Institutional Handbook of Operating Procedures Policy 02.19.06	
Section: General Administrative Policies and Service	Responsible Vice President: Senior Vice President & General Counsel
Subject: Computers/Automated Information Systems	Responsible Entity: Information Security

I. Title

Information Resources Security

II. Policy

The UTMB information resources infrastructure is an integrated network of computer resources which exists to support essential UTMB services and missions. This policy will address:

1. General
2. Confidentiality and Security of Data,
3. Acceptable Use of Email,
4. Acceptable Use of the Internet and Internet Access,
5. Incidental Use of Information Resources
6. Addition Requirements for Portable or Remote Computing
7. Password Management
8. Acquisition of hardware, software and peripherals

General

1. University Information Resources (IR) are provided for the purpose of conducting the business of the University of Texas Medical Branch at Galveston (UTMB or University). However, users are permitted to use UTMB IR for use that is incidental to the user's official duties for UTMB (Incidental Use) as permitted by this policy.
2. Users who are UTMB employees, including student employees, or who are otherwise serving as an agent or are working on behalf of UTMB have no expectation of privacy regarding any data they create, send, receive, or store on University owned computers, servers, or other information resources owned by, or held on behalf, of UTMB. UTMB may access and monitor its Information Resources for any purpose consistent with UTMB's duties and/or mission without notice.
3. Users have no expectation of privacy regarding any UTMB data residing on personally owned devices, regardless of why the data was placed on the personal device.
4. All users must comply with applicable UTMB Information Resources Use and Security policies and Practice Standards at all times.
5. Users shall not share their UTMB account(s), passwords, Personal Identification Numbers (PIN), security tokens (e.g., Two factor authentication tokens), or similar information or devices used for identification and authorization purposes. (Note: This is not applicable to the 'delegation' of access permissions; the intent is to prohibit the literal shared use of access privileges via the same User ID and password).
6. If there has been no activity on a computer terminal or workstation for 15 (fifteen) minutes, the system must automatically terminate the session or invoke a password enabled screensaver. Authentication to re-establish the session must occur after the lockout due to idle time.

7. Users shall never use UTMB IR to deprive access to individuals otherwise entitled to access University information, to circumvent UTMB computer security measures, or in any way that is contrary to the UTMB's mission(s) or applicable law.
8. Use of UTMB IR to intentionally access, create, store, or transmit sexually explicit materials is prohibited unless such use is required as part of the user's official duties as an employee of UTMB and is approved in writing by the President or a specific designee. Viewing, accessing, storing, or transmission of sexually explicit materials as incidental use is prohibited.
9. Users must clearly convey that the contents of any email messages or social media posts that are the result of incidental use are not provided on behalf of UTMB and do not express the opinion or position of UTMB. An example of an adequate disclaimer is: "The opinions expressed are my own, and not necessarily those of my employer, The University of Texas Medical Branch at Galveston."

Confidentiality & Security of Data

1. UTMB IR users are required to protect confidential digital data which, as defined by UTS 165, includes social security numbers, protected health information (PHI), confidential research data, digital data associated with an individual and/or digital data protected by law). Confidential digital data must be secured using a minimum of 128 AES encryption while at rest (electronic storage on a hard drive, digital or optical media), mobile (SMART Phone, tablets, flash drives or any other device capable of storing digital data) and in transit (via email or the Internet). Users must report any weaknesses in UTMB computer security and any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management, the UTMB Compliance Hotline at (800) 898-7679 or the Office of Information Security at (409) 772-3838. Incident reports can also be submitted online by clicking here.
2. Users shall access UTMB data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access. Users shall maintain all records containing University data in accordance with UTMB's Records Retention Policy and Records Management Guidelines.
3. Users shall not disclose confidential digital data except as permitted or required by law and only as part of their official University duties.
4. Whenever feasible, users shall store confidential digital data or other information essential to the mission of UTMB on a centrally managed server, rather than a local hard drive or portable device.
5. In cases when a user must create or store confidential or essential University data on a local hard drive or a portable device such as a laptop computer, tablet computer, or smart phone, the user must ensure the data is encrypted in accordance with UTMB practice standard 16.1, Data Encryption.
6. The following University data must be encrypted during transmission over an unsecured network, i.e., the Internet: Social Security Numbers; personally identifiable medical information and medical payment information; driver's license numbers and other government issued identification numbers; education records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other UTMB data about an individual that if disclosed would be likely to expose the individual to identity theft.
7. Email sent to and received from U.T. System and U. T. System institutions using UTMB provided email accounts is automatically encrypted. The Office of Information Security or other

applicable office, will provide tools and processes for users to send encrypted data over unsecured networks to and from other locations.

8. Users who store University data using commercial cloud services must use services provided or sanctioned by UTMB, rather than personally obtained cloud services. A list of sanctioned cloud services can be found at www.utmb.edu\infosec\sanctionedservices.pdf
9. Users must not use security programs or utilities except as such programs are required for the user to perform their official duties on behalf of the University.
10. All computers connecting to a University's network must run security software prescribed by the Office of Information Security as necessary to properly secure UTMB IR.
11. Devices determined by UTMB to lack required security software or to otherwise pose a threat to University IR may be immediately disconnected from a University network without notice.

Acceptable Use of Email

1. Emails sent or received by users in the course of conducting UTMB business are UTMB data that are subject to state records retention and security requirements.
2. Users are to use University provided email accounts, rather than personal email accounts, for conducting University business.
3. The following email activities are prohibited when using a University provided email account:
    - Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work related purpose.
    - Accessing the content of another User's email account except: 1) as part of an authorized investigation; 2) as part of an approved monitoring process; or 3) for other purposes specifically associated with the user's official duties on behalf of University.
    - Sending or forwarding any email that is suspected by the user to contain computer viruses.
    - Any incidental use prohibited by this policy.
    - Any use prohibited by applicable University or U.T. System policy.

Acceptable Use of the Internet or Internet Access

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 Office of Information Security. 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.

Incidental Use of Information Resources

1. Incidental use of UTMB IR must not interfere with user's performance of official UTMB business, result in direct costs to the UTMB, expose UTMB to unnecessary risks, or violate applicable laws or other UTMB policy.

2. Users must understand that they have no expectation of privacy in any personal information they store or transmit on a UTMB IR, including UTMB email accounts.
3. A user's incidental personal use of IR does not extend to the user's family members or others regardless of where the IR is physically located.
4. Incidental use to conduct or promote the user's outside employment or activities, including self-employment, is prohibited.
5. Incidental use for purposes of political lobbying or campaigning is prohibited.
6. Storage of any email messages, voice messages, files, or documents created as incidental use by a user must be nominal (less than 5% of a user's allocated mailbox space).
7. Files not related to UTMB business may not be stored on network file servers.
8. All electronic devices including personal computers, smart phones or other devices used to access, create or store UTMB data, including email, must be password protected and encrypted in accordance with University requirements, passwords must be changed whenever there is suspicion that the password has been compromised.
9. University data created or stored on User's personal computers, smart phones or other devices, or in databases that are not part of UTMB's information resources are subject to Texas Public Information Act (TPIA) requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to UTMB information resources.

Additional Requirements for Portable and Remote Computing

1. University issued mobile computing and digital storage devices must be encrypted.
2. Any personally owned computing devices on which Confidential UTMB data is stored or created must be encrypted.
3. University data created and/or stored on personal computers, other devices and/or non-UTMB databases should be transferred to UTMB IR as soon as feasible.
4. Unattended portable computers, smart phones and other computing devices must be physically secured.
5. All remote access to networks owned or managed by UTMB must be accomplished using a remote access method approved by the Office of Information Security, as applicable.

Password Management

1. University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), digital certificates, two factor authentication tokens, or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.
2. Each User is responsible for all activities conducted using the User's password or other credentials.

Acquisition of Hardware, Software and Peripherals

1. All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized UTMB officer and must be approved as to form by the Legal Department.
2. UTMB IR computer systems and/or associated equipment used for UTMB business that is conducted and managed outside of UTMB control must meet contractual requirements and be subject to monitoring.
3. External access to and from UTMB's IR must meet appropriate published UTMB security guidelines.

4. All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product.
5. Volume licensed software products (such as Microsoft products provided through the Library Bookstore) provided to students, staff and faculty are provided to facilitate UTMB's core functions and are for the use of the students, staff and faculty of UTMB Only. These licenses are invalid when the student, staff or faculty relationship with UTMB ends.
6. Personnel must abide by all license agreements and must not illegally copy licensed software. The Chief Information Officer, and the Office of Information Security, reserves the right to remove any unlicensed software from any computer system.
7. The Chief Information Officer, and the Office of Information Security, reserves the right to remove any non-business related software or files from any system.

III. Relevant Federal and State Statutes

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Family Educational Rights and Privacy Act of 1974 (FERPA)
Texas Administrative Code 1 TAC §202 (Information Security Standards)

IV. Relevant System Policies and Procedures

The University of Texas System, UTS165 – Information Resources Use and Security Policy

V. Related UTMB Policies and Procedures

IHOP - 02.01.03 - Release of Information under the Texas Public Information Act
IHOP - 02.01.04 - Records and Information Management
IHOP - 02.19.07 - Social Networking
IHOP - 03.01.03 - Telecommuting (Alternate Work Site)
IHOP - 06.02.00 – Maintaining Patient Confidentiality through the Appropriate Use and Disclosure of PHI
IHOP - 06.02.29 - De-Identification of PHI
IHOP - 02.19.09 - Digital Millennium Copyright Act

VI. Additional References

UTMB Employee Information Security Acknowledgment and Nondisclosure Agreement
Non-UTMB Employee Information Security Resources Security Acknowledgment and Non-Disclosure Agreement

VII. Dates Approved or Amended

Originated: 09/15/1995	
Reviewed with Changes	*Reviewed without Changes*
03/31/2012	10/16/2017

VII. Contact Information

Office of Information Security
(409) 772-3838