UTEP Standard 4: Access Management

The access granted to authorized individuals (e.g., employees, students, vendors, contractors, retirees, others, etc.) to UTEP non-public Information Resources (IR) is a privilege, not a right. The University may limit, restrict, deny or extend access to its Information Resources in any manner that may be required to protect information held confidential by law, to protect the integrity of the contents of data, and to provide for orderly and efficient use of Information Resources. Information Resources usage may be subject to security testing and monitoring by Information Security Office (ISO) authorized individual(s) within the University at any time without the knowledge of the Information Resources user and/or owner.

4.1 Access Management Requirement. Information Resource accounts are the means used to grant access to UTEP's Information Resources. These processes ensure that access to Information Resources are restricted to authorized Users.

Authorized users of University Information Resources are:

i. University students who are limited to the use of those Information Resources specifically assigned to serve educational purposes;

ii. University employees who are provided access to those Information Resources required for the performance of their duties in the conduct of official business. Access to any particular administrative data file/system must be based on an employee's "need to know" as established by their official duties and reflected in the advance provision of specific authorization codes, passwords or other access-enabling means to the employee;

iii. University retirees who are afforded WiFi/UTEPSecure access; and

iv. Non University-affiliated individuals or entities after written agreement for purposes related to the University's missions.

(a) All UTEP offices or departments that create access accounts for networks, applications, or systems are required to manage the accounts in accordance with defined processes and the requirements of the U. T. System Identity Management Federation Member Operating Practices (MOP).

(b) Access to an Information Resource may not be granted by another user without the permission of the Owner or the Owner's delegated custodian of the Information Resource.

4.2 Access Management Process. All accounts that access non-public University Information Resources must follow an account creation process. This process shall document and state, via an associated Service Desk Request associated with the account, the purpose for which the account was created, level of access being requested, and who approved the creation of the account. All accounts wishing to access the University's non-public Information Resources must have the approval of the Owner of those resources. These measures also apply to accounts created by/for use of outside vendors or contractors. All accounts created are to be created and managed using the following required account management practices:

(a) assigning a unique identifier for each applicant, student, employee, insured dependent, research subject, patient, alumnus, donor, contractor, and other individuals, as applicable, at the earliest possible point of contact between the individual and UTEP;

(b) creating uniquely identifiable accounts for all users and Vendors (see also Standard 22), and provisioning accounts for all new and future date employees as soon as new employee record is provided by the current UTEP HRMS system;

(c) disabling all generic and default accounts;

(d) Data/System Owners, System Administrators, and/or other authorized personnel are responsible for reviewing, removing and/or disabling accounts in a timely manner, or more often if warranted by risk, to reflect current User needs or changes to User roles or employment status. Unless otherwise documented and approved by the ISO, please follow the guidelines established below:

    i. disabling accounts for individuals separated from their relationship with UTEP within 120 days for faculty and 60 days for staff;

    ii. disabling new user accounts if not accessed within 30 days of creation;

    iii. disabling individuals on extended leave for more than 120 days;

    iv. disabling any accounts immediately upon notification by ISO;

    v. documenting a process to modify a user account to accommodate situations such as name changes, status or role change, accounting changes and permission changes to reflect their current status;

    vi. documenting a process for reviewing existing accounts for validity at least annually and for reflecting their current status;

vii. enabling password aging and expiration dates, where supported by the underlying accounting mechanism, on all accounts created for outside vendors, external contractors, or those with contractually limited access to the University's information resources;

viii. are subject to independent audit review;

ix. providing a list of accounts for the systems they administer when requested by the ISO;

x. cooperating with ISO personnel investigating security incidents.

(e) expiring passwords or disabling accounts based on risk. It will be the responsibility of the employing or sponsoring department/college to notify Human Resources and/or the Information Security Office when this occurs;

(f) managing access for wired and wireless devices and from remote locations. This is the sole responsibility of the Telecommunications Infrastructure (TI) group; and

(g) default passwords for accounts must be constructed in accordance with UTEP Passwords Standard.

4.3 Remote and Wireless Access. Remote and wireless access to UTEP’s Network Infrastructure must be managed to preserve confidentiality, integrity, and availability (CIA) of UTEP Information. All devices connecting to remote and wireless UTEP Information Resources (e.g., personal computers, cellular phones, PDAs, tablets, etc.) or any other technology (including any form of wireless communication device capable of transmitting packet data) must abide by all standards and policies relating to the Acceptable Use of Information Resources. By the use of these technologies, users acknowledge and understand that their systems are a de facto extension of UTEP’s network, and as such are subject to the same rules and regulations that apply to UTEP-owned equipment (i.e., their devices must be configured to comply with The University of Texas at El Paso Information Resources Use and Security Policies and Standards. Users agree to bear the responsibility for the consequences should the access be misused. The following guidelines also apply:

(a) In the course of monitoring individuals improperly using University Resources, or in the course of system maintenance, the activities of authorized users may also be monitored.

(b) Individuals (authorized or unauthorized) using a wired or wireless network should proceed as if there were no guarantee of security or no expectation of privacy except as otherwise provided by applicable privacy laws. Therefore, it is recommended that information of a personal nature, Controlled Unclassified Information (CUI), or information protected by FERPA, HIPAA, PCI, etc. or any information a user would or should consider Confidential or Controlled not be transmitted over a wireless network. Only approved individuals may utilize UTEP's VPN connection;

(c) users are required to use secure and encrypted connections when accessing Information Resources containing Confidential Data across the Internet, or across open segments of the UTEP network or wireless network (e.g., use of VPN for access, SFTP for transfers, encrypted wireless, encrypted email, etc.);

(d) unauthorized (i.e., rogue) wireless access points or networks operating on campus without the permission of the TI group or any device found to be interfering with the UTEP network are within the scope of this document and subject to monitoring, disabling, confiscation and/or removal from service. VPN dual (split) tunneling is NOT permitted; only one network connection is allowed;

(e) users with remote access privileges to UTEP Information Resources (e.g., network, devices, etc.) must not use non-UTEP email accounts (e.g., Hotmail, Yahoo, AOL, Google mail, etc.), or other external resources to conduct University business; thereby ensuring that official business is never confused with personal business, and that University Information Resources and/or Confidential Data are not placed at risk;

(f) devices must have an anti-virus software installed and enabled. Anti-virus software should be configured to update signatures or definitions daily and scan at least weekly; on-demand option should be enabled. The firewall should also be enabled. Note that these requirements also apply to personal computers and devices accessing UTEP Information Resources, as well as third party connections;

(g) remote users may connect to UTEP Information Resources only through an ISP and using protocols approved by the University;

(h) installation, engineering, maintenance, and operation of wired and wireless networks serving University faculty, staff, or students, on any property owned or tenanted by the University, are the sole responsibility of the TI group. Individuals and departments are prohibited from extending university networks through means wireless technologies.

4.4 Access to UTEP Networks. The TI group is charged with maintaining the Network Infrastructure and is required to establish processes for approval of all network hardware connected to the UTEP network or UT System network and the methods and requirements for attachment, including any non-UTEP owned computer systems or devices, to ensure that such access does not compromise the operations and reliability of the network, or compromise the integrity or use of information contained within the network.

(a) Creation of Service Desk requests are required for approval or rejection, and must be routed through TI for all access methods, installation of all network hardware connected to the local area network (LAN), and methods and requirements for attachment of any computer system or devices to any university network. A business justification must be provided along with a point of contact and any pertinent device information;

(b) Creation of Service Desk requests, routed through TI and approved or rejected by the ISO, are required for issuance of static IP addresses, DNS entries, or MAC authentication of devices. A business justification must be provided along with a point of contact and any pertinent device information;

(c) Creation of a Service Desk request, routed through TI for and approved or rejected by the ISO, are required for use of departmental firewalls or firewall exceptions. Their use is not permitted without appropriate ISO authorization;

(d) Users are permitted to use only those network addresses issued to them by the UTEP TI group;

(e) Users inside the UTEP firewall may not be connected to the UTEP network at the same time a modem or other like device is being used to connect to an external network;

(f) Users must not install network hardware or software that provides network services, and must not extend or re-transmit network services in any way (e.g., router, switch, hub, or wireless access point, etc.) without the approval of the UTEP TI group;

(g) Use of security programs or utilities that reveal weaknesses in the security of the network and/or any Information Resource, or the use of password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the UTEP network infrastructure are expressly prohibited;

(h) Users are not permitted to alter network hardware in any way;

(i) Non-University devices that require network connectivity must conform to The UTEP Information Resources Use and Security Policies, Standards, and Guidelines;

(j) IP addresses belonging to the University must not be registered or recorded with any domain name registration service(s) for any purpose whatsoever;

(k) Hosting of any .com, .org, or .net sites without seeking prior approval from the ISO is strictly prohibited.

4.5 Data Access Control Requirements. All Owners and Custodians must control and monitor access to Data within their scope of responsibility based on Data sensitivity and risk and through use of appropriate administrative, physical, and technical safeguards including the following:

(a) Owners must limit access to records containing Confidential Data to those employees who need access for the performance of the employees' job responsibilities.

i. an employee may not access Confidential Data if it is not necessary and relevant to the employee's job function.

(b) Owners and Custodians must monitor access to records containing Confidential Data by the use of appropriate measures as determined by applicable policies, standards, procedures, and regulatory requirements. Access must be properly documented, authorized, and controlled.

(c) Owners and custodians must follow log capture and review processes based on risk and applicable policies, standards, procedures, and regulatory requirements (See 17.4). Such processes must include the:

i. data elements to be captured in logs;

ii. time interval for custodial review of the logs; and

iii. appropriate retention period for logs.

(d) Employees may not disclose Confidential Data to unauthorized persons or Institutions except:

i. as required or permitted by law;

ii. with the consent of the Data Owner;

iii. where the third-party is the agent or contractor for the Institution and the safeguards described in Standard 4.6 are in place to prevent unauthorized distribution; or

iv. as approved by the UTEP's Legal Office or the Office of General Counsel.

4.6 Access for Third-Parties. If University Data is provided to a third-party acting as an agent of, or otherwise on behalf of, UTEP (e.g., application service provider) a written, signed Third-Party Agreement is required along with UTEP Standard 2: Information Resources Acceptable Use and Security Policy Agreement. Vendor must comply with all applicable UTEP Policies, Standards and Agreements.

(a) Such third-party agreements must specify:

   i. the data authorized to be accessed;

   ii. the circumstances under the purposes for which the Data may be used;

   iii. that all Data must be returned to UTEP, or destroyed, in a manner specified upon end of the third-party engagement; and

   iv. how UTEP information is to be protected by the vendor.

(b) If UTEP determines that its provision of Data to a third-party will result in significant risk to the confidentiality, availability, or integrity of such Data, the agreement must specify terms and conditions, including appropriate administrative, physical, and technical safeguards for protecting the Data.

4.7 Two-Factor Authentication Requirements. Effective August 31, 2015, two-factor authentication is required in the following situations:

(a) when an employee or individual working on behalf of the University such as a student worker, contractor, retiree, or volunteer logs onto a University network using a browser or an enterprise remote access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;

(b) when a retiree logs onto a University network using a browser or an enterprise remote access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;

(c) when an individual working from a remote location uses an online function such as web page to modify employee banking, tax, or financial information; or

(d) when a server administrator or other individual working from a remote location uses administrator credentials to access a server that contains or has access to Confidential University Data.

Effective November 9, 2018, two-factor authentication is required:

(e) when an individual described in 4.7(a-b) above who is working from a Remote Location accesses a web-based interface to University mail.

(f) Requests for other exceptions to this policy may be submitted to the Chief Information Security Officer at security@utep.edu.

Effective February 15, 2019, two-factor authentication is required to be used by faculty, staff, or retirees:

(g) when accessing UTEP’s Microsoft Outlook Web Access (OWA) application remotely (off campus).

4.8 Spam. Spam is the use of electronic messaging systems to send unsolicited email including personal or commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services.

(a) It is prohibited to:

i. create, send, or forward irrelevant or inappropriate messages as this consumes time and resources;

ii. send mass emails without using the approved bulletin process;

iii. send email under another individual’s name or email; or

iv. purposefully engage in activity that may harass, threaten, intimidate, or abuse others. Contact the Campus Police or the ISO if you receive threatening/harassing email.

(b) Forward all spam and chain letters to spam@utep.edu or security@utep.edu.

4.9 Phishing. Phishing is the term used to describe an email that attempts to obtain sensitive information from the recipient by masquerading as a legitimate/trustworthy entity, and may include links to web sites or attachments containing malware.

(a) Never provide the following information:

i. User name(s) and/or password(s);

ii. Credit card or bank account/routing numbers;

iii. Social security number; or

iv. IRS tax information.

(b) Never click, open or respond to a suspected phishing email. When in doubt, please forward the original email as an attachment to security@utep.edu.

(c) If you inadvertently respond to a suspected phishing email, please change your password immediately.

4.10 Revision History

Created: May 11, 2017 (to align with UTS165)
Approved: June 16, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer
Revised: June 12, 2018 Reference to Controlled Unclassified Information (CUI) incorporated into 4.3 (a). Effective November 9, 2018: addition of 4.7 (d) require use of 2FA when accessing web-based interface to University mail from

a Remote Location; and 4.7 (e) exceptions to policy must be submitted to CISO (to align with UTS directive).

Approved: June 12, 2018
Gerard D. Cochrane Jr., Chief Information Security Officer

Revised: January 10, 2019: 4.2 (d) i. correction for disabling accounts within a number of days based on account type; and addition of 4.7 (f) to require use of 2FA to access OWA application remotely by faculty and staff.

Approved: January 10, 2019
Gerard D. Cochrane Jr., Chief Information Security Officer

Revised: June 6, 2019: Grant UTEP Retirees access to UTEPSecure/ WiFi access [new 4.1 iii; and 4.7 (b)]; 4.3(a) expand to include no expectation of privacy, etc.; fix broken links

Approved: June 14, 2019
Gerard D. Cochrane Jr., Chief Information Security Officer