TEXAS A&M UNIVERSITY

Identity Management Office

Division of Information Technology

NetID Account Management

For Texas A&M University System Employees

Table of Contents

Employment Lifecycle Stages 3

NetID Account 7

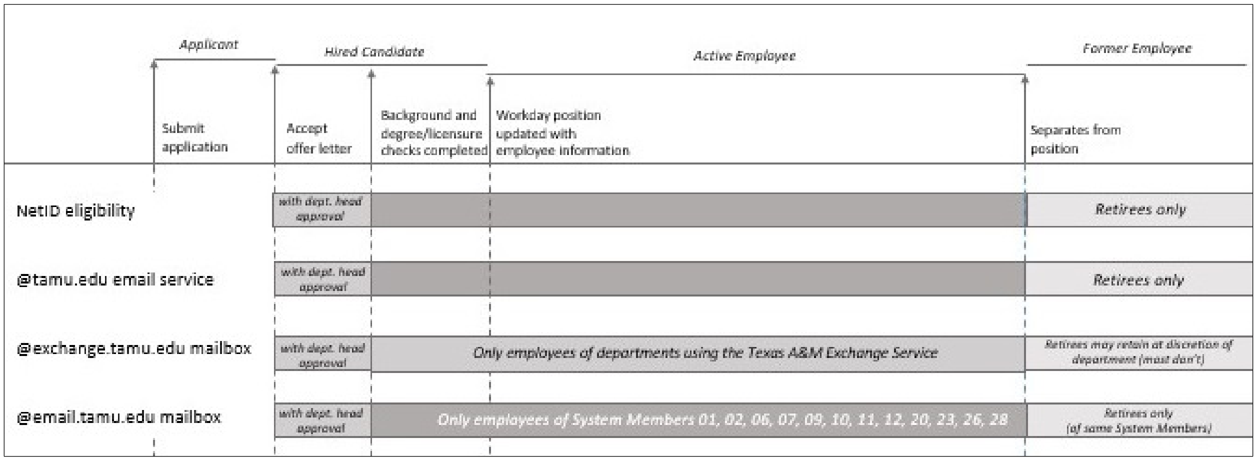
NetID Account Management 8

HR Identity Agent Program 15

Appendix A: Employee Data sent to the Texas A&M NetID IdMS 16

Appendix B: Employee Directory Entries 18

Employee access to electronic resources is critical for them to carry out their job duties. This document summarizes the management of an employee's NetID account through the various stages of the employee lifecycle to assist departments and employees better understand the processes at work.


Applicant
Hired Candidate
Active Employee
Former Employee
Submit application
Accept offer letter
Background and degree/licensure checks completed
Workday position updated with employee information
Separates from position
NetID eligibility
@tamu.edu email service
@exchange.tamu.edu mailbox
@email.tamu.edu mailbox
with dept. head approval
with dept. head approval
with dept. head approval
with dept. head approval
Retirees only
Retirees only
Only employees of departments using the Texas A&M Exchange Service
Retirees may retain at discretion of department (most don't)
Only employees of System Members 01, 02, 06, 07, 09, 10, 11, 12, 20, 23, 26, 28
Retirees only (of same System Members)

Employment Lifecycle Stages

The following summarizes different stages an employee will go through during the employment lifecycle. Please see Appendix A for information about how these affiliations are calculated.

Applicant

Employment application materials and submission varies depending on the type of position being sought:

- **faculty position**: apply for position via the college or department
- **staff position**: apply for position on https://jobpath.tamu.edu/
- **graduate assistant position**: apply for position via department
- **student worker position**: apply for position on https://jobsforaggies.tamu.edu/

Applications are evaluated by the position manager, qualified candidates identified and interviewed.

Possible transitions:

1) Applicant offered position and accepts. Transition to **hired candidate**.
2) Applicant offered position and declines. Relationship to University ends.
3) Applicant is not offered position. Relationship to University ends.

Hired Candidate

Before a position offer is finalized, the hired candidate must undergo:

- Criminal history background check
- Verification of degree(s) and/or licensure (if position requires a degree and/or licensure or candidate claims to have a degree and/or licensure)
- Verification of Selective Service registration (if candidate is male)

Possible transitions:

1) Hired candidate cleared for work. Transition to an **active employee** on hire date.
2) Hired candidate's background checks uncovered information that make the hired candidate ineligible for position. Relationship to University ends.

Active Employee

An active employee is one who is currently working at their job.

Possible transitions:

1) Employee takes a leave of absence. Transition to **leave of absence**.
2) Employee quits or is fired. Transition to **terminated**.
3) Employee retires. Transition to **retiree**.
4) Employee dies. Transition to **deceased**.

Employee on Leave of Absence

An employee on leave of absence (LOA) is one who has obtained permission to take an extended period of time off from their job. Each LOA is negotiated independently. LOAs can be granted for any number of reasons such as sabbatical, medical, to serve in the military, or in rare cases, disciplinary in nature. Time periods can be of any length, but generally would not extend beyond a year. Sometimes benefits are retained and paid while on leave, and other times not.

Possible transitions:

1) Employee returns to work. Transition to **active employee** status.
2) Employee quits or is fired. Transition to **terminated** status.

Terminated Employee

A terminated employee is one who has left their position voluntarily or involuntarily.

Possible transitions:

1) Employee takes another position with the system. Transition to **active employee** status.

Retired Employee

A retired employee is one who has retired from their position.

Possible transitions:

1) Employee takes a new position with the system. Transition to **working retiree** status.
2) Employee dies. Transition to **deceased** status.

Working Retiree

A working retiree is a retired employee who has taken another position with the system.

Possible transitions:

1) Employee quits or is fired. Transition to **retiree** status.
2) Employee dies. Transition to **deceased** status.

Deceased Employee

A deceased status is set when a current/retired employee dies.

Non-Employee Roles Tracked in Employee System

There are several non-employee groups that will have a record in the employee system and whose NetID accounts are sponsored.

Benefits Recipient: Surviving Dependent/Military Leave Dependent

A benefits recipient is a person receiving System Health Benefits due to their relationship with an employee or former employee.

Graduate Fellow

A graduate fellow is a person receiving System Health Benefits due to having been awarded a graduate fellowship at one of the Texas A&M System member institutions.

Possible transitions:

1) Graduate fellow completes fellowship term. Transitions to **inactive affiliate** status.

Affiliate

An affiliate is a person that is not employed by the Texas A&M System but who requires access to Workday because they supervise Texas A&M System employees.

Possible transitions:

1) Affiliate's relationship with the Texas A&M System ends. Transition to **inactive affiliate** status.

Inactive Affiliate

An inactive affiliate is a person that at one time had a non-employee relationship with the System requiring access to Workday.

Possible transitions:

1) Former affiliate’s relationship with the Texas A&M System is renewed. Transition to **affiliate** status.
2) Former affiliate takes a position in the Texas A&M System. Transition to **active** status.

NetID Account

What is a NetID account?

A NetID account is the Texas A&M University login account. It consists of the following:

	Example
Identity Data	
Biographical information	name, birth date
Contact information	work address, office phone number, email address
Identifiers	UIN, NetID
Affiliations with organization	faculty, staff, employee, student, affiliate For employees: position type, title, department For students: classification, major department
Login Credential	
Login Identifier	NetID
Material used to verify person logging in is the account holder	Password Password + Duo two-factor authentication

How is the NetID account used?

Campus personnel use the NetID account to access a variety of university, commercial and federal services.

When a person logs in to an application, two things happen:

- They enter the login credential to verify they are the account holder (authenticate)
- The application evaluates what features should be displayed to the person (authorization).

To make the authorization decision, the application can use either internally or externally maintained information The Canvas Learning Management System is an example of an application using internally maintained information, which are preloaded class rosters. When the student or instructor logs into Canvas, they will only see the sections on which they are listed, and the functionality they have is determined by their role. Instructors can assign homework and see grades for all students in the section, while students can edit and submit their own homework and view their own grades. An example of an application using externally maintained information is Linked In Learning. It uses information in the NetID IdMS to determine whether or not someone is eligible to access material under the Texas A&M contract.

Because applications increasingly rely on data in the NetID record to determine what features an account holder is allowed to use, the identity data associated with a NetID account is just as important as whether or not the login credential is functioning.

NetID Account Management

The NetID account lifecycle consists of an initialization phase, an operational phase, and a termination phase.

Initialization Phase

The initialization phase results in the successful enrollment of the employee or Texas A&M System affiliate in the Texas A&M NetID Identity Management System (IdMS) and the establishment of the NetID Credential.

Enrollment

Creation of a record for the employee or Texas A&M System affiliate in the Texas A&M NetID IdMS

In order for a person to claim a NetID account, the following identity data is required by the Texas A&M NetID IdMS: UIN, Full Name, Date of Birth. Systems of Record that sponsor NetID accounts typically provide information about a person's role or relationship with the university in addition to this basic data.

Workday serves as the System of Record and sponsor for employee and System affiliate NetID accounts and sends data about employees, along with details about their positions and work locations, to the NetID IdMS. This data is used to automate management of the employee and System affiliate NetID accounts. The NetID IdMS receives updates from Workday once per day, after business hours. Enrollment of a new employee or affiliate in the Texas A&M NetID IdMS is triggered when a record for the employee or affiliate is received by Texas A&M Identity Services via the Workday update.

Any delays in getting data added to or updated in Workday means it can be a few days after the hire date before Workday includes a record for a newly hired employee in the update to the NetID IdMS. With most positions requiring electronic access to perform work duties, this type of delay results in lost productivity.

To get an employee record created in the NetID IdMS before Workday begins supplying information for the employee, the department can have the record manually added by the Identity Management Office[1] or by an HR Identity Agent.

Employee NetID account eligibility prior to start date

In certain situations, the department may want to permit an employee to claim a NetID account prior to the first day of work. This is allowed as long as the department has the following:

- Signed job acceptance letter from new hire.
- Successful completion of criminal background check and verification of degree(s)/licensures.

[1] To have the Identity Management Office create an account, a NetID Request Form (http://url.tamu.edu/netidrequest) must be filled out and submitted.

Employee NetID account eligibility prior to start date, continued

In special situations, an account can be set up with just the job acceptance letter, but the department head will need to authorize this.

To set up an employee’s account before the employee’s start date, the department can request the account be manually created by the Identity Management Office[1] or by an HR Identity Agent.

Credential Issuance

Establishment of employee’s or System affiliate’s Texas A&M NetID Credentials

Initially, an employee or System affiliate will establish a NetID Credential that consists of a NetID/password pair. Texas A&M NetID Credential establishment or activation is a self-service on-line process, accessed by going to http://gateway.tamu.edu and clicking the **Claim Your NetID** link. The employee will then be stepped through the process of selecting a NetID and setting a password.

Two-factor NetID Credential

All active and working retiree employees are required to set up two-factor authentication on their NetID account. Retirees have the option of setting up two-factor authentication on their account, but are not required to do so.

The Texas A&M University System uses Duo Two-Factor Authentication to support the second factor. An employee or retiree enables Duo on his or her NetID account by completing the enrollment process using the self-service NetID Duo Enrollment application (**https://gateway.tamu.edu/duo-enroll**).

Operational Phase

During the operational phase, the employee or System affiliate manages his or her NetID Credential and keeps it secure. The Texas A&M NetID IdMS manages the NetID Credential data and status and securely maintains the identity information supplied by Workday. The employee or System affiliate uses his or her NetID Credential to access on-line resources.

Employee/System Affiliate Use of Credential

Campus applications have the option of utilizing the NetID account for their users instead of maintaining their own accounts. When an employee or System affiliate authenticates to an application that relies on the NetID account for authentication, the application passes the authentication request to the NetID IdMS to verify the supplied Credential is valid.

Employee/System Affiliate Education

To reduce the risk of an employee compromising his or her Credential, Information Technology's Risk Management and Policy group has developed the Information Security Awareness Training course available through the employee training system, TrainTraq. Texas A&M University System employees are required to complete Information Security Awareness Training annually. System Affiliates have access to TrainTraq and may be required to take the training by their host department.

NetID IdMS Credential Management

Temporary Lockouts

If an account holder mistypes their password multiple times in a row, the account holder will be temporarily locked out. CAS will not accept an authentication attempt from a user for 15 minutes after they type their password incorrectly seven times in seven minutes. For account holders with Two-Factor authentication set up on their account, Duo will not accept an authentication attempt for 15 minutes after seven consecutive failed Duo authentication events.

Monitoring Suspicious Credential Activity

Monitoring of NetID Credential activity is a program operated by Texas A&M NetID IdMS Operations in conjunction with the Division of IT Security.

CAS login activity is audited for suspicious Credential activity. Reports are delivered to the Texas A&M NetID IdMS Operations administrators for review and further action if necessary. If a Credential is determined to be compromised, the Credential is revoked and the employee's NetID account locked.

The account holder's NetID account can be unlocked only by designated Division of IT Security or NetID IdMS Operations staff.

Credential Expiration/Re-issuance

For security reasons, employees and System affiliates are required to change their passwords periodically. The life of a password depends on the length. Passwords that are eight to sixteen characters must be changed after one year of use. Passwords over sixteen characters can be used for four years before the account holder has to set a different password.

Three weeks prior to password expiration, the account holder is notified via e-mail of the pending expiration. If the user does not establish a new password, a second notice is sent via e-mail two weeks prior to the expiration date. One week prior to the expiration date, a final notice is sent.

The account holder can set a new password in one of three ways:

- The account holder logs into the Password Change application (https://gateway.tamu.edu/change-password) with his or her existing NetID Credential prior to the expiration date and set a new password.
- If the account holder has previously set up Self-Service Password Reset, the account holder may use the Self-Service Password Reset application (https://gateway.tamu.edu/password-reset/) to set a new password. The Self-Service Password Reset application sends a short-lived single use Secret to the e-mail or phone number on record that the account holder must submit in order to establish a new Credential.

- The account holder may call or stop by HelpDesk Central to have their NetID account flagged for a password reset via the Forgotten Password Reset application. For employees, the ability to have the account flagged by calling HelpDesk Central may be prohibited by their department.

If the employee or System affiliate does not change his or her password prior to the expiration date, the NetID Credential will be destroyed and the account holder will not be able to authenticate to any application until a new password is set. At this point, the account holder will only be able to reset their password by using Self-Service Password Reset or by contacting HelpDesk Central for assistance.

Termination Phase

In the termination phase, the employee separates from employment with the Texas A&M University System or the affiliate's relationship with the Texas A&M System ends.

Terminated employees are not eligible for NetID accounts unless their separation from employment is due to retiring. **Non-retiring terminating employees should plan on losing access their NetID account on their termination date.**

Retiree NetID account and email service eligibility

All retirees of the Texas A&M University System are eligible to possess and use a NetID account.

Workday handles disbursement of health benefits for retirees, and sponsors NetID accounts for retirees utilizing System health benefits. If a retiree decides to cash out their health benefits, they no longer have an active relationship with the Texas A&M System and Workday will not sponsor the account. To retain a NetID account in this situation, the retiree needs to contact the Identity Management Office. The account will be manually maintained, with the retiree confirming every year that they still want the account.

@tamu.edu Email Service

The retiree's @tamu.edu email alias is a forwarding address that can be set to forward to any destination whether that is a mailbox managed by Texas A&M or a personal address, like a gmail.com account. The delivery address can be updated by the retiree logging into **https://gateway.tamu.edu**, clicking the **Email Setttings** icon, and updating the section labeled **Forwarding Settings for Your Published Email Address**.

Texas A&M Exchange mailbox

Employee access to a Texas A&M Exchange mailbox after retirement is at the discretion of the department. Most departments do not continue sponsoring access to an Exchange mailbox for their retirees.

Texas A&M Gmail mailbox/GoogleApps account

Only retirees of the following member institutions are eligible for a Texas A&M Gmail mailbox: Texas A&M University (02), Texas A&M University at Galveston (10), Texas A&M Health Science Center (23), Texas A&M AgriLife Research (06), Texas A&M AgriLife Extension Service (07), Texas A&M Engineering Experiment Station (28), Texas A&M Engineering Extension Service (09), Texas A&M Transportation Institute (11), Texas A&M

Retiree NetID account and email service eligibility, continued

Forest Service (12), Texas A&M Veterinary Medical Diagnostic Laboratory (20), Texas A&M System Shared Service Center (26) or Texas A&M System Offices (01).

The GoogleApps account can be set up by the retiree logging into https://gateway.tamu.edu, clicking the **Email Setttings** icon, and updating the section labeled **Google Apps**.

If the retiree worked for a department that prohibited them from using a GoogleApps account as an employee, they will become eligible to claim a GoogleApps account as soon as their status switches to retired in Workday. If they would like to set up the account prior to retirement so that they can transfer email from their departmental email account, their departmental HR will need to send an email to the Identity Management Office requesting that the employee be made eligible for a GoogleApps account. The email should include the retiree's name and UIN and retirement date. The earliest that a retiree from one of these departments will be made eligible for a GoogleApps account is 2 weeks prior to the retirement date.

Credential Revocation

To render the employee's or System affiliate's NetID Credentials invalid and unusable.

Assuming that the employee's termination information is added to Workday prior to the termination date,

- the employee's email delivery will be disabled on the termination date, and
- the NetID account will be locked the day after the termination date.

As soon as a System affiliate's status switches to inactive, their email delivery is disabled and their NetID account is locked.

If the terminating employee or inactive affiliate is associated with the university in multiple ways[2], the presence of the other affiliations on the NetID account will prevent the account from being locked or disabled in any way.

Expedition of Account Locking

To promptly remove an employee's access to their NetID account at termination, the HR representative should send an email to helpdesk@tamu.edu to request immediate locking of the account. The email should include the terminating employee's full name and UIN.

[2] For example, the individual is an enrolled student pursuing a degree as well as an employee or affiliate.

Email Forwarding and Exports

As part of transitioning job responsibilities from one employee to another, the department may wish to keep the terminating employee's email delivery operational for a period of time so that the new employee may monitor and respond to emails. To retain email delivery for a period of time after the employee leaves the department, the department's HR representative or the employee's supervisor (copying departmental HR on the message), may email helpdesk@tamu.edu requesting that email delivery remain operational, specifying when email can be disabled. *Note: This request will not enable account access for the terminated employee. Please see next section, **Extended Account Access**, for information on extending the terminated employee's access to the account.*

Employee mailbox contents are property of the department[3]. Upon termination of an employee, the department may request that contents of the Exchange.tamu.edu mailbox be exported. GoogleApps mailbox contents and drive contents can also be exported and/or assigned to a different owner. To make this request, the department's HR representative or the employee's supervisor (copying departmental HR on the message), may email helpdesk@tamu.edu requesting the export or content transfer.

Handling of Deceased Employee Accounts

As soon as an employee's status switches to deceased in the NetID system, the employee's NetID account is locked, the White Pages directory entry is suppressed (no longer publicly available) and @tamu.edu mail delivery is disabled.

If the department wishes to have any changes made to the account (retain or change mail forwarding, etc), NetID IdMS administrators will need documented consent from the organizational unit head in order to make the change. The organizational unit head should send an email helpdesk@tamu.edu to provide authorization for the requested change.

Extended Account Access

In some situations, a terminating employee may have a legitimate need to continue using his or her NetID account.

Part-time employees

For part-time personnel, it may be desirable for the employee to retain their NetID account during the inactive period. As long as the employee has committed to returning within the next 12 months, this is permitted. The department can have an onboarding employee role manually added by the Identity Management Office[4] or by an HR Identity Agent. The presence of this role will prevent the account being locked during the interim.

[3] Per SAP 29.01.03.M1.17 Information Resources – Privacy

[4] To have the Identity Management Office update the account, a NetID Request Form (http://url.tamu.edu/netidrequest) must be filled out and submitted that documents the situation.

Employee transitioning to a different type of relationship with department

Occasionally, an employee will continue to have an active relationship with departmental personnel after the period of employment ends that necessitates continued access to a NetID account. Examples of this type of change include a graduate student who wants to continue working in the professor's lab on a volunteer basis or collaborate with their former professor remotely after completing their assistantship.

To preserve the former employee's access to the NetID account, the department will fill out and submit a NetID Request Form documenting the nature of the new relationship. The Identity Management Office will then update the NetID account with a role that reflects the person's new affiliation.

Extended access for former employee

If the department would like a terminating employee to have access to the NetID account and email beyond the termination date for knowledge transfer or as a professional courtesy, the department can sponsor an account extension for up to one year after the termination date. The department will fill out and submit a NetID Request Form to have this extension put in place.

HR Identity Agent Program

The HR Identity Agent Program supports departmental use of NetID accounts. The program relies on selected staff designated by authorized departmental officials to act as trusted authorities for NetIDs. Upon completion of all training requirements, Identity Agents will be given access to the NetID system and enabled to perform functions specific to their role.

The NetID Identity Management System (IdMS) relies on data in Workday employee records to automate creation, maintenance, locking and removal of NetID accounts for employees. While this works well for maintaining employee account information, issues can arise when an employee is in transition due to delays in employee record updates.

Designated HR Identity Agents are able to view, create and edit personnel records in the NetID IdMS, enabling their employees to activate NetID accounts and gain access to departmental systems on day one of employment. HR Identity Agents are also able to preserve part-time employee access to their NetID accounts while not actively working.

How to become an HR Identity Agent

To become a designated HR Identity Agent, you must meet eligibility requirements, submit a designation request, and complete the required training courses.

Eligibility Requirements

- For TAMU (02)
  - be a designated HR Liaison (see http://employees.tamu.edu/liaisons/)
- For other system members
  - hold a position responsible for providing human resources services for your department

Designation Request

The HR Identity Agent Designation Request Form will need to be filled out and submitted.

Training Requirements

Two TrainTraq courses will need to be completed:

- Export Control training (2111212)
- HR Identity Agent training (2112334)

Appendix A: Employee data sent to the Texas A&M NetID IdMS

The Texas A&M NetID IdMS utilizes data from the Texas A&M University System employee system, Workday, to manage employee accounts. Employee data is exported from Workday to the Enterprise Data Warehouse (EDW), which distributes the data to all downstream systems. This appendix documents the record inclusion criteria for the employee feed from the Enterprise Data Warehouse.

Workday record organization

In Workday, all records are referred to as “worker”. Each record is categorized as either Employee or Contingent Worker.

- Employees will always be people who are in an employer/employee relationship and paid through Workday Payroll, or are receiving TAMUS employee benefits, such as surviving dependents.
- The other worker category, Contingent Worker, are people with an HR or Payroll business need to have a Workday record or who manage TAMUS employees. Contingent Worker records will be Qatar, federal Homeland Security, Agriculture or Military personnel who supervise TAMUS employees; since they manage employees, they will have a Workday record to perform their supervisory responsibilities.

The employment status provided in the feed for a given employee is determined using the logic in the below table. For each record, the logic for each status is tested in the order presented in the table. The first employment status that returns a True value when evaluated is the employment status assigned to the record.

Employment Status Code	Employment Status Description	Logic
D	Death	Date of Death is not null
R	Retire	Active Status = False, and Is Retiree = True
W	Working Retiree	Active Status = True, and Is Retiree = True
X	Terminated Contingent Worker	Primary Termination Reason is not null, and Worker Type = Contingent Worker
T	Terminated	Primary Termination Reason is not null
L	Leave of Absence	Active Status = True, and Leave Type is not null
F	Graduate Fellow	Active Status = True, and Job Profile Description = Graduate Fellow
M	Military Leave Dependent	Active Status = True, and Job Profile Description = Military Leave Dependent
S	Surviving Dependent	Active Status = True, and Job Profile Description = Surviving Dependent
N	Affiliate Non-Employee	Active Status = True, and (Job Profile Description = Qatar Local Worker OR Worker Type = Contingent Worker)
A	Active	Active Status = True, and Worker Type = Employee
P	Hired Candidate	Active Status = False and Worker Type = Employee

Table 1: Rules governing inclusion of personnel records in data feed from the Enterprise Data Warehouse

Feed Status Code	Feed Status Description	TAMU IdMS feed inclusion rules	employmentStatus in NetID IdMS
Non-employee records:			
M	Military Leave Dependent	all	set to ‘B’
S	Surviving Dependent	all	set to ‘B’
F	Graduate Fellow	all	set to ‘F‘
N	Affiliate Non-employee	all	set to ‘N‘
X	Inactive Non-employee	If (current date - inactive date < 120 days)	set to ‘X‘
Employee records:			
P	Hired Candidate	If (current date < hire date)	Set to ‘P’
A	Active	all	set to ‘A‘
L	Leave of Absence	all	set to ‘L‘
T	Terminated	if (Primary Termination Reason is not NULL) and (current date – last paid date < 120 days)	
		if currentDate < terminationDate	set to ‘A’
		else if terminationReason = ‘Retirement’	set to ‘R’
		else	set to ‘T‘
R	Retired	all	set to ‘R‘
W	Working Retiree	all	set to ‘W’
D	Deceased	if (current date – last paid date < 120 days)	set to ‘D‘

Appendix B: Employee Enterprise Directory Entries

EDW-supplied data stored in Enterprise Directory People branch entries

Table 3: EDW data in Enterprise Directory People branch entries

Attribute	Comments
Personal data	
Universal Identification Number (tamuEduPersonUIN)	
Name:	
Official Name (tamuEduPersonOfficialName)	
Common Name (cn)	cn attribute will always have tamuEduPersonOfficialName as one of the values
Last Name (sn)	
First Name (givenName)	
Date of Birth (birthDate)	
Employee Home Phone (homePhone)	
Position data	
TAMU Role-based Affiliations: tamuEduPersonAffiliation	***Position category*** (faculty/staff/graduateassistant/studentworker) ***Status*** (future/active/workingretiree/loa/retired/terminated/deceased) captured in role flags
Higher Ed Role-based Affiliations: eduPersonAffiliation eduPersonPrimaryAffiliation	***Broader role categories*** (faculty/staff/employee/member)
Role@Location Affiliations	
TAMU Scoped Affiliations (tamuEduPersonScopedAffiliation)	Employee's tamuEduPersonAffiliation flag scoped to AdLoc location, e.g. employee:staff:active@cs.tamu.edu
Higher Ed Scoped Affiliations (eduPersonScopedAffiliation)	eduPersonAffiliation flags scoped to identity provider domain (@tamu.edu)

Attribute	Comments
Physical Mail:	
Employee/Affiliate Work Address (postalAddress)	
Employee/Affiliate Campus Mail Stop (mailStop)	
Employee Work City (localityName)	
Employee Work State (stateOrProvinceName)	
Employee Work Zip Code (postalCode)	
Employee Work County (countyName)	
Employee Public Office Telephone Number (telephoneNumber)	
Employment-related attributes:	
System Member:	
System Member Codes (tamuEduPersonMember)	For employees, Adloc and EmpLoc system member codes included
Primary System Member Code (tamuEduPersonPrimaryMember)	The AdLoc system member code, e.g. 28
Primary System Member (tamuEduPersonPrimaryMemberName)	The AdLoc system member name, e.g. Texas Engineering Experiment Station
tamuEduPersonScopedAffiliation scoping	Incorporates FAMIS system member abbreviations, e.g. @tees.edu
Campus:	
tamuEduPersonScopedAffiliation scoping for 02/10/23 employees	@cs.tamu.edu @gv.tamu.edu @hsc.tamu.edu @qt.tamu.edu @law.tamu.edu
Department:	
Employee/Affiliate Primary Department (tamuEduPersonDepartmentName)	1st choice: EmpLoc department; 2nd choice: AdLoc department
Employee AdLoc Code (tamuEduPersonAdLoc)	
Employee EmpLoc Code (tamuEduPersonEmpLoc)	
Position:	
Employee/Affiliate Official Title (title)	
Employee Title Code (tamuEduPersonTitleCode)	
Employee Supervisor UIN (tamuEduPersonSupervisorUIN)	
Data Source (tamuEduDataFeed)	EDW is listed as one of the account owner's data source affiliations

Employee-supplied data stored in Enterprise Directory People branch entries

In addition to data provided by EDW, employees can add the following information to their directory entries.

Table 4: Account holder-supplied data in Enterprise Directory People branch entries

Attribute	Comments
NetID (tamuEduPersonNetID)	
Display Name (displayName)	
Published Email Address (mail)	
Primary and Alternate Aliases (mailLocalAddress)	Email domains assigned to an employee vary according to primary system member code: member 24: @tamuct.edu all others: @tamu.edu
Email Destination Address (mailRoutingAddress)	
@email.tamu.edu Alias(es) (tamuEduNeoLocalAddress)	
All Texas A&M Email Aliases (tamuEduLocalMailAddresses)	
Published Home Page URL (personalURI)	

Management of EDW-supplied data stored in Enterprise/White Pages People Branch Entries

Presence/absence of data

Storage of employment information in LDAP is affected by the employee's status:

- When an employee record drops out of the EDW data feeds, all attributes listed under the **Position Data** category are cleared of EDW data.
- When an employee retires, primary department name and official title are prefixed with 'Retired –'.
- When an employee is terminated, all attributes listed under the **Position Data** category except the affiliation and tamuEduDatafeed attributes are cleared of EDW data.
- When an employee has a status of deceased, all attributes listed under the **Position Data** category except the affiliation and tamuEduDatafeed attributes are cleared of EDW data.

Accessibility of data

Data in the Enterprise Directory is accessible only via web services or Shibboleth.

The default data returned about a person from the web service is that classified as publicly or anonymously readable. In order to access restricted data, a request for data access must be submitted and approved.

- For faculty or staff employees, employment information is considered to be public information.
- Positions categorized as a graduate assistant or student worker position require the employee to be a student as a condition of employment. Access to position-related information for these two categories is restricted to comply with FERPA.
    - This type of suppression is triggered when the tamuEduSuppress attribute contains a 'studentEmployment' flag.

In some circumstances access to all data in an entry will be restricted. This type of suppression is triggered when the tamuEduSuppress attribute contains a 'name' or 'administrative' flag.

Employee accounts will be administratively suppressed in the following situations:

- Death of the employee.
- Employee's account is in grace period prior to deletion (see next section for more details).
- UPD requests suppression of the employee's directory information for security reasons.
- The employee is also an enrolled student and requests full suppression of personal data under FERPA.

If an employee specifies a proxy for their account, the proxy gains account owner access level privileges and the ability to edit all LDAP-authoritative settings such as aliases, email forwarding, etc.

Table 5: Data access for attributes storing EDW and employee-supplied data as a function of account owner's position category.

Attribute	Accessibility of data	
Account owner's position category:	faculty/staff	grad asst/student wrkr
Personal data		
Universal Identification Number (tamuEduPersonUIN)	**restricted**	**restricted**
Name:		
Official Name (tamuEduPersonOfficialName)	public	public
Common Name (cn)	public	public
Last Name (sn)	public	public
First Name (givenName)	public	public
Display Name (displayName)	public	public
Date of Birth (birthDate)	**restricted**	**restricted**
Employee Home Phone (homePhone)	**restricted**	**restricted**
Home Page URL (personalURI)	public	public
Position data		
Role-based Affiliations:		
TAMU Role-based Affiliations (tamuEduPersonAffiliation)	**restricted**	**restricted**
Higher Ed Role-based Affiliations (eduPersonAffiliation)	**restricted**	**restricted**
Higher Ed Primary Role-based Affiliation (eduPersonPrimaryAffiliation)	**restricted**	**restricted**
Role@Location Affiliations:		
TAMU Scoped Affiliations (tamuEduPersonScopedAffiliation)	**restricted**	**restricted**
Higher Ed Scoped Affiliations (eduPersonScopedAffiliation)	**restricted**	**restricted**
Physical Mail:		
Employee Work Address (postalAddress)	public	**restricted**
Employee/Affiliate Campus Mail Stop (mailStop)	public	**restricted**
Employee Work County (countyName)	public	**restricted**
Employee Work City (localityName)	public	**restricted**
Employee Work State (stateOrProvinceName)	public	**restricted**
Employee Work Zip Code (postalCode)	public	**restricted**
Employee Public Office Telephone Number (telephoneNumber)	public	**restricted**
System Member:		
System Member Codes (tamuEduPersonMember)	public	**restricted**
Primary System Member Code (tamuEduPersonPrimaryMember)	public	**restricted**
Primary System Member (tamuEduPersonPrimaryMemberName)	public	**restricted**
Department:		
Employee Primary Department (tamuEduPersonDepartmentName)	public	**restricted**
Employee AdLoc (tamuEduPersonAdLoc)	public	**restricted**
Employee EmpLoc (tamuEduPersonEmpLoc)	public	**restricted**
Position:		
Employee Official Title (title)	public	**restricted**
Employee Title Code (tamuEduPersonTitleCode)	public	**restricted**
Employee Supervisor UIN (tamuEduPersonSupervisorUIN)	**restricted**	**restricted**
Data Source (tamuEduDataFeed)	**restricted**	**restricted**

Attribute	Accessibility of data	
Account owner's position category:	faculty/staff	grad asst/student wrkr
Account-related data		
NetID (tamuEduPersonNetID)	**restricted**	**restricted**
Email:		
Primary/Published Email Address (mail)	public	public
Primary and Alternate Aliases (mailLocalAddress)	public	public
Email Destination Address (mailRoutingAddress)	**restricted**	**restricted**
@email.tamu.edu Alias(es) (tamuEduNeoLocalAddress)	public	public
All Texas A&M Email Aliases **(**tamuEduLocalMailAddresses**)**	**restricted**	**restricted**