TEXAS TECH UNIVERSITY
HEALTH SCIENCES CENTER
EL PASO

eRaider Business Partner 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. Use another page if more room is required for answers.

APPLICANT SECTION

_____ _____
Name (First, Middle Name, Last) Title

_____ _____
Date of Birth (MM/DD/YYYY) Citizenship / Country of Access Origin

_____ _____
Email Address (Unique for Each Person) Phone

_____ _____
Vendor/Company/Institution Department

Role: [ ] Vendor/Contractor [ ] Visiting Student [ ] Other: _____

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 El Paso Information Technology and Information Security policies. I have signed and agreed to TTUHSC El Paso'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 privacy / security and may be cause for disciplinary action.

Printed Name: _____ Signature: _____ Date: _____

SPONSOR SECTION

_____ _____
Name Title

_____ _____
Department Office Phone

_____
Email Address

Justification for Access: _____

_____

Specify Application Access: _____

Deactivate Account On: _____

The assigned duties of the applicant require that he/she/they 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):_____

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. Quarterly compliance audits will be completed to review if access is still needed for the business partner account.

Printed Name: _____ Signature: _____ Date: _____

Research / Student Affairs OFFICE SECTION

Printed Name: _____ Signature: _____ Date: _____

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

CONFIDENTIALITY AGREEMENT

I acknowledge receipt of HSCEP OP 52.09, Confidential/Sensitive 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 El Paso) policy or applicable federal or state law, I agree to hold as strictly confidential "Confidential/Sensitive Information" to which I have access to or obtain as an employee, student, volunteer, or any member of the TTUHSC El Paso workforce with whom the entity for which I work has a relationship (contractual or otherwise) involving the exchange of any Confidential/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 El Paso policies and procedures, including, but not limited to:

- HSCEP OP 52.09, *Confidential Information*
- HSCEP OP 52.02, *Privacy and Security of Health Information*
- HSCEP OP 77.13, *Student Education Records*
- Texas Administrative Code Rule §202

I agree to the following:

1. Only access Confidential Information as required to perform my duties and responsibilities at TTUHSC El Paso.
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 El Paso and then only to the extent disclosure is consistent with the authorized purpose for which the information was obtained.
4. Agree to use the resource *only* for the purpose specified by the institution or information-owner as mandated by TAC 202
5. 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 El Paso 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 El Paso 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 El Paso; 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/Sensitive Information I have obtained in the past as well as future Confidential/Sensitive 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 El Paso workforce _____ Date _____

Print Name _____ Tech ID R# _____

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 52.09, Confidential Information

PURPOSE: The purpose of this Texas Tech University Health Sciences Center El Paso Operating Policy and Procedure (HSCEP OP) is to identify and protect information made confidential by law or TTUHSC El Paso policy.

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

POLICY/PROCEDURE:

I. **Definitions**

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

1) 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.

2) 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.

3) Protected Health Information (PHI) has the same meaning as set forth in HSCEP 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.

4) Education Records has the same meaning as set forth in HSCEP 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.

5) Medical Committee and Medical Peer Review Committee records.

6) Any other information made confidential by federal or state law or TTUHSC El Paso 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 El Paso.

C. **Volunteers** are those individuals as defined in HSCEP OP10.28, Volunteer Policy.

II. General Policy

A. Anyone who has access to CONFIDENTIAL INFORMATION regarding TTUHSC El Paso employees, students, patients, affiliates, or any other information made confidential by TTUHSC El Paso 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 HSCEP 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 El Paso 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 HSCEP 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.

1) Legitimate Educational Interest. A "University Official" has a "Legitimate Educational Interest" if the official is:
   - (1) Performing a task that is specified in his/her position description or responsibilities designated by contract or state law;
   - (2) Performing a task related to a Student's education;
   - (3) Performing a task related to the discipline of a Student; or,
   - (4) Providing a service or benefit relating to the Student or Student's family, such as health care, counseling, job placement, or financial aid.

E. Use of portable devices containing Confidential Information is subject to the requirements of HSCEP OP 56.01,

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

G. With the exception of those sections of this policy governed by other HSCEP OPs, responsibility for implementing this policy shall rest with the Assistant Vice President of Compliance or Institutional Compliance Officer for all employees; the respective Dean of each School; the Registrar.

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

2) 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 El Paso and other parties which involve use of and/or access to TTUHSC El Paso CONFIDENTIAL INFORMATION shall require the other parties to comply with TTUHSC El Paso policies regarding confidentiality.

III. Suggested Departmental Safeguards

Each School is responsible for establishing procedures necessary to implement this HSCEP 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 ofrecords 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, such as federal and state mandates that govern the confidentiality, integrity, and access.

IV. 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 Senior Director for Student Services, or in accordance with TTUHSC El Paso Information Security Plan for Financial Information, HSCEP OP 56.01, Use of InformationTechnology Resources, HSCEP OP 77.13, Student Education Records, and/or HSCEP OP 52.02, Privacy and Security of Health Information, as applicable.

1) 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.

2) Reports may also be made through the anonymous Fraud and Misconduct Line at www.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.

V. 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:

1) Non-faculty employees. See HSCEP OP 70.31, Standards of Conduct, Discipline, and Separation of Employees.

2) Faculty employees. See HSCEP 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 El Paso Students Affairs Handbook.

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

VI. **Right to Change Policy** TTUHSC El Paso 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.

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, **Acceptable Use of Information Technology Resources**

PURPOSE: The purpose of this Texas Tech University Health Siecnces Center El Paso (TTUHSC El Paso) Operating Policy and Procedure (HSCEP OP) is to provide policy requirements for the use of Information Technology (IT) resources and associated data within TTUHSC El Paso. This policy outlines general compliance instructions and responsibilities for the use of information technology resources. Detailed policy information and a comprehensive set of IT policies is located at the IT homepage under the policies link, which is adopted by reference in this HSCEP OP.

This policy governs the use of IT resources by students, faculty, staff and authorized users within TTUHSC El Paso.

REVIEW: This HSCEP OP will be reviewed in February of each odd-numbered year (ONY) by the chief information officer (CIO).

POLICY/PROCEDURE:

I. General

A. Information Resources (IR) procured with TTUHSC El Paso funds are owned by the State of Texas and administered by the IT Department. TTUHSC El Paso IR are provided for the express purpose of conducting the business of TTUHSC El Paso. However, incidental use of IR is permitted for official duties as permitted by this policy.

B. Users of state property and those working on behalf of the institution have no expectation of privacy regarding information created, sent, received, or stored on institution-owned computers, servers, or other information resources owned by, or held on behalf of TTUHSC El Paso.

C. Users have no expectation of privacy for institutional data residing on personally owned devices, regardless of why the data was placed on the personal device. TTUHSC El Paso may monitor its IR without notice.

D. TTUHSC El Paso has the right to disclose the contents of electronic files when required by legal purposes; audit purposes; or legitimate federal, state, local, or institutional purposes.

E. Users are responsible for managing their use of IR and are accountable for their actions relating to IT security policies and procedures and are required to comply with institutional IR use and security policies at all times.

F. TTUHSC El Paso may temporarily or permanently revoke access, privileges, and/or use of IR at any time for abusive conduct or policy violations.

G. Use of IR to deprive access to individuals otherwise entitled to access institutional information, to interfere with the fair use of IR by others, to circumvent institutional computer security measures; or, in any way that is contrary to the TTUHSC El Paso's mission(s) or applicable law is prohibited.

H. Incidental use must not interfere with the normal performance of an employee's job duties.

I. Use of TTUHSC El Paso 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 and is approved in writing by the president or a specific designee. Viewing, access to, storage or transmission of sexually explicit materials as incidental use is prohibited.

J. All messages published as representative of TTUHSC El Paso must be approved by TTUHSC El Paso prior to public communication.

K. Users are required to report misuse of IR or violations of this policy to the TTUHSC El Paso information security officer (ISO).

L. All products and information created on Institutional property belong to the institution. These products shall be considered "intellectual property" as defined by the Board of Regents Rules and Regulations, Chapter 10-Intellectual Property Rights.

II. Privileged Users

A. All personnel with elevated privileges pose a higher risk to the institution than a standard user. As such, privileged users have greater responsibilities to ensure the secure operation of any TTUHSC El Paso system, and are held to a higher standard in regards to disciplinary action.

III. Confidentiality and Security of Data

A. Users may use only the IR to which they have been given authorized access and only for the capacity to conduct official business for which the user is employed.

B. Users must not attempt to access any data or programs for which they do not have authorization or explicit consent to access. Access only information that is your own, that is publicly available, or to which you have been given authorized access.

C. Users must not disclose or share confidential information, except as required by law, authorized by official duties, and with formal agreements that ensure third parties will adequately protect it.

D. Whenever feasible, users shall store confidential information or other information essential to the mission of TTUHSC El Paso on a centrally managed server, rather than a local hard drive or portable device.

E. Users should not store confidential data on mobile devices without proper authorization; however, in cases when a user must create or store confidential or essential information on a portable device such as a laptop computer, tablet computer, or, smart phone, the user must ensure the data is encrypted in accordance with applicable information security data handling requirements. The same security requirements apply to storage on local hard drives as well.

F. Users must not transport, transfer, email, remotely access, or download non-public information, unless such action is explicitly permitted by the manager or owner of such information.

G. Users are responsible for understanding TTUHSC El Paso data handling requirements, and ensuring their data handling and usage is in compliance at all times.

H. Email sent to and received from institutionally provided email accounts is automatically encrypted in transit. The IT Department will provide tools and processes for users to send encrypted data over unsecured networks to and from other locations.

I. Users must not Intentionally acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data that includes information subject to the Privacy Act, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

J. Any computers on the TTUHSC El Paso network using unapproved peer-to-peer applications, mallicous applications, or software that does not agree with the institution's mission and vision, are subject to removal from the network until the application is removed or disabled.

K. Students, faculty, and staff must not use the guest wireless if they use their personally owned computers to connect to the TTUHSC El Paso network. Non-TTUHSC El Paso devices that connect to the TTUHSC El Paso guest network may be disconnected without notice by the ISO.

L. All remote access to networks owned or managed by TTUHSC El Paso must be accomplished using a remote access method approved by IT Security and comply with IT Security policies.

M. All computers connecting to a TTUHSC El Paso network remotely, must run security software approved by the Information Security Officer to properly secure Institutional Resources.

N. Users who store institutional Data using commercial cloud services must use only those services provided or sanctioned by TTUHSC El Paso, rather than personally obtained cloud services.

O. A user must not download, install, modify software or run security programs or utilities that reveal or exploit weaknesses in the security of a system unless the individual user has explicit written consent from the institution's ISO.

P. Users must not use security programs or utilities except those programs that are required to perform their official duties on behalf of institution, or those that information security requires to be installed in order to access the TTUHSC El Paso network and IR.

Q. Devices lacking required security software or otherwise posing a threat to IR and the institution, may be immediately disconnected from the network without notice.

R. Intentionally running a program that attempts to violate the operational integrity of the TTUHSC El Paso network or intentionally circumvent or disrupt information security in any way is prohibited.

IV. Email

A. Use of organization-provided IT resources for personal commercial purposes, in support of "for-profit" activities or in support of other outside employment or business activity is prohibited.

B. Emails sent or received in the course of conducting institutional business are subject to state records retention and security requirements.

C. Users are to use institutional provided email accounts, rather than personal email accounts, for conducting official business.

D. The following email activities are prohibited when using an institutional provided email account:

1. Sending an email under another individual's name or email address,

2. 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 TTUHSC El Paso.

3. Sending or forwarding any email that is unauthorized mass mailing or suspected by the user to contain computer viruses.

4. Forwarding your TTUHSC El Paso email to your personal email account, or creating rules to automatically forward emails to a personal account or cloud storage.

5. Copying institutional emails to a personal device.

E. Any incidental use prohibited by this policy.

V. Incidental Use of Information Resources

A. Incidental use of IR must not interfere with user's performance of official business, result in direct or indirect costs to TTUHSC El Paso, expose the institution to unnecessary risks, or violate applicable laws or other Institutional policy.

B. Users must understand that they have no expectation of privacy in any personal information stored or created on an IR.

C. Incidental personal use of information resources does not extend to a user's family members or other acquaintances regardless of physical location. Employees and students must not allow family members or other non-employees to access TTUHSC El Paso IR.

D. Incidental use to conduct or promote the user's outside employment, self-employment, outside fundraising, endorsing any product or service, for partisan political purpose, lobbying, or campaigning is prohibited.

E. Using institutional IR to store personal email messages, voice messages, files, and documents may result in removal without notice or consent.

F. All messages, files, and documents— including personal messages, files, and documents— located on institutional IR are owned by the institution and may be subject to open records requests and may be accessed in accordance with this policy.

G. Files not related to System business may not be stored on network file servers.

VI. Portable and Remote Computing

A. All electronic devices including personal computers, smart phones or other devices used to access, create or store IR must be password protected in accordance with information security requirements.

B. Data created or stored on user's personal computers, smart phones or other devices, or in data bases that are not part of TTUHSC El Paso's IR are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to institutional information resources.

C. Institution-owned mobile computing devices must be encrypted.

D. Any personally owned computing devices on which non-public institutional data is stored or created must be encrypted.

E. Institutional data created and/or stored on personal computers, other devices and/or non-institutional data bases should be transferred to institution-owned IR as soon as feasible.

F. Unattended portable computers, smart phones and other computing devices must be physically secured. Methods to secure institutional resources include but are not limited to:

1. Logging off or locking systems when leaving them unattended,

2. Securing sensitive information (on paper and in electronic formats) when left unattended, and

3. Keeping sensitive information out of sight when visitors are present.

VII. Authentication Management

A. Passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone. All authentication mechanisms must be approved by TTUHSC El Paso IT Security.

B. Each User is responsible for all activities conducted with the user's authentication credentials.

VIII. Disciplinary Repercussions/Sanctions

A. Misuse of TTUHSC El Paso IR is a violation of the policies contained herein and will result in disciplinary action in accordance with HSCEP OP's 70.31 and 77.05 as well as the Student Affairs Handbook. Users of IR are also subject to 56.50 IT Sanctions policy (SN), for failure to adhere to IT Security policies and procedures.

All other IT Policies can be found at https://elpaso.ttuhsc.edu/it/policies/