in accordance with UTMB Practice Standard 1.2.8, Encryption Standards.
4. Data owners must provide explicit approval prior to sensitive UTMB data being stored on portable computing devices.
5. Sensitive UTMB data must not be transmitted via wireless to or from a portable computing device unless approved wireless transmission protocols, along with approved encryption techniques, are utilized.
6. All remote access (dial in services) to UTMB must be either through an approved modem pool or a Virtual Private Network connection via an Internet Service Provider (ISP).
7. If sensitive UTMB data is being stored on a portable computing device, users will not permit anyone else to use the portable device for any purpose.
8. When flying aboard commercial airlines, users must not check portable computing devices that contain sensitive UTMB information. The devices must remain in the possession of the traveler as hand luggage.
9. Portable computing devices must not contain a single (only) source of data. All critical data stored on portable devices must be a copy or backed up in accordance with Practice Standard 1.3.2, Backup/Data Recovery.
10. Non-UTMB computer systems that require network connectivity must conform to UTMB IS Standards.

11. Unattended portable computing devices must be physically secure. This means they must be locked in an office, in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system.

12. All lost, stolen or compromised devices must be reported to the Information Security Officer in accordance with Practice Standard 1.4.1, Reporting of Lost or Stolen Information Resources and Data.
27.0 Remote Access

The use of high speed cable and DSL services, as well as improved wireless (Wi-Fi) network technology have made the remote access of UTMB Information Resources (IR) a relatively simple process. Whether you are telecommuting or accessing email from a remote business site, as access is made more convenient, the requirements to provide this access in a business secure manner becomes more complicated. State and federal regulatory statutes require certain administrative, technical and physical security controls to be in place, verified and reported on. These controls are made more complicated when the user community is not centrally located and is potentially mobile.

This chapter provides requirements and guidelines to support the accessing of UTMB’s information resources from remote locations in accordance with established policy, regulatory requirements and best practices.

27.1 Remote Access Implications

1. All published policies and practice standards related to Information Resources apply to users connecting to UTMB remotely.
2. Remote locations include any place that a UTMB controlled first point of network contact cannot be established. These may include private homes, associated business locations and public access points.
3. Remote access methods may include dial-up lines, high-speed cable or DSL, site-to-site internet tunnel, leased line, or publicly accessible Wi-Fi access points.
4. Time duration limits on active and inactive connections will be enforced.

27.2 Remote Access Practice Standard

1. Anyone requiring remote access to the UTMB network is required to sign a non-disclosure agreement prior to being granted access. For non UTMB personnel, non-disclosure agreements are valid for one year from the date it was signed. Failure to renew the agreement will result in revocation of network access.
2. A UTMB domain user account with the necessary VPN access or an IS approved/generated “guest” user account is required to remotely access UTMB resources. These accounts will be used to access UTMB resources only by the persons to whom it was assigned.
3. Remote access is provided to specific UTMB resources for UTMB related business functions. Access will not be used as a jumping platform or pass-through to non-UTMB networks or systems.
4. Internet access via remote connection to UTMB networks is supported. All appropriate and incidental use practice standards apply to Internet access via remote connection to UTMB.
5. As a condition of gaining access to UTMB’s network, remote users must secure their own connected systems in a manner consistent with UTMB’s requirements.
6. UTMB IR users may only access the UTMB network through an institutionally established dedicated circuit, VPN or modem pool. Direct IR access methods (modem lines on individual IR systems) must be approved by IS and disconnected when not in use.
7. Remote users must maintain physical access controls to insure that only authorized users and appropriate uses of IR occur while remotely connected to UTMB networks.
8. Unless explicitly approved by the data owner, sensitive and/or confidential information will not be maintained on remote systems. In other words, a remote
system may access UTMB information as needed for appropriate use but not store or archive this information.

9. Remote users must report all security incidents directly to the Computer Incident Response Team (CIRT) at (409) 772-3838 or cirt@utmb.edu.

10. Remote users should be aware that an expectation of privacy DOES NOT extend to information generated, maintained, used or transmitted, or to UTMB network services accessed, while remotely connected to the UTMB network.
28.0 Encryption
Cryptography is the science of transforming data so that it is interpretable only by authorized persons. Data that is unencrypted is called plaintext. The process of disguising plaintext data is called encryption, and encrypted data is called ciphertext. The process of transforming ciphertext back to plaintext is called decryption. The Texas Administrative Code states that, "encryption techniques for storage and transmission of information shall be used based on documented security risk management decisions."

This chapter sets the minimum required standards for encrypting data that has been classified as “Confidential” by specific laws, policy or at the data owner’s request.

28.1 Encryption Implications
1. All confidential data sent over a public network will be encrypted using a minimum of 128 bit encryption.
2. All encryption methods must employ a key recovery so that data can be recovered in the event that an employee leaves UTMB or the employee’s key is lost or stolen.

28.2 Encryption Standards
1. If information that is considered to be confidential, such as PHI, SSN’s, credit card, or other data classified as confidential by the data owner, traverses an un-trusted public network, such as the Internet, then the data shall be encrypted with at least 128-bit encryption.
2. Options for encrypting data in transit include:
   a) Secure Socket Layers (SSL) – which use public key cryptography to encrypt Web application sessions between the user’s browser and the Web server. The Web server must have a certificate that has been generated by a Public Key Infrastructure (PKI). Users' browsers come pre-configured to “trust” the certificates of these well-known CAs, and browser client side certificates are not required.
   b) Virtual Private Networks (VPN) –use software and/or hardware to encrypt data between participating networks, or clients and networks. IP Security (IPSec) increasingly is becoming the standard for providing authentication and encryption between sites. IPSec authentication is based on the exchange of keys between communicating devices.
   c) Public Key Infrastructure (PKI) - A PKI (public key infrastructure) enables users of a basically unsecured public network, such as the Internet, to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.
   d) E-Mail – e-mail systems can support some types of encryption. Major mail clients can support encryption natively using Transport layer security (TLS) or S/MIME.
   e) Documents – The Microsoft Office Suite and the Adobe Portable Document Format have native encryption features that support algorithms up to 128 bits.
3. For Web servers using SSL, the certificate shall be purchased from a recognized Certificate Authority (CA) vendor. The Texas Department of Information Resources (DIR) has approved the following PKI service providers:
   a) Baltimore Technologies
b) Digital Signature Trust Company  
c) Entrust, Inc  
d) VeriSign, Inc

4. Options for encrypting data in transit include:
   a) Microsoft Encrypting File System (EFS) - Encrypting File System (EFS) is a 
      feature of Windows that allows you to store information on your hard disk in an 
      encrypted format. Encryption is the strongest protection that Windows provides to 
      help you keep your information secure.

5. Encryption keys shall be considered synonymous with UTMB’s most sensitive 
   category of information, and access to those keys must be restricted on a “need-to- 
   know” basis. The keys to be used for encryption must be generated by means that 
   are not easily reproducible by outside parties.

6. The following features shall be required when purchasing encryption products:
   a) The vendor must be financially stable.
   b) The product shall provide a way for management to recover encrypted files in the 
      event that an employee leaves UTMB or the employee’s key is lost or stolen.
   c) The product shall employ features that enhance system integrity, such as self- 
      testing, to the maximum degree possible.
29.0 Data Classification
Confidentiality, Integrity, Availability (CIA), are three words to be considered when protecting data.

Data classification is something that institutions have been struggling with for many years. Some data, such as PHI, financial, Student, and certain elements of personal information are clearly defined and regulated by statutes, laws and policy. Other types of data classification are not so clear; it is up to the data owner to review and apply the necessary classification to ensure that sensitivity and confidentiality are adequately maintained.

The purpose of this standard is to set minimum requirements so that data is properly and consistently classified and adequately protected throughout UTMB.

29.1 Data Classification Categories
Owners are required to classify all data stored and processed within their respective information resources and to apply the appropriate technical and administrative safeguards to adequately protect the data from unauthorized disclosure, access or manipulation. Data owners will also ensure that data is available when needed.

All UTMB data must be classified into one of the three categories:
- Confidential
- Sensitive
- Public

1. Confidential - Any data that UTMB is legally, morally and/or ethically obligated to protect, and where the unauthorized disclosure or manipulation would have a negative impact to UTMB, either financially, legally, or through the loss professional reputation. Access to confidential data will be limited to authorized users.

Examples of confidential information include but are not limited to the following:
   a) Patient Medical/Health Information (HIPAA)
   b) Student Records (FERPA)
   c) Donor/Alumni Information (UTS, Texas Identity Theft Enforcement and Protection Act, HIPAA)
   d) Research Information (Granting Agency Agreements, Other IRB Governance)
   e) Employee personal Information
   f) Access credentials
   g) Human Resource related issues
   h) Business/Vendor Data (Gramm-Leach-Bliley Act, Non-Disclosure agreement)
   i) Proprietary Information, i.e. data network maps, certain management information critical infrastructure detail.
   j) Any data classified as confidential by the data owner

2. Sensitive – Any data which requires integrity and continuous availability shall be maintained on an institutional server and guarded against unauthorized manipulation by limiting its modify/write permissions to authorized users. Examples of Sensitive information include; but are not limited to the following:
   a) Publicly accessible directory entries
   b) Library Catalog
c) Official web-site postings

d) Research data

e) Any data classified as sensitive by the data owner

3. Public – Any unofficial data that, if disclosed or manipulated would not negatively impact UTMB and the does not meet the requirements of the confidential or sensitive categories. Examples of public information include but are not limited to the following:

   a) Blogs
   b) Certain types of unofficial/non-business related emails
   c) News group posting
   d) Chat room posting
   e) Public domain data
   f) Any data classified as public by the data owner

The below matrix is designed to assist data owners with classification requirements and to provide them the appropriate controls to adequately protect sensitive and confidential data.

<table>
<thead>
<tr>
<th>Data Security Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need for Confidentiality</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>
29.2 Data Reclassification
With suitable justification, data classifications may be downgraded. Upon request by the Data Owner, the UTMB President and/or Office of Legal Affairs will review all data downgraded reclassification requests and approve as appropriate.

<table>
<thead>
<tr>
<th>Need for Confidentiality</th>
<th>Need for Data Integrity</th>
<th>Need for Availability</th>
<th>Category</th>
<th>Required Technical Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Public/Sensitive</td>
<td>Host data on an institutional server.</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Public</td>
<td>None</td>
</tr>
</tbody>
</table>

Data Security Matrix (cont.)
30.0 Security Training and Awareness

UTMB cannot protect the confidentiality, integrity, and availability of information in today’s highly networked systems environment without ensuring that all people involved in using and managing IT:

1. Understand their roles and responsibilities related to UTMB’s mission.
2. Understand UTMB’s information resource security policies, practice standards and procedures.
3. Have adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

It is generally understood by the IT security professional community that people are strongest and weakest links when it comes to securing systems and networks. The “people factor” - not technology - is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this “asset.” Security training and awareness program is paramount to ensuring that people understand their IT security responsibilities, policies and practice standards.

This chapter sets the minimum requirements for developing and maintaining a comprehensive training and awareness program.

30.1 Training and Awareness Responsibilities

The ISO, working with ISA’s, ISL and the CSAG will develop, publish and maintain a comprehensive information security training and awareness program that will adequately educate ISA’s, developers and end-users on how to properly use and protect the information resources entrusted to them.

30.2 End-user Training

1. Initial security training will be delivered at New Hire Orientation and will consist of an overview of the following topics:

   a) Acceptable use
   b) Data Classifications
   c) Privacy Statement
   d) Key Roles and Responsibilities
   e) Statutory Authority
   f) How You Can Help
   g) Failure to Comply (Individually)
   h) Failure to Comply (Institutionally)

2. Mandatory bi-annual end-user training will be delivered utilizing UTMB’s on-line compliance training system. The course will consist of the following topics:

   a) Acceptable use
   b) Data Classifications
   c) Privacy Statement
   d) Key Roles and Responsibilities
e) Statutory Authority
f) How You Can Help
g) Failure to Comply (Individually)
h) Failure to Comply (Institutionally)

30.3 Information Security Administrators and Program Developer Training
Information Security Administrators, security analysts and Program developers are required to obtain 8 hours of Continuing Professional Education (CPE) Credits with an emphasis on Information Security per year. CPE Credits can be obtained by the following:

1. Attend security related user groups
   a) ISSA Monthly Meeting
   b) Infragard Monthly Meetings
   c) UTInfoSec Quarterly conferences

2. Attend formal training with an emphasis on security
   a) Professional Development classes
   b) UTMB Sponsored security training

3. Publish Papers
   a) Publish a security related article in a local or national publication
   b) Read a security related book and submit a book report to the ISO for review.

4. Provide Security related presentations/training
   a) Prepare and present a security presentation to the ISA working group.

30.4 Information Security Awareness
The ISO, working with ISA’s, ISL and the CSAG will develop, maintain and deliver an Information Security Awareness program aimed at reminding UTMB personnel the importance of information security and provide tips on how to be compliant with published standards and policies. The ISO will, at a minimum:

1. Publish security awareness articles in the UTMB newsletter, Impact, at least quarterly.
2. Develop, publish and maintain an Information Security website with user awareness tips and other pertinent security related materials
3. Work with department chairs and directors to construct information security related emails that will be sent by the department to their respective staff.
4. On an annual basis, present security related material at IS sponsored technology forums.
5. Work with the Office of University Advancement; and during the month of October (National Information Security Awareness Month), produce security awareness literature and posters to be displayed in high traffic areas and on electronic billboards, i.e., TV’s, plasma screens, etc.
31.0 Information Security Councils, Groups and Meetings
The Information Security Officer will form, chair and attend various information security councils and meeting throughout UTMB and UT System. These councils are an important conduit to identify, discuss, and address high risk areas, potential non-compliant/problem areas, security enhancements etc.

1. At a minimum, the ISO will form and chair the following councils:
   a) Information Services Leadership Security Council
   b) Information Security Administrator Council
   c) Incident after action meeting

2. At a minimum, the ISO will attend and participate in the following councils:
   a) University of Texas Security Council
   b) Computer Services Advisory Group
   c) Information Services Leadership Council

31.1 Information Services Leadership Security Council
The Information Services Security Council is developed and chaired by the ISO and is comprised of the Information Resource Manager, IS directors, Internal Auditors and Compliance investigators. The role of the council is to address information security related issues that require leadership involvement. These issues can range from new technology recommendations to legislation concerns to policy review and approval.

1. At a minimum, the ISO is responsible for the following:
   a) Conduct meetings bi-monthly
   b) Set meeting agendas
   c) Facilitate the meeting
   d) Record and publish meeting minutes
   e) Address or assign actionable items

31.2 Information Security Administrator Council
The Information Security Administrator (ISA) Council is a critical component of the overall information security program. These individuals are considered the subject matter experts with regard to the security of critical information resources within their respective areas. ISA’s (council members) are appointed by the owners of critical data, usually their department head. ISA’s will work closely with the ISO to develop, publish, maintain and enhance the Information Security Program.

1. Department heads and/or owners of critical data, working with the ISO will:
   a) Appoint an Information Security Administrators for their respective area and/or system.

2. The ISO will:
   a) Form and chair an ISA council and conduct meetings on at least a quarterly basis.
   b) Set the agenda for the ISA council meeting.
   c) Form high risk advisory groups utilizing ISA’s.

3. The individual ISA will:
a) Implement all UTMB practice standards as they relate to his/her assigned systems.
b) Conduct annual information security risk assessments on assigned mission critical information resources.
c) Report general computing and security incidents to the ISO.
d) Act as a member of the ISA council.
e) Attend ISA council meetings.
f) Report at least annually to the ISO about the status and effectiveness of assigned information resources security controls.

4. The ISA council will:
   a) Assist the ISO in developing, implementing, and monitoring the Information Security Program.
   b) Establish reporting guidance, metrics, and timelines for ISOS to monitor effectiveness of security strategies in both the centralized and decentralized operations.
   c) Act as an advisory group with regards to identified high risk areas within the Information security program.
   d) Establish training requirements for individual ISA’s.

31.3 Incident After Action Meetings
The ISO will conduct an After Action Meeting for any incident involving information resources which significantly impacts UTMB’s network or productivity. After Action Meetings are important in that they allow response team members to share and document lessons learned and enhance processes and procedures, which in turn, will hopefully reduce the impact caused by future incidents.
32.0 Media Sanitization
One of the key elements in assuring that confidential information is not disclosed is media sanitization. Eventually all Information Resources will be retired and either disposed of, sold or if leased, transferred back to the leasing company. It is imperative that all devices capable of storing UTMB information be sanitized in a way that will make data recovery impossible.

This chapter sets the standard for properly sanitizing information resources prior to being transferred, sold or disposed.

32.1 Sale, Transfer and Disposal of Information Resources
Prior to the sale, transfer or disposal of UTMB owned information resources, system owners will take the appropriate steps to ensure all data is removed from any associated storage device.

1. Information Resources shall be sanitized using one of the following methods:
   a. *Clear* - One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable.
   
b. *Purge* - Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging.
      Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
   
c. *Destroy* - There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.
      *Disintegration, Pulverization, Melting, and Incineration* - These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

      *Shredding* - Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough so there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.
Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks must be destroyed by pulverizing, crosscut shredding or burning.

32.2 Record Keeping
Records of media sanitization will be maintained either electronically or by hard copy and will contain the following information:

1. Date
2. Description of the item(s) and serial number(s)
3. Inventory number(s)
4. Process and sanitization tools used to remove the data or method of destruction
5. Name and address of the organization the equipment was transferred to.

32.3 Media Sanitization Matrix

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Destroy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hand Held Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cell Phones</td>
<td>Manually delete all information, such as calls made, phone numbers; then perform a full manufacturer’s reset to reset the cell phone back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>Shred. Disintegrate. Pulverize. Incinerate by burning cell phones in a licensed incinerator.</td>
</tr>
<tr>
<td>Personal Digital Assistant (PDA)</td>
<td>Manually delete all information; then perform a manufacturer’s hard reset to reset the PDA to factory state. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear</td>
<td>Shred. Disintegrate. Pulverize. Incinerate. Incinerate PDA’s by burning in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>Networking Devices</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Routers (home, home office, enterprise)</td>
<td>Perform a full manufacturer’s reset to reset the router back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>Shred. Disintegrate. Pulverize. Incinerate. Incinerate routers by burning the routers in a licensed incinerator.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Destroy</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td><strong>Equipment</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Copy Machines</td>
<td>Perform a full manufacturer's reset to reset the copy machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.</td>
<td>Same as Clear.</td>
<td>Shred. Disintegrate. Pulverize. Incinerate. Incinerate copiers by burning in a licensed incinerator.</td>
</tr>
<tr>
<td>Fax Machines</td>
<td>Perform a full manufacturer's reset to reset the fax machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedures.</td>
<td>Same as Clear.</td>
<td>Shred. Disintegrate. Pulverize. Incinerate. Incinerate fax machines by burning the fax machines in a licensed incinerator.</td>
</tr>
<tr>
<td>Magnetic Disks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floppies</td>
<td>Overwrite media by using UTMB-approved software and validate the overwritten data.</td>
<td>Degauss in a UTMB-approved degausser.</td>
<td>Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator. Shred.</td>
</tr>
<tr>
<td>Media Type</td>
<td>Clear</td>
<td>Purge</td>
<td>Destroy</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------</td>
<td>----------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Magnetic Disks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zip Disks</td>
<td>Overwrite media by using UTMB-approved and validated overwriting technologies/methods/tools.</td>
<td>Degauss using a UTMB-approved degausser. <strong>Degaussing any current generation zip disks will render the disk permanently unusable.</strong></td>
<td>Incinerate disks and diskettes by burning the zip disks in a licensed incinerator. Shred.</td>
</tr>
<tr>
<td><strong>Magnetic Tapes</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reel and Cassette Format Magnetic Tapes</td>
<td>Clear magnetic tapes by either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data.</td>
<td>Degauss using an NSA/CSS-approved degausser.</td>
<td>Incinerate by burning the tapes in a licensed incinerator. Shred.</td>
</tr>
</tbody>
</table>
## Optical Disks

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Destroy</th>
</tr>
</thead>
</table>
| CDs/DVDs   | See Physical Destruction. | See Physical Destruction. | Destroy in order of recommendations: Remove the information bearing layers of CD media using a commercial optical disk grinding device. Incinerate optical disk media (reduce to ash) using a licensed facility. Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm²). **

** This is a current acceptable particle size. Any

## Memory

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Clear</th>
<th>Purge</th>
<th>Destroy</th>
</tr>
</thead>
</table>
Appendix (a) Security PracticeBulletins

<table>
<thead>
<tr>
<th>Number:</th>
<th>Security Practice Bulletin #1 (SPB-1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title:</td>
<td>Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices.</td>
</tr>
<tr>
<td>Date:</td>
<td>June 1, 2007</td>
</tr>
</tbody>
</table>
| Purpose:| The purpose of this University of Texas System Information Security Practice Bulletin is to:  
1) establish encryption as a requirement in the event that Confidential University Data are to be stored on a Portable Computing Device or a Non-University Owned Computing Device, and  
2) specify practices to ensure that there is a legitimate need before Confidential University Data are stored on a Portable Computing Device or a Non-University Owned Computing Device and that the Owner and User can ensure that encrypted data remain accessible in the event that an encryption key becomes lost or forgotten. |
| Definitions: | **Confidential Data:** Data maintained by state agencies and universities that are exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws. The controlling factor for Confidential Data is that of disclosure.  
**Confidential University Data:** Confidential Data maintained by an Entity of The University of Texas System.  
**Entity or Entities:** The University of Texas Institutions, System Administration, and UTIMCO.  
**Non-University Owned Computing Device:** Any device that is capable of receiving, transmitting, and/or storing electronic data and that is not owned or leased by or under the control of an Entity of The University of Texas System.  
**Owner:** The manager or agent responsible for the function that is supported by the resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared.  
**Portable Computing Device:** Any easily portable device that is capable of receiving, transmitting, and/or storing electronic data. This includes but is not limited to, notebook and tablet computers, handheld computers, personal digital assistants (PDAs), pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs, magnetic tapes, and similar storage devices.  
**User:** An individual, automated application or process that is authorized by the Owner to access the resource, in accordance with the Owner's procedures and rules. Has the responsibility to (1) use the resource only for the purpose specified by... |
### Definitions: Cont.

- The user is any person who has been authorized by the Owner of the information to read, enter, or update that information. The user is the single most effective control for providing adequate security.

### Rationale:

Experience demonstrates that many incidents involving unauthorized exposure of confidential data, such as social security numbers and personal health information, are the result of stolen or lost Portable Computing Devices and Non-University Owned Computing Devices. The best way to prevent these exposures is to avoid storing confidential data on these devices. However, in situations that require Confidential University Data be stored on such devices, use of encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

While encryption mitigates risk of unauthorized data exposure, encryption can result in loss of access to the data by authorized Users, therefore procedures to mitigate this risk are also necessary.

### Expectations:

1. As a general practice Confidential University Data are not to be copied to or stored on a Portable Computing Device or a Non-University Owned Computing Device.
2. Specific permission must be obtained from the data Owner before a User may store Confidential University Data on a Portable Computing Device or a Non-University Owned Computing Device. Such permission should be granted only upon demonstration of a business need and an assessment of the risk of unauthorized access to or loss of the data.
3. Any Confidential University Data stored on a Portable Computing Device or Non-University Owned Computing Device must be encrypted using products and/or methods approved by the Entity's Chief Information Security Officer (CISO or ISO).
4. Data Owners and Users of Portable Computing Devices and Non-University Owned Computing Devices containing Confidential University Data must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the Owner in the event that an encryption key becomes lost or forgotten. Various methods may be used to meet this requirement including:
   - Maintaining an accessible copy of the data on a server managed by the Entity, using procedures specified by the Entity.
   - Use of whole-disk encryption technologies that provide an authorized systems administrator access to the data in the event of a forgotten key.
   - Escrowing the encryption key with a trusted party designated by the data Owner or the Entity's Chief Information Security Officer.
   - Use of other methods approved by the Entity's Chief Information Security Officer.

### Exceptions:

Under certain circumstances the CISO of the Entity may grant or issue an exception to the use of encryption on Portable Computing Devices and Non-University Owned Computing Devices containing Confidential University Data.
Exceptions are of two types: 1) An exception may be granted to address the specific circumstances or business needs relating to an individual program or department. Requests for exceptions of this type should be in writing and should be initiated by the data Owner. 2) Broader exceptions may be issued to cover circumstances that span the Entity as a whole. Requests for exceptions of this type may come from any person, or such exceptions may be initiated by the CISO.

- All exceptions must be based on an assessment of business requirements weighed against the likelihood of an unauthorized exposure and the potential adverse consequences for individuals, other organizations, or the Entity were an exposure to occur.
- As a condition for granting an exception, the CISO of the Entity may require compensating controls be implemented to offset the risk created by the lack of encryption.
- Exceptions must be documented and must include the following elements:
  - A statement defining the nature and scope of the exception in terms of the data included and/or the class of devices included,
  - The rationale for granting the exception,
  - An expiration date for the exception,
  - A description of any compensating security measures that are to be required.

The signature of the CISO of the Entity, and in the case of an exception resulting from a data Owner request, the data Owner’s signature.
Appendix (b) - References

a) Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C, Rules §202.70 – §202.78
b) University of Texas System Policy 165 (UTS-165)
c) National Institute of Standards and Technology, Special Publications (800 Series)
d) UT Austin Data Classification Standard
e) The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
f) The Copyright Act of 1976, as amended
g) Family Educational Rights and Privacy Act of 1974 (FERPA)
h) Texas Penal Code, Chapter 33 (Texas Computer Crimes Statute)
i) Texas Penal Code, Chapter 33A (Telecommunications Crimes)
j) General Appropriations Act, Section 135 Article IX
k) Texas Government Code, Section 441 & Section 2054.001(a)(1)
l) Texas Ethics Commission Advisory Opinion No. 372
m) UTMB Records Retention Schedule
n) UTMB Portraits of Integrity
o) UTMB Computer Services Advisory Group
Appendix (c) - Definitions

802.1x: An authentication standard often used as an access control for wireless networks.


Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

Access Point (AP): Hardware or software that facilitates end user wireless connectivity to a wired network.

Ad-Hoc mode: A networking framework in which wireless devices communicate directly with one another without the use of an access point.

Back Door: Undocumented program code within the otherwise secure system used to gain access to the system through the 'opening' created and then exploit or attack the system. The back door usually leads to privileged access or a supervisor state and typically bypasses normal audit trails.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system failure.

Change: Any addition, modification or update, or removal of an Information Resource that can potentially impact the operation, stability, or reliability of an Entity network or computing environment.

Change Management: Process of controlling the communication, approval, implementation, and documentation of modifications to hardware and software to ensure that information resources are protected against improper modification before, during, and after system implementation.


Certificate Authority (CA): A company that has been established to manage the issuance and verification of certificates used in securing Internet data transfers (SSL and TSL certificates).

Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization (cirt@utmb.edu).

Computer Services Advisory Group: The Computing Standards Advisory Group was established in April, 2002 to provide an ongoing means of obtaining institutional input and feedback regarding telecommunications and desk-top services such as internet access, e-mail, security policies and desktop standards. The group is advisory to the
Members serve for a two-year period, with staggered membership rotation each year to ensure continuity.

The Computing Standards Advisory Group meets at least quarterly to: 1) review and recommend service level standards for UTMB network and telecommunications performance; 2) review and recommend UTMB desktop computing hardware and software standards; 3) Review and recommend UTMB computer security standards; and, 4) Identify, review, and recommend other UTMB computing standards that may be needed to ensure that UTMB attains its mission.

Confidential Data: Data maintained by state agencies and universities that is exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws. The controlling factor for confidential Data is that of disclosure.

Custodian: An individual or entity responsible for implementing Owner-defined controls and access to an Information Resource. Custodians include Information Security Administrators, institutional information technology/systems departments, vendors, and any third party acting as an agent of or otherwise on behalf of an Entity.

Data: Recorded data, regardless of form or media in which it may be recorded, which constitute the original data necessary to support the business of U. T. System or original observations and methods of a study and the analyses of such original data that are necessary to support Research activities and validate Research findings. Data may include but is not limited to: printed records, observations and notes; electronic data; video and audio records, photographs and negatives, etc.

Digital Data: The subset of Data (as defined above) that is transmitted by or maintained made available in, electronic media.

Digital Signature: electronic signature used to authenticate identity of the sender of the message or the signer of a document.

Electronic mail: Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system

Electronic Media: Any of the following: a) Electronic storage media including storage devices in computers (hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card; or b) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, intranet, and the physical movement of removable/transportable electronic storage media.

Email: Abbreviation for electronic mail.

Encryption: In cryptography, encryption is the process of transforming information (referred to as plaintext) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). In many contexts, the word
encryption also implicitly refers to the reverse process, decryption (e.g. “software for encryption” can typically also perform decryption), to make the encrypted information readable again (i.e. to make it unencrypted).

**Entity or Entities:** The U. T. Institutions, System Administration, and UTIMCO.

**Emergency Change:** when an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

**Extranet:** an intranet that is accessible or partially accessible to authorized users outside the organization.

**Firewall:** an access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture used to protect internal networks or network segments from unauthorized users or processes.

**Host:** a computer system that provides computer service for a number of users.

**Information:** Data organized, formatted and presented in a way that facilitates decision making. All information is data.

**Information Attack:** an attempt to bypass the physical or information security measures and controls protecting an IR. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

**Information Operations:** actions taken to affect adversary information and information systems while defending one’s own information and information systems.

**Information Resources (IR):** Any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

**Information Resources Manager (IRM):** The IRM is responsible for management of all of the institution’s information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state agency’s information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards and Guidelines to protect the Information Resources of the institution.
including both centralized and decentralized systems. If an agency does not designate an IRM, the title defaults to the institution’s president, and the president is responsible for adhering to the duties and requirements of an IRM.

**Information Security Officer (ISO):** responsible to the Information Resources Manager (IRM) for administering the information security functions within UTMB. The ISO is UTMB’s internal and external point of contact for all information security matters.

**Information Services (IS):** the name of the UTMB department responsible for computers, networking and data management.

**Information System:** An interconnected set of information resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, information, data, applications, communications and people.

**Integrity:** The accuracy and completeness of information and assets and the authenticity of transactions.

**Internet:** A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.

**Intranet:** a private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization’s intranet is usually protected from external access by a firewall.

**Intrusion:** the misuse or unauthorized access of a system and its data, which can either be initiated externally or internally.

**Intrusion Detection System:** an intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting break into or compromise a system.

**Lead Researcher:** The person engaged in the conduct of Research with primary responsibility for stewardship of Research Data on behalf of an Entity.

**Local Area Network (LAN):** a data communications network spanning limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates relatively low error rates.

**Malware:** short for malicious software, programs or files developed purpose of doing harm. Thus, malware includes computer viruses, worms, and Trojan horses.

**Mission Critical Information Resources:** Information Resources defined by an institution of higher education or state agency to be essential to the Entity’s function and which if made unavailable will inflict substantial harm to the Entity and the Entity’s ability
to meet its instructional, research, patient care, or public service missions. Mission Critical Information Resources include Confidential Data and Sensitive Data.

**Offsite Storage:** based on data criticality, offsite storage should be geographically different location from the UTMB campus that does share the same disaster threat event. Based on an assessment of the backed up, removing the backup media from the building and storing another secured location on the UTMB Campus may be appropriate.

**Owner:** The manager or agent responsible for the function that is supported by the resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared.

**Packet:** a piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.

**Password:** A string of characters used to verify or "authenticate" a person's identity.

**Personal Identifying Information:** Information that alone or in conjunction with other information identifies an individual, including an individual's name, social security number, date of birth, or government-issued identification number; mother’s maiden name; unique biometric data, including the individual’s fingerprint, voice print, and retina or iris image; unique electronic identification number, address, or routing code; and telecommunication access device.

**Platform:** Any device that is capable of storing, processing or transmitting digital data.

**Platform Hardening:** to secure the configuration parameters of a given system in such a manner as to mitigate known system vulnerabilities and help protect against unauthorized access and/or use.

**Portable Computing Devices:** Any easily portable device that is capable of receiving, transmitting, and/or storing data. These include, but are not limited to, notebook computers, handheld computers, PDAs (personal digital assistants), pagers, cell phones, Universal Serial Bus (USB) drives, memory cards, external hard drives, data disks, CDs, DVDs and similar storage devices.

**Remote Access:** Pertaining to communication with a data processing facility from a remote location or facility through a data link. One of the more common methods of providing this type of remote access is using a VPN.

**Research:** Systematic investigation designed to develop and contribute to knowledge and may include all stages of development, testing and evaluation.

**Researcher:** Lead Researchers, faculty, staff, graduate Students, postdoctoral fellows, residents and visiting/affiliated scientists who are engaged in or responsible for Research activities.
**SANS:** System Administration, Networking and Security Institute at Bethesda, Maryland.

**Scheduled Change:** Formal notification received, reviewed, and approved through the review process in advance of a change being made.

**Security Administrator:** the person charged with monitoring and implementing security controls and procedures for a system. Whereas each agency will have one Information Security Officer, technical management may designate a number of security administrators.

**Security Incident:** an event which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.

**Sensitive Data:** Information maintained by state agencies or institutions of higher education that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. It is information that requires a higher than normal assurance of accuracy and completeness as stated in Section 8.3 of this Policy. The controlling factor for sensitive data is that of integrity.

**Server:** A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

**Service Set Identifier (SSID):** a unique identifier (essentially a name that identifies a wireless network) attached to packets sent via wireless services that acts as a password (clear text) when a wireless device attempts to connect to the network.

**SMTP (Simple Mail Transfer Protocol):** a protocol for sending email messages between servers.

**Stand-alone mode:** an operational state in which wireless devices communicate directly with one another without the use of an access point.

**Strong Passwords:** A strong password is constructed so that another User or a "hacker" program cannot easily guess it. It is typically a minimum number of positions in length and contains a combination of alphabetic, numeric, or special characters.

**System Administrator:** person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls to enforce an organization’s security policy.

**Trojan Horse:** a malicious program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. It may also be used to locate password information or facilitate remote access, bundled within a free game or other utility.
Trusted Requestor (TR): employees who are trusted to make requests for authorized access to information resources on behalf of staff within their organizational jurisdiction.

Unscheduled Change: failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability.

User: An individual, automated application or process that is authorized by the Owner to access the resource, in accordance with the Owner's procedures and rules. Has the responsibility to (1) use the resource only for the purpose specified by the Owner, (2) comply with controls established by the Owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized by the Owner of the information to read, enter, or update that information. The user is the single most effective control for providing adequate security.

User ID: Refers to an individual’s unique system identifier.

UTMB Network: the collection of all wired and wireless access points across campus connected to the UTMB campus data network providing access to University computing resources and the Internet.

UTIMCO: The University of Texas Investment Management Company that manages U. T. System’s investment assets.

U. T. Institution: The University of Texas System’s nine academic teaching institutions and the six health centers.

U. T. System Administration: The central administrative offices that lead and serve the U. T. Institutions by undertaking certain central responsibilities that result in greater efficiency or higher quality than could be achieved by individual institutions or that fulfill legal requirements.

Vendor: Someone outside of U. T. System who exchanges goods or services for money or other consideration.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows Users to generate macros.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system Owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.
Appendix (d) - Acronyms

AP: Access Point
CA: Certificate Authority
CD: Compact Disk
CDROM: Compact Disk Read Only Memory
CD-RW: Compact Disk Read Write
CIA: Confidentiality, Integrity, Availability
CIRT: Computer Incident Response Team
CM: Change Management
CPE: Continuing Professional Education
CSAG: Computer Services Advisory Group
DHCP: Dynamic Host Configuration Protocol
DIR: Department of Information Resources
DMZ: Demilitarized Zone
DNS: Domain Name Service
DVD: Digital Video Disk
EFS: Encrypting File System
Email: Electronic Mail
FERPA: Family Educational Rights and Privacy Act
FTP: File Transfer Protocol
HIPAA: Health Insurance Portability and Accountability Act
HTTP: Hypertext Transport Protocol
ID: Identification
IDS: Intrusion Detection System
InfoSec: Information Security
IP: Internet Protocol
IPS: Intrusion Prevention System
IPSec: Internet Protocol Security
IR: Information Resources
IRB: Institutional Review Board
IRSP: Information Resource Security Program
IRM: Information Resource Manager
IS: Information Services
ISA: Information Security Administrator
ISL: Information Services Leadership
ISO: Information Security Officer
ISP: Internet Service Provider
LAN: Local Area Network
NDA: Non-Disclosure Agreement
NSS: Network and Security Services
OIS: Office of Information Security
PC: Personal Computer
PDA: Personal Digital Assistant
PIN: Personal Identification Number
PKI: Public Key Infrastructure
RF: Radio Frequency
SMIME: Secure/Multipurpose Internet Mail Extensions
SMTP: Simple Mail Transport Protocol
SPB: Security Practice Bulletin
SSID: Service Set Identifier
SSL: Secure Socket Layer
TAC: Texas Administrative Code
TCP: Transport Control Protocol
TLS: Transport Layer Security
USB: Universal Serial Bus
UT: University of Texas
UTMB: University of Texas Medical Branch
UTS: University of Texas System
VPN: Virtual Private Network
WEP: Wired Equivalent Privacy
Appendix (d) - Document Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Purpose</th>
<th>By Whom</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 1, 2008</td>
<td>Initial Release</td>
<td>President, CIO, ISO</td>
</tr>
</tbody>
</table>