

Non-Employee Personnel UIN Processing Checklist

(Independent Contractors, Clinical Non-Paid Personnel, etc)



HEALTH

Below you will find a check list for all the information needed before we are able to begin to process your request. All documents must be submitted to Laserfiche under TAMHSC\9.0 In-Boxes\VPS/NonPaidPersonnel/Academic Form Dropoff Folder for review and approval. Please be aware you may be asked to provide additional information during this process. If you have questions, please contact TAMH Compliance at (979) 436-9251 or by email to compliance@health.tamu.edu.

Component/Department Information

Component: _____ Department/Center _____

Department Contact: _____ Email: _____

Title: _____ Phone: _____

Non-Employee Information

Full Name: _____

Requested Start Date: _____ End Date: _____

Mandatory Items

- UIN Issue Certification Form
- Copy of Identity Verification Documents *(Driver's license, passport, birth certificate, etc.)*
- Background Check Authorization Form and Visual Compliance Screening Form
- Waiver, Indemnification and Medical Treatment Authorization & Consent Form
(Be sure to fill in all blanks with information specific to the individuals role and activities)

- HSC Data Use and Confidentiality Agreement Form
- HSC Computing Account Request *(To be completed on-line in HSC-ID for access)*
- HSC Training Needs Assessment Form
- Other _____

Departure Process

- Completion of the on-line [Notification of Resignation and Termination](#) form is required at the end of the term.

Subject:

Request Date:

Division of Information Technology NetID Account Request



Instructions: This form is used by Texas A&M departments and affiliate organizations to request a NetID account for personnel 1) who must have a NetID account to access authorized university information resources; and 2) who are not affiliated with any Texas A&M NetID Identity Management System Registration Authority. All information should be typed except for signatures and initials.

Submit form to: Division of Information Technology Identity & Access Management tamiam@tamu.edu If requesting VPN access, also send a copy of form to vpn-review@tamu.edu	Need Help? Division of Information Technology Help Desk Central helpdesk@tamu.edu
--	---

State law requires that you be informed of the following: (1) you are entitled to request to be informed about the information about yourself collected by use of this form (with a few exceptions as provided by law); (2) you are entitled to receive and review that information; and (3) you are entitled to have the information corrected at no charge to you.

Subject Information:

Universal Identification Number (UIN):

A UIN is required to create an entry for the Subject in the NetID Identity Management System.

- 1 Subject already has UIN. Enter UIN here ► _____
- 2 Subject's UIN needs to be created.

Name as shown on Subject's identity document:

First Name: _____

Middle Name: _____

Last Name: _____

Suffix: _____

Maiden Name: _____

Date of Birth (month dd, yyyy): _____

Gender: Male Female

Country of Citizenship: _____

U.S. Permanent Resident

Contact Information: Email Address: _____ Phone Number: _____

Organizational Unit Contact for this Request:

The contact must be a full-time Texas A&M University System faculty or staff employee. The contact also serves as the account sponsor.

Full Name: _____

UIN: _____ Title: _____

Dept: _____

Texas A&M System Member Institution: _____

Phone Number: _____ Email Address: _____

Request Date: _____

Subject:

Request Date:

Subject's Relationship with Sponsoring Organizational Unit:

If **not** an onboarding new employee, provide the following information:

Enter affiliation start date here (month dd, yyyy) ▶ _____

Enter affiliation expiration date here (month dd, yyyy) ▶ _____

Enter external employer organization name here ▶ _____

Enter external employer city, state, province, country here ▶ _____

Check one of the following ten options that best describes the type of relationship the Subject has with the Sponsoring Organizational Unit.

1 Onboarding **new employee**.

Enter hire date here (month dd, yyyy) ▶ _____

Position Type: Faculty Staff Graduate Assistant Student Worker

2 **Adjunct Faculty**

3 **Graduate Faculty/serving on graduate student committee**

4 **Visiting scholar/Unpaid research intern (Please provide a copy of the signed SVS or AG-713 with the account request.)**

5 **Remote research collaborator (Please provide a copy of the signed SVS or AG-713 with the account request.)**

6 **Medical Resident/Intern/Practicum student**

7 **Continuing education student/Research Experiences for Undergraduates (REU) student**

8 **Member of an affiliated organization or group:**

Description of affiliation ▶ _____

Organization/Group:

ROTC The Association of Former Students 12th Man Foundation Board of Regents

Texas A&M Mexico Office Texas A&M Soltis Center Institute of Nautical Archeology

Veterans program Veterinary Medicine, clinical trainee program Texas A&M Medical Library

Division of Research Advisory Board Texas A&M Bookstore

Easterwood Airport

9 **Contractor, vendor or temp agency employee – person has contract with TAMUS and is being paid for services**

10 **Other:** Description of affiliation ▶ _____

Business Reason for NetID Account ▶ _____

Subject:

Request Date:

Subject IT Services:

Affiliated personnel are not eligible for some IT Services by default. If any of the below services are required, check them and enter justification.

VPN access

Please provide a business need for enabling this service.

@tamu.edu email

Please provide a business need for enabling this service.

TAMU Gmail account

Please provide a business need for enabling this service.

Subject:

Request Date:

Texas A&M NetID Identity Management System Statement of Responsibility

- You certify the Subject cannot perform necessary business for the university without a Texas A&M NetID account.
- You certify you have entered accurate identity and affiliation information for the Subject.
- If the Subject's relationship with the organizational unit ends prior to the stated expiration date, you will inform the Division of Information Technology via email at tamiam@tamu.edu.
- You certify you have obtained all needed approvals for this access.
 - If an adjunct faculty member, Dean of Faculties has been informed.
 - If a graduate faculty member, Office of Graduate Studies has been informed.
 - If a visiting scholar or remote research collaborator, all requirements of SAP 15.99.99.M0.01 Visiting Scholars Not Involved in an Employee/Employer Relationship with Texas A&M University and SAP 15.02.99.M1 Export Controls have been met and all necessary approvals from the Office of Vice President for Research and Graduate Studies have been obtained.
 - For a vendor or contractor, all necessary approvals from the Department of Contract Administration have been obtained.
- You certify you have informed the Subject of all Information Resource Acceptable Use policies and procedures as outlined in SAP 29.01.03.M0.02.
- You understand that violation of this agreement may result in disciplinary action, up to and including termination of employment.

The agreement is bound by the University FERPA Policy and University Acceptable Use Guidelines

I HAVE READ, UNDERSTOOD AND AGREED TO THE ABOVE TERMS.

Organizational Unit Contact.

Printed (Typed) Name

X _____
Signature

Date Signed

Unit Head or Designee or Unit's HR Liaison.

Printed (Typed) Name

X _____
Signature

Date Signed



Data Use and Confidentiality Agreement Access to Technology and Information Resources

Access to Texas A&M Health Science Center data and information, and access to IT accounts, systems, and applications, is based on your need for access and your assent to use that access appropriately. These services are integral to the operation of the university, and security and privacy laws and other institutional policies protect much of the information.

Therefore, before you can be granted access, you must read and agree to follow these acceptable usage standards, and must accept responsibility to preserve the security and confidentiality of information that you access, in any form, including oral, print, or electronic formats.

Although these general provisions apply to all Health Science Center information and IT accounts, systems, and applications, please be aware that managers of certain services or information types may require you to complete additional agreements and/or training.

Usage responsibilities:

The following points detail your responsibilities as you access, use, or handle information or information technology (IT) at Texas A&M Health Science Center.

Secure Usage

You agree to:

- **Never share your account password(s) or passphrase(s) with anyone.**
- Select strong password(s) and passphrase(s).
- Be mindful that different computer systems and applications provide different levels of protection for information, and seek advice on supplemental security measures, if necessary. For example, a mobile laptop provides inherently less protection than a desktop computer in a locked office. Therefore, the level of protection provided to information accessed or stored using a laptop is to be supplemented by using additional safeguards such as encryption technology, enhancing physical security, restricting file permissions, etc.
- Respect the university's information and system security procedures (i.e., never attempt to circumvent or "go around" security processes).
- Maintain information in a secure manner to prevent access, viewing, or printing by unauthorized individuals.
- Secure unattended devices (e.g., log off, lock, or otherwise make inaccessible), even if you will only be away from the computer or device for a moment.
- Store Restricted and Critical data securely (e.g., on secure servers, in locked file cabinets, etc.).
- Securely dispose of Restricted and Critical information (e.g., by shredding, disk wiping, physical destruction, etc.).
- Never copy and/or store Restricted or Critical data outside of institutional systems (e.g., on desktop workstations, laptops, USB drives, personally owned computers, etc.) without proper approval from the senior executive officer of the department and only in cases where it is absolutely necessary for the operation of the department.
- Take appropriate steps to secure information (e.g., password protection, encryption, etc.) on mobile storage devices (e.g., laptops, USB drives, cell phones, etc.).
- Ensure, in the rare cases where Critical data has been approved for use and storage outside of institutional systems, that the data are appropriately encrypted, especially on mobile storage devices (e.g., laptops, cell phones, USB drives, CD-ROMs).
- Ensure, in the rare cases where it is necessary to email Critical or Confidential data, that the data are sent to the correct recipient and only via encrypted email methods.
- All PHI stored on electronic devices will be de-identified where applicable.



Legal Usage

You agree to:

- Use information and resources for legal purposes only.
- Respect and comply with all copyrights and license agreements.
- Never use your access to information or devices to harass, libel, or defame others.
- Never damage equipment, software, or data belonging to others.
- Never make unauthorized use of computer accounts, access codes, or devices.
- Never monitor or disrupt the communications of others, except in the legitimate scope of your assigned duties.
- Abide by applicable laws and policies with respect to access to, use, disclosure, and/or disposal of information.

Applicable laws and policies include but are not limited to:

- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act (FERPA)
- TAMHSC rules and policies (<http://www.tamhsc.edu/facultystaff/rules/>)

Ethical Usage

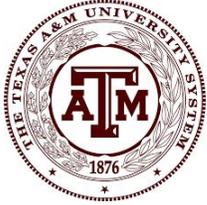
You agree to:

- Access institutional information only in the conduct of business and in ways consistent with furthering the mission of education, research, and public service.
- Use only the information needed to perform assigned or authorized duties.
- Never access any institutional information to satisfy your personal curiosity.
- Use information and IT in ways that foster the high ethical standards of the university.
- Never use information or IT to engage in academic, personal, or research misconduct.
- Never access or use institutional information (including public directory information) for your own personal gain or profit, or the personal gain or profit of others, without appropriate authorization.
- Respect the confidentiality and privacy of individuals whose records you may access.
- Preserve and protect the confidentiality of all internal, restricted, or Critical information as a matter of ongoing responsibility.
- Never disclose internal, Restricted, or Critical data (as defined by policy; see above) or distribute such data to a third party in any medium (including oral, paper, or electronic) without proper approval, and in the case of Restricted or Critical data, without a contract processed through or waived by the Health Science Center Purchasing Department.

To be entrusted with access to Texas A&M Health Science Center data and information, and access to IT accounts, systems, and applications, new or continuing faculty, staff, students, visiting scholars, volunteers and all other authorized individuals must accept these responsibilities and standards of acceptable use. By accepting these terms, you agree to follow these rules in all of your interactions.

I have read, understand, and agree to abide by the practices outlined in this agreement.

Signature _____ Date _____



THE TEXAS A&M UNIVERSITY SYSTEM

AGREEMENT FOR WAIVER, INDEMNIFICATION, ASSUMPTION OF RISK AND MEDICAL TREATMENT AUTHORIZATION

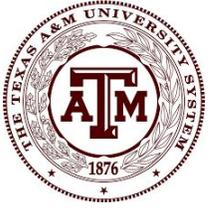
I, _____, age _____, desire to participate voluntarily in all activities of the _____ (“Activity”), which is sponsored or conducted by or under the auspices of _____ (“Sponsor”), a member of The Texas A&M University System. I am fully aware that there are inherent risks to myself and others involved with the Activity, including but not limited to illness, including the COVID-19 virus, its variants and other mutations, injury (including death), and loss of personal property, and I choose to voluntarily participate in the Activity and do voluntarily assume the above mentioned risks as to myself and my property, and to the person and property of others. I acknowledge that the Activity may be physically strenuous. I know of no medical reason why I should not participate.

HOLD HARMLESS, INDEMNITY AND RELEASE:

For myself, my heirs, personal representatives or assigns, I do hereby release, waive, covenant not to sue, indemnify and agree to hold harmless for any and all purposes the Sponsor, The Texas A&M University System, the Board of Regents for The Texas A&M University System, and their members, officers, agents, volunteers, or employees (“RELEASEES” and/or “INDEMNITEES”) from any and all liabilities, claims, demands, injuries (including death), or damages, including court costs and attorney’s fees and expenses, which may occur to myself, other participants, and third-persons as a result of my participation and conduct in the Activity, while traveling to and from the Activity, or while on the premises owned, leased, or controlled by RELEASEES/INDEMNITEES, **including injuries sustained as a result of the sole, joint, or concurrent negligence, negligence per se, statutory fault, or strict liability of RELEASEES/INDEMNITEES.** I understand this waiver does not apply to injuries caused by intentional or grossly negligent conduct.

NO INSURANCE:

I understand that RELEASEES/INDEMNITEES do not maintain any insurance policy covering any circumstance arising from my participation in the Activity or any event related to that participation. **As such, I am aware that I should review my personal insurance coverage.** Sponsor does not carry general liability insurance to cover claims arising from the Activity so it seeks a waiver of claims as additional consideration for my right to participate such that Sponsor, a governmental unit of the State of Texas, can (a) provide the activity at the lowest possible cost to participants; and (b) provide access to a greater number of participants by expending limited resources on program materials rather than on liability insurance.



WAIVER, INDEMNIFICATION, AND MEDICAL TREATMENT AUTHORIZATION

SIGNING THIS DOCUMENT INVOLVES THE WAIVER OF VALUABLE LEGAL RIGHTS.

Should you have any questions about these rights and the ramifications of signing this document you should consult an attorney.

SIGNED this _____ day of _____, 20__.

Participant Signature: _____

Printed Name: _____

Participant's Date of Birth: _____

Parent or Legal Guardian Signature: _____

(If Participant is under 18 years old)

Parent or Legal Guardian Printed Name: _____

(If Participant is under 18 years old)

Participants Name:			
Address:			
Phone:			
UIN or Driver's License#			
Student	Fac/Staff	Dependent	General Public
Participant Emergency Contact Information			
Emergency Contact Name:			
Address:			
Phone:			
Alternate Phone:			
Relationship to Participant:			