TEXAS TECH UNIVERSITY™

Operating Policy and Procedure

OP 61.47: University Identification

DATE: May 12, 2021

PURPOSE: The purpose of this Operating Policy/Procedure (OP) is to establish the standards and guidelines for university identification, including uses, components, issuance, replacement, and access and security.

REVIEW: This OP will be reviewed in October of even-numbered years by the Associate Vice President for Operations, the Managing Director of Operations Division Planning and Administration (ODPA), the Office of the Chief Information Officer, and the Unit Manager of the TTU ID System with substantive revisions forwarded to the Campus Security Committee.

POLICY/PROCEDURE

1. Uses of University Identification

a. Verification of Identity or Affiliation

(1) The RaiderCard is the official University Identification card and is the property of Texas Tech University.

(a) RaiderCard holders shall present the card when requested to do so by TTU officials.

(2) If required by an institution or area's operating procedures, individuals may wear a university identification card as a badge. Texas Tech University Health Sciences Center identification and access badges are issued in accordance with HSC OP 76.02.

(3) RaiderCards shall not be used to prove affiliation with the university after an individual is no longer a student or employed with Texas Tech University or Texas Tech University Health Sciences Center. The individual's ID account will be automatically disabled once he or she is no longer affiliated with Texas Tech University or Texas Tech University Health Sciences Center.

(4) Each Texas Tech University student, faculty, and staff member is responsible for maintaining a valid RaiderCard that is in proper working condition. The RaiderCard should always be carried while on campus and at campus-sponsored events.

(5) Access to certain services, facilities, and activities on or off campus may only be obtained by using a current RaiderCard. Persons not possessing a current ID must contact the University ID Office to receive a replacement. Replacements are subject to a replacement fee. (See section 4 below for replacement procedures.)

b. Financial Transactions

(1) RaiderCards hold various pre-deposited fund accounts. These accounts are a record of pre-deposited funds accessed by the card holder for the purpose of purchasing products and services, by means of RaiderCash or Dining Bucks.

(2) The RaiderCard is the only means of accessing a participant's RaiderCash and Dining Bucks accounts and, as such, must be presented at the time of purchase. The card holder may be required to sign a receipt for goods and/or services received. If the point of sale terminal is equipped to provide a receipt, the card holder will either receive a receipt as a matter of course or upon request. It is the card holder's responsibility to ensure that the receipt is correct.

(3) Card holders may obtain information regarding their RaiderCash or Dining Bucks accounts, including the amount of funds remaining on the account, recent transactions, where the account was used, and any new amounts added to the account, by accessing the accounts at the following locations:

(a) For RaiderCash, information is provided at the "Manage Your Account" page on the RaiderCard website (http://www.depts.ttu.edu/unvid/) or visit the University ID Office in person.

(b) For Dining Bucks, information can be obtained at the Hospitality Services e-accounts website at (https://ttu-sp.transactcampus.com/eAccounts/) or (www.hospitality.ttu.edu). Information can also be requested in person by visiting the Dining Plan Office located in the Student Union Building, Room 238C.

(4) Texas Tech University—including the University ID Office and Hospitality Services—is not responsible for the refusal to accept or honor the RaiderCard by any of the participating establishments under, but not limited to, the following circumstances:

(a) Insufficient funds in the account at the time of the purchase request.

(b) Malfunctions of the vendor's equipment at the time of the transaction attempt.

(c) Temporary or permanent suspension of the account due to violation(s) of this policy.

(d) Card deactivation due to lost or stolen reports.

2. Card Components

a. Identifying Information

(1) University identification cards will contain a student or employee's university identification number (R#) and will display a patron's affiliation with the university (i.e., student, faculty, staff, etc.).

(2) Photo

(a) All patrons must take a photo or submit a photo for their first ID. Photos must be approved by University ID Office staff.

(b) Applicants are not permitted to wear any article of clothing or eyewear that obscures their physical features, nor may any other person be in the photo.

(c) Reprinting a RaiderCard for vanity reasons will result in a fee.

(3) Name

(a) Student name changes should be routed through the Registrar's Office.

(b) Employee name changes should be routed through Human Resources.

(c) Name changes must be reflected on a government-issued ID card before a new RaiderCard can be issued.

(d) Preferred first names may be included and will display on the front of a patron's RaiderCard.

(4) Design

(a) All card designs must be appropriately approved before implementation.

(b) Hospitality Services and University Student Housing will approve the following cards:

- Dining Cards with Dining Bucks
- Special Purpose card involving Dining Bucks
  - VIP card, Training cards
- Conference Cards with Dining Bucks and/or Housing access
- Temporary worker cards related to Hospitality Services
- Temporary access cards related to Hospitality Services facilities
- Temporary access cards related to University Student Housing facilities

b. Additional information on the identification card may include important phone numbers, a barcode, an ISO number, an email address, and rules about proper card maintenance.

c. CBORD Mobile ID App

(1) Patrons may download the CBORD Mobile ID app from their service carrier's application store. The CBORD Mobile ID app allows patrons to utilize their geolocation to unlock the doors they have been granted access to through CS Gold. (See section 7 below for CS Gold policies.)

(2) Patrons will not allow others to use their eRaider information to share access on the CBORD Mobile ID app.

(3) Patrons will not be able to use Mobile ID on any University Student Housing doors.

(4) Any fees incurred with the download of the CBORD Mobile ID app will not be reimbursed by the Texas Tech University System.

(5) Patrons should never open doors using the CBORD Mobile ID app if they are not directly in front of that door. Opening doors for others using Mobile ID at a distance is prohibited and may result in disciplinary or legal action.

3. Issuance of University Identification

a. At any given time, patrons may only have one valid RaiderCard.

b. Proof of Identity

(1) All patrons must present government-issued photo ID in order to obtain a university identification card. Examples of approved documents include driver's license, state ID, passport, military ID, etc. Government-issued cards or documents without a photo will not be accepted.

(2) Identification cards must be picked up in person at the University ID Office during normal business hours: Monday–Friday, between 8:00 a.m. and 5:00 p.m., or other locations as scheduled or arranged.

c. Students

(1) Students must be enrolled in at least one credit hour to receive an initial ID.

(2) Students are expected to abide by all rules and regulations regarding the use of the student identification card as outlined in the *Student Handbook*, section L.

(3) Other Texas Tech University Campuses

(a) The University ID Office produces identification cards for students of all Texas Tech University and Texas Tech University Health Sciences Center campuses, with the exception of the El Paso campus. Cards are distributed in accordance with established guidelines for each campus.

(4) Distance

(a) Distance students should print out an *ID Verification Form* in order to obtain a university identification card. The form must be notarized, and the original must be mailed back to the University ID Office. This process must be repeated for all replacements.

(b) TTU K-12 students should complete the *Identity Verification Form* located on the TTU K-12 website to receive their ID card. Further information can be obtained by contacting the TTU K-12 office.

d. Faculty/Staff

(1) Employees must have a completed *Electronic Personnel Action Form* (ePAF) on file with the university in order to obtain an ID card.

(2) The University ID Office produces identification cards for employees of all Texas Tech University campuses, with the exception of satellite Health Science Center (HSC) employees. Cards are distributed in accordance with established guidelines for each campus.

(a) Employees at satellite Health Science Center locations should contact their onsite TTUHSC campus police department to obtain identification cards.

e. Retirees

(1) Retirees must present a signed retiree ID request from Human Resources in order to obtain a retiree identification card.

(2) Replacement retiree identification cards can be obtained in the University ID Office and are subject to a replacement fee.

f. Temporary Access Cards

(1) Approved university contractors or vendors may request short-term access using short-term identification cards. Such cards should have defined start and end dates and permit access only to applicable areas of work. Some contractors may be asked to check out physical keys via the Texas Tech University Lock Shop in accordance with OP 61.15, Control and Issue of Keys to University Buildings.

(2) All access by vendors/contractors should be routed through the University Lock Shop, with exception of Hospitality Services and University Student Housing locations. Short-term contractor cards are subject to a fee for both new and replacement cards. Fees may be paid either by the contractor/vendor or by the area or department with a valid FOP. Hospitality Services and University Student Housing creates and issues temporary access cards for their respective facilities.

4. Card Replacement

a. Lost or stolen identification cards should be reported online immediately at www.raidercard.ttu.edu.

(1) Found identification cards can be turned into the University ID Office in person during normal business hours or through campus mail at Mail Stop 2035.

b. All non-functioning cards must be surrendered at the time of replacement. Upon issuance of a replacement card, all remaining balances and door access will be transferred to the new RaiderCard.

c. Fees for initial and replacement cards are subject to change.

d. All lost, stolen, and damaged cards are subject to a replacement fee. The fee will automatically be assessed to a card holder presenting a non-functioning card that has been tampered with (including, but not limited to, hole-punched, gouged, and/or broken with a ragged break).

(1) If a RaiderCard is non-functioning as a result of normal wear and tear caused by swiping the card through authorized equipment, the University ID Office may elect not to assess the fee.

5. Non-Transferability and Card Alteration

a. The RaiderCard may not be altered in any way.

b. RaiderCards are not to be used by anyone other than the person that is pictured and named on the card.

c. Unauthorized use, sharing, alteration, or duplication of a RaiderCard for any purpose will result in immediate confiscation of the card and may result in disciplinary or legal action.

6. Physical Access

a. Permitted Use

(1) Educational & General Facilities

(a) Permanent access to interior building spaces must be requested through the Operations Division Key Management System (KMS) in accordance with OP 61.15, Control and Issue of Keys to University Buildings.

(b) Short-term access for classes or events may be added to an individual's RaiderCard. Such access should be limited to a defined area and include specific start and end dates.

i. Short-term access is defined as access granted for between one day and one long semester—with dates not extended into the next long term. For dates extending into multiple terms, a separate request should be submitted for each term.

ii. Short-term access will be submitted through Operations Division Key Management System (KMS) for review by the applicable area's authorized approver before access is granted. Authorized approvers will be required to consider all requirements (lab safety, training, etc.).

(c) Facilities access will be reviewed through KMS protocols and secondary validation methods to ensure security and consistency between systems.

(2) Auxiliaries

(a) Auxiliary access includes, but is not limited to, Recreational Center, University Student Housing buildings, Hospitality Services, and athletic events.

i University Student Housing access will be granted by a combination of University Student Housing and Hospitality Services.

ii Hospitality Services related access shall be granted by Hospitality Services.

iii Athletic event access will be granted by a combination of the University ID Office and Athletics.

iv Recreational Center access will be granted by Recreational Center staff.

b. Door Schedules

(1) Door schedules should be determined with input from the department requesting the door schedule and Operations Division Information Systems.

(2) All Hospitality Services and University Student Housing door schedules will be determined by their respective departments.

7. System Access

a. Access to CS Gold requires eRaider authentication for standard users.

b. Authorized users must comply with all security protocols and acceptable use standards.

c. Users must complete and sign a confidentiality agreement in order to gain access to the CS Gold system. Current FERPA training must be maintained for all users.

d. Permissions granted in the CS Gold system should be limited to a user's specific functional purpose.

e. Access to the CS Gold system will be limited to authorized individuals who have been approved through the Security Protocol Workgroup.

f. The Security Protocol Workgroup will be responsible for the following:

(1) Review and approval of the existing security groups and the creation of new groups

(2) Review and approval of current users

(3) Review and approval of new user access requests

(a) Users must first comply with existing security protocol before they may be added to an existing approved group.

g. Review Protocol

(1) Users of the CS Gold system are to be reviewed monthly by the group's owner(s) to ensure appropriate access levels for each user's current position.

(2) User groups within CS Gold are to be reviewed quarterly to ensure appropriate levels of access.

8. System Security

a. Data transfers must adhere to security standards defined by Texas Tech University Information Technology and Operations Division and in accordance with TTU OP 52.04, Information Technology (IT) Security.

b. Device Installation Protocol

(1) Installed devices should have geofencing completed for the location by the installer.

(2) Devices installed in a University Student Housing location will be updated in the database to reflect an offsite location that is non-accessible from TTU Campus.