TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER™

eRAIDER REQUEST FORM

This form is to be used ONLY for business partners/visiting students requesting eRaider accounts. All TTUHSC employees/non-tech employees/adjunct must go through the ePaf process. Complete all of the requested fields.

APPLICANT SECTION

Name: _____ Title: _____

Department: _____ Phone: _____

Email Address: _____ Citizenship: _____ Date of Birth: _____

Role: ☐Vendor/Contractor ☐VisitingStudent ☐Other_____

Justification for Access: _____

_____

APPLICANT ACKNOWLEDGEMENT

I understand that the eRaider user account assigned to me at the request of the sponsor listed below is to be used only in connection with my assigned duties and may be revoked without notice. I agree to safeguard and not reveal my password nor allow anyone to use the account assigned to me, and understand that I am responsible for all actions, changes, and activity made with my eRaider account. I agree to comply with all TTUHSC Information Technology and Information Security policies. I have signed and agreed to TTUHSC's Confidentiality Agreement which includes Acceptable Use, and I am aware that any violation of these policies may lead to the immediate suspension of my computer privileges. I understand that unauthorized release of sensitive or restricted information is a breach of data security and may be cause for disciplinary action.

Signature: _____ Date: _____

DEPARTMENT CHAIR / HEAD / ADMINISTRATOR / SPONSOR SECTION

Name: _____ Title: _____

Department: _____ Phone: _____

Email Address: _____ Deactivate Account On: _____

The assigned duties of the applicant requires that he/she view, process, or otherwise have access to

☐ Protected Health Information (PHI) ☐ Personally Identifiable Information (PII)

☐ Student Records ☐ Other Confidential Information: _____

☐ No Confidential Information ☐ Research Data (include IRB and/or IACUC Number, if applicable):_____

Department Chair / Head / Administrator / Sponsor Acknowledgement

I agree to sponsor an eRaider user account for the applicant listed above. I understand that it is my responsibility to inform Information Technology when there is a change in the applicant's status to include but not be limited to dismissal, separation and transfer or otherwise no longer require access to the eRaider user account.

Signature: _____ Date: _____

INFORMATION SECURITY OFFICE SECTION

Signature: _____ Name: _____ Date: _____

☐ Confidentiality Agreement Returned / Signed ☐ Not Required ☐ APPROVED ☐ DENIED

PRIVACY OFFICE SECTION

Signature: _____ Name: _____ Date: _____

☐ HIPAA Training Received / Verified ☐ Not Required ☐ APPROVED ☐ DENIED

RESEARCH OFFICE SECTION

Signature: _____ Name: _____ Date: _____

☐ Processing Complete ☐ Not Required ☐ APPROVED ☐ DENIED

STUDENT AFFAIRS SECTION

Signature: _____ Name: _____ Date: _____

☐ Processing Complete ☐ Not Required ☐ APPROVED ☐ DENIED

Return completed form to ELP.Helpdesk@ttuhsc.edu

Ver.2017.07.07

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

CONFIDENTIALITY AGREEMENT

I acknowledge receipt of TTUHSC EP OP 52.09, Confidential Information, including Attachment A – Information Security Plan for Financial Information. As defined in this OP and in any other Texas Tech University Health Sciences Center El Paso (TTUHSC EP) policy or applicable federal or state law, I agree to hold as strictly confidential "Confidential Information" to which I have access to or obtain as an employee, student, volunteer, or any member of the TTUHSC EP workforce with whom the entity for which I work has a relationship (contractual or otherwise) involving the exchange of any sensitive information.

I understand the importance of maintaining the strict confidentiality, both in accessing and releasing Confidential Information, and I agree to comply with applicable policies, laws and regulations in performing my duties and responsibilities as these relate to Confidential Information. I understand I must comply with TTUHSC EP policies and procedures, including, but not limited to:

- HSC OP 52.09, *Confidential Information*
- HSC OP 52.02, *Privacy and Security of Health Information*
- HSC OP 77.13, *Student Education Records*

I agree to the following:

1. **Only** access Confidential Information as required to perform my duties and responsibilities at TTUHSC EP.

2. Handle all Confidential Information, **whether written, electronic, oral or in some other form,** in such a way that it shall not be revealed or disclosed to an unauthorized person. This includes but is not limited to any unauthorized **electronic social networking sites or means,** such as twitter, Facebook, etc.

3. **Not** disclose Confidential Information now, or at any time in the future, except as required to perform my job duties and responsibilities at TTUHSC EP and then only to the extent disclosure is consistent with the authorized purpose for which the information was obtained.

4. Will **never:**
   - Share/disclose passwords.
   - Use tools or techniques to break/exploit/disable security measures.

I further agree that on or before the date of separation of my employment or association with TTUHSC EP for any reason, I will return any and all Confidential Information in any form, including paper or electronic, in my possession, custody or control to the appropriate TTUHSC EP authority, and I will destroy any and all duplicate Confidential Information that may remain on my personal electronic device(s) or that is otherwise under my personal control.

I acknowledge and agree that any breach of this Confidentiality Agreement by me may result in disciplinary action which may include immediate termination of my employment or affiliation with TTUHSC EP; further, I understand that such a breach may result in legal action.

The terms of this Confidentiality Agreement are effective immediately and apply to all Confidential Information I have obtained in the past as well as future Confidential Information. I understand that this document will become a part of my permanent employment, volunteer, and/or student record.

_____ _____

Signature of Employee, Student, Volunteer or any member of TTUHSC EP workforce — Date

_____ _____

Print Name — Tech ID R#

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSC OP: 52.09, **Confidential Information**

PURPOSE: The purpose of this Health Sciences Center Operating Policy and Procedure (HSC OP) is to identify and protect information made confidential by law or TTUHSC EP policy.

REVIEW: This HSC OP will be reviewed on May 1 of each odd-numbered year (ONY) by the Assistant Vice President (AVP) of Compliance, Institutional Compliance Officer, the Executive Director for Human Resources, the AVP of Student Services, the Registrar, the Office of General Counsel, and the Assistant Vice President for Information Technology, CIO, then forwarded to the President by July 1.

POLICY/PROCEDURE:

1. **Definitions.**

   a. **CONFIDENTIAL INFORMATION** includes, but is not limited to, the following in any form or format:

      i. Financial information obtained in connection with the award and issuance of student loans which is protected under the Gramm-Leach-Bliley Act of 1999 (GLBA), 15 U.S.C. 6801, *et.seq*, implemented by 16 C.F.R. Part 314, and as may be amended.

      ii. Private and personally identifiable information obtained in the regular course of business, such as social security numbers, driver's license numbers, unpublished home addresses or phone numbers, personal account numbers, computer passwords and accounts, biometric information, educational records, financial information, credit card information, and protected health information.

      iii. Protected Health Information (PHI) has the same meaning as set forth in HSC OP 52.02, *Privacy and Security of Health Information*, and is information protected under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 C.F.R. Parts 160 *et. seq.,* Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. § 300jj *et. seq.*; 17901 *et. seq*., as may be amended.

      iv. Education Records has the same meaning as set forth in HSC OP 77.13, *Student Education Records*, and is information protected under the Family Educational Rights and Privacy Act of 1974 (FERPA), also known as the Buckley Amendment, 20 U.S.C. §1232g, as may be amended.

      v. Medical Committee and Medical Peer Review Committee records.

      vi. Any other information made confidential by federal or state law or TTUHSC EP policy including, but not limited to, research information, passwords, and access codes.

   b. **Students** refers to individuals who are or have been enrolled at TTUHSC EP.

   c. **Volunteers** are those individuals as defined in HSC OP 10.28, Volunteer Policy.

2. **General Policy.**

a. Anyone who has access to CONFIDENTIAL INFORMATION regarding TTUHSC EP employees, students, patients, affiliates, or any other information made confidential by TTUHSC EP policies or law, will take reasonable and necessary steps to maintain the confidentiality and privacy of such information.

b. Security, access to, and use and/or disclosure of protected health information (PHI) shall be governed by TTUHSC EP OP 52.02, Privacy and Security of Health Information.

c. Security, access to, and use and/or disclosure of certain financial information that is covered by the Gramm-Leach-Bliley Act of 1999, shall be governed by the TTUHSC EP INFORMATION SECURITY PLAN FOR FINANCIAL INFORMATION **(Attachment A)**.

d. Security, access to, and use and/or disclosure of student education records shall be governed by TTUHSC EP OP 77.13, Student Education Records. Access to student educational records is granted on the basis of a legitimate educational interest of the employee, student or volunteer.

e. Use of portable devices containing Confidential Information is subject to the requirements of TTUHSC EP IT Policy, Section 1.4.14, Portable Computing.

f. TTUHSC EP shall require execution of a CONFIDENTIALITY AGREEMENT **(Attachment B)** by employees, students, and volunteers at the start of employment or affiliation with TTUHSC EP, and upon request thereafter.

g. With the exception of those sections of this policy governed by other TTUHSC EP OPs, responsibility for implementing this policy shall rest with the Assistant Vice President of Compliance or Managing Director, Compliance for all employees; the respective Dean of each School; the Registrar; and the individuals designated by the Regional Dean for each regional campus.

i. Notice. Implementation shall include notifying employees, students and volunteers of this policy, and when appropriate, also notifying any other individuals designated by TTUHSC EP Information Security Plan for Financial Information, TTUHSC EP OP 56.01- *Use of Information Technology Resources*, TTUHSC EP OP 77.13, *Student Education Records,* and/or TTUHSC EP OP 52.02, *Privacy and Security of Health Information*.

ii. Procedures. Implementation shall include developing procedures to obtain a signed CONFIDENTIALITY AGREEMENT (**Attachment B**) from all individuals in an area of responsibility, and confirming that properly signed Confidentiality Agreements become part of an individual's employment, student, or volunteer record.

h. Written agreements between TTUHSC EP and other parties which involve use of and/or access to TTUHSC EP CONFIDENTIAL INFORMATION shall require the other parties to comply with TTUHSC EP policies and applicable Federal and state laws regarding confidentiality.

3. **Suggested Departmental Safeguards.**

Each School is responsible for establishing procedures necessary to implement this HSC OP. It is recommended that Schools utilize the following practice to protect CONFIDENTIAL INFORMATION:

a. **Printed Copies.**
Use. Records containing CONFIDENTIAL INFORMATION should be secured when not in use. For example, the records may be locked in a desk drawer or filing cabinet. Departments should review documents to confirm that ONLY the last four digits of the consumer credit card account number or social security number (where feasible) is readable before scanning or exporting paper documents into an electronic document management system.

Disposal. When necessary to discard documents containing CONFIDENTIAL INFORMATION, such documents should be disposed of by shredding, or using a comparable method designed to ensure privacy.

b. **Electronic Data.**
Persons with access to electronic data containing CONFIDENTIAL INFORMATION should take adequate steps to ensure that such information is not used by or made accessible or released to unauthorized sources. When it becomes necessary to erase files containing such information, the files should be erased completely so that the information contained in the files cannot be recovered by accessing undeleted programs.

c. **Review of Departmental Processes.**
Department personnel should be aware of the types of information being gathered within the department, such as sign-in sheets, forms of identification, retrieval and use of records and posting of information. Department personnel or the Information Owner should determine the necessity of obtaining private or personally identifiable information and revise processes where appropriate.

d. **Other.**
The effort to safeguard CONFIDENTIAL INFORMATION should not be limited to the above three categories. Changing technologies or laws may make additional safeguards necessary.

4. **Reporting Violations.**

a. Anyone who knows of or suspects a violation of this policy shall report that incident promptly to his/her immediate supervisor or the appropriate dean, the Registrar, and/or the AVP for Student Services, or in accordance with TTUHSC EP Information Security Plan for Financial Information, TTUHSC EP OP 56.01, Use of Information Technology Resources, TTUHSC EP OP 77.13, Student Education Records, and/or TTUHSC EP OP 52.02, Privacy and Security of Health Information, as applicable.

i. In cases where the immediate supervisor is the known or suspected violator, employees shall report the known or suspected violation to the next higher administrative supervisor.

ii. Reports may also be made through the anonymous Compliance Hotline at ethicspoint.com or through the toll-free number, 1-866-294-9352.

b. All information acquired in the investigation of any known or suspected violation of this policy shall be confidential unless disclosure is authorized or required by law.

5. **Disciplinary Action.**

a. **Employees.** Employees found to be in violation of this policy may be subject to legal action and may be disciplined in accordance with applicable policies including, but not limited to, the following:

i. Non-faculty employees. See TTUHSC EP OP 70.31, Standards of Conduct, Discipline, and Separation of Employees.

ii. Faculty employees. See HSC OP 60.01, Tenure and Promotion Policy.

b. **Students.** Policies and procedures concerning students are set forth in the Code of Professional and Academic Conduct in the TTUHSC EP Students Affairs Handbook.

c. **Volunteers.** Violation of this policy will result in loss of privileges, removal from institutional facilities, and possible legal action.

5. **Right to Change Policy.** TTUHSC EP reserves the right to interpret, change, modify, amend, or rescind this policy in whole or in part at any time without the consent of employees.

TTUHSC IT Policies

1.4.1 ACCEPTABLE USE

Conduct Yourself Responsibly

The use of TTUHSC I.T. resources may be temporarily or even permanently revoked at any time for abusive conduct. Such conduct includes placing unlawful information on a system, copyright violations, using abusive or otherwise objectionable language in either public or private messages, sending messages that are likely to result in the loss of recipients' work or systems, sending unauthorized messages to individuals, or any use that would cause congestion of the networks or otherwise interfere with the work of others.

Use of peer-to-peer programs on TTUHSC computers and/or network for downloading and/or uploading of illegal copies of copyrighted media is strictly prohibited. All students, faculty, and staff should remove these applications immediately from TTUHSC computers. Students, faculty, and staff who use their personally-owned computers to connect to the TTUHSC network must disable all peer-to-peer applications and services before connecting to the network. This includes direct connection or remote connection via PPP, VPN, or wireless accounts. Any computers using peer-to-peer applications on the TTUHSC network are subject to removal from the network until the application is removed or disabled.

Misuse of TTUHSC information resources is a violation of the policies contained herein and will result in disciplinary action in accordance with HSC OP's 70.31 and 77.05 and the Student Affairs Handbook .

Computing Ethics And User Responsibilities

Information technology resources at TTUHSC are owned by the State of Texas and administered by the Information Technology Division. All products created on Institutional property belong to the Institution. These products shall be considered "intellectual property" as defined by and managed according to Board of Regents Rules and Regulations, Chapter 10 - Intellectual Property Rights. TTUHSC will provide access to appropriate central and campus I.T. resources, and to their attached networks to all members of the TTUHSC community. Users are responsible for managing their use of I.T. resources and are accountable for their actions relating to information technology security.

General Principles

Users must abide by the following list of standards that have been established:

1. Report any weaknesses in TTUHSC computer security, any incidents of possible misuse, or violation of these policies to the appropriate I.T. management.
2. Access only information that is your own, that is publicly available, or to which you have been given authorized access. Users may use only the I.T. resources they are authorized to use and only for the purposes specified when their accounts were issued or permission to use the resources was granted.
3. For security reasons, protect your USER ID, password, and system from unauthorized use. Users who share their access with another individual shall be responsible and will be held accountable for **ALL** usage of their accounts.
4. Use only legal versions of copyrighted software in compliance with vendor license requirements. Users shall not transport software provided by TTUHSC to another computer site without prior authorization from the departmental administrator. To do so constitutes theft.
5. DO NOT attempt to circumvent or subvert system, network, destroy the integrity of computer-based information, or access controlled information on the TTUHSC network.
6. DO NOT install software/hardware for personal use on TTUHSC systems.
7. Sexually explicit material in any form is not allowed on TTUHSC systems. See Sexually Explicit Material section for more detailed guidelines.
8. Users must not unreasonably interfere with the fair use of I.T. resources by another. Examples of unreasonable interference include playing games, listening to or viewing streaming audio/video for recreation, intentionally misconfiguring or tampering with videoconferencing equipment, interfering with the scheduled use of a distance learning classroom by failing to promptly vacate the room at the end of a session, and intentionally running a program that attempts to violate the operational integrity of the TTUHSC network.
9. Users are prohibited from using the TTUHSC's systems or networks for personal or commercial gain, such as, selling access to your USER ID or to TTUHSC systems or networks, performing work for profit with TTUHSC resources in a manner not authorized by the TTUHSC, marketing/advertising, and/or personal business transactions with commercial organizations.
10. TTUHSC systems are not to be used for partisan political purposes, such as using electronic mail to circulate advertising for political

candidates or lobbying of public officials.

11. DO NOT use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, or by repeatedly sending unwanted mail.

The above list is by no means exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use.

Sexually Explicit Material

Users shall not view, retrieve, transmit, distribute, print, or save any electronic files that may be deemed sexually explicit on TTUHSC I.T. resources. This includes both visual and textual sexually explicit material as defined by Chapter 43 of the State of Texas Penal Code on Public Indecency. Exceptions are material used for scientific, medical, and/or educational purposes.

It is also illegal to use sexually explicit material to intimidate, persecute, or otherwise harass another individual. This is considered sexual harassment. For more detailed guidelines on sexual harassment, refer to HSC OP 70.14.

Do not open any emails which you believe to contain obscenity or pornography. If obscenity and/or pornography are received through email, there will be no disciplinary proceedings if the mail is deleted immediately. If the offending email originates from a TTU or TTUHSC email address, report the receipt of said material to the Assistant Vice President for Human Resources and/or the Information Security Officerimmediately. Reporting of such a violation will be held in the strictest confidence.