The University of Texas at El Paso
Information Resources Use and Security Policy

1.4 Applicability

1.4.1 This Policy applies to:

(a) all Information Resources owned, leased, operated, or under the custodial care of the University, organization, or facility;

(b) all Information Resources owned, leased, operated, or under the custodial care of third-parties operated on behalf of the University, organization, or facility; and

(c) all individuals accessing, using, holding, or managing University Information Resources on behalf of the University.

1.5 Compliance with State Law

Information that is collected pursuant to or that is related to any University Information Security Program is subject to [illegible]

(m) UTEP Standard 13: Control and Protection of Social Security Numbers

(n) UTEP Standard 14: Information Services (IS) Privacy

(o) UTEP Standard 15: Passwords

(p) UTEP Standard 16: Data Center Security

(q) UTEP Standard 17: Security Monitoring

(r) UTEP Standard 18: Security Training

(s) UTEP Standard 19: Server and Device Configuration and Management

(t) UTEP Standard 20: Software Licensing

(u) UTEP Standard 21: System Development and Deployment

(v) UTEP Standard 22: Vendor Controls and Compliance (coming soon)

(w) UTEP Standard 23: Security Control Exceptions

(x) UTEP Standard 24: Disciplinary Actions

1.8 Definitions

(a) **Authentication**: A process used to verify one's identity.

(b) **Backup**: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system failure or other data loss event.

(c) **Centralized IT**: The institutional information technology services and support organization, reporting to the highest-ranking information technology administrator/officer in the institution, that support institutional legacy administrative systems or enterprise resource planning (ERP) systems such as student administration (admissions, financial aid, registration, etc.), financial information systems, procurement systems, human resource systems, payroll, research administration (grants and contracts), Network Infrastructure, institutional electronic communications, video, library systems, etc.

(d) **Change**: Any addition or removal of, and any modification or update to, an Information Resource.

(e) **Change Management**: Process of controlling the communication, approval, implementation, and documentation of modifications to hardware, software, and procedures to ensure that information resources are protected against improper modification before, during, and after system implementation.

(f) **Chief Administrative Officer**: The highest ranking executive officer at each institution. For most institutions, this is the President.

(g) **Cloud Computing (Cloud Services)**: Has the same meaning as

(n) **Decentralized IT**: Information technology service and support organizations reporting to the heads of business units, departments, or programs that manage or support their own information systems.

(o) **Digital Data**: The subset of Data (as defined above) that is transmitted by, maintained, or made available in electronic media.

(p) **Emergency Change**: A change to an Information Resource made in response to unexpected events or circumstances that pose a threat to the environment or institution and thereby justify use of expedited change procedures.

(q) **Electronic Communication**: Method used to convey a message or exchange information via Electronic Media instead of paper media. It includes the use of Electronic Mail, instant messaging, Short Message Service (SMS), facsimile transmission, Social Media, and other paperless means of communication.

p-3(a)5(l)-3(t)2na7pe(c)-15 -1.1ihSs and otiiriTJ 0 T

departments, vendors, and any third-party acting as an agent of or otherwise on behalf of an institution.

(z) **Information Resources Manager (IRM)**: The executive responsible for IT across the whole of the institution as defined in Texas Government Code, Chapter 2054, Subchapter D. The IRM retains ultimate responsibility for enforcement of the Business Continuity Plan for Disaster Recovery, and all security and risk management policies.

(aa) **Information Resources Owner (Owner)**: The manager or agent responsible for the business function that is supported by the Information Resource or the individual upon whom responsibility rests for carrying out the program that uses the resources. The Owner is responsible for establishing the controls that provide the security and authorizing access to the Information Resource. The Owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared. NOTE: In the context of this Information Security Policy and Standards, Owner is a role that has security responsibilities assigned to it by Texas Administrative Code (TAC), Section 202.72; it does not imply legal ownership of an Information Resource. All University Information Resources are legally owned by The University of Texas System or the member institution.

(bb) **Information Security Administrator**: A departmental employee, designated by management, who assists with information security tasks as described in UTS165 Standard 1 - Information Resources Security Responsibilities and Accountability.

(cc) **Information Security Program**: The Policies, Standards, Procedures, Guidelines, elements, structure, strategies, objectives, plans, metrics, reports, resources, and services adopted for the purpose of securing University Information Resources.

(dd) **Information System**: An interconnected set of Information Resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, Network Infrastructure, information, data, applications, communications, and people.

(ee) **Information Technology (IT)**: The hardware, software, services, supplies, personnel, facilities, maintenance, and training used for the processing of data and telecommunications.

(ff) **Inherent Impact**

(gg) **Institution**: U.T. System Administration, The University of Texas Management Company ("UTIMCO"), or any individual University that is a component of The University of Texas System. (Used interchangeably with "University".)

(hh) **Integrity**: The accuracy and completeness of information and assets, and the authenticity of transactions.

(ii) **Internet**: A global system interconnecting computers and public computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and institutions.

(jj) **Lead Researcher**: The person engaged in the conduct of Research with primary responsibility for stewardship of Research Data on behalf of an Institution. For the purpose of this Policy, the term is synonymous with Principal Investigator.

(kk) **Local Area Network (LAN)**: A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

(ll) **Low Impact Information Resources**: Information resources whose loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

i. cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;

ii. result in minor damage to organizational assets;

iii. result in minor financial loss; or

iv. result in minor harm to individuals.

(mm) **Malware**: A computer program that is inserted into an Information System, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of data, applications, or operating system, or of otherwise disturbing or disrupting the User or Information System. Malware (malicious software) may attach itself to a file or application; deliver a payload without the knowledge or permission of the User; insert itself as a service or process to intercept sensitive information and/or keystrokes and deliver it to a third-party; or compromise the User's computer and use it to launch compromises against other computers, among other capabilities. Viruses, worms, Trojan horses, spyware, adware, ransomware, and any code-based entity that infects a host are examples of malicious software.

(nn) **Mission Critical Information Resources**: Information Resources defined by an Institution or State agency to be essential to U.T. System or the Institution's ability to meet its instructional, research, patient care, or public service missions. The loss of these resources or inability to restore them in a timely fashion would result in the failure of U.T. System or Institution's operations, inability to comply with regulations or legal obligations, negative legal or financial impact, or endanger the health and safety of faculty, students, staff, and patients. Mission Critical Information Resources include but are not limited to:

i. Information Systems managing Confidential Data;

ii. Common Use Infrastructures;

iii. Institutional Network and Data Center Infrastructure;

iv. Identity and Access Management Systems, such as single-sign-on or other applications required to enable access to other critical system;

v. Administrative systems (e.g., HR, Finance, Payroll, student/patient enrollment and billing, etc.);

vi. Student information systems;

vii. Patient care and life-support systems, etc.

(oo) **Moderate Impact Information Resources**: Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

i. cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;

ii. result in significant damage to organizational assets;

iii. result in significant financial loss; or

iv. result in significant harm to individuals that does not involve loss o03 0 life or serious life threatening injuries.

(pp) **Network Infrastructure**: The distributed hardware and so03 0tware (i.e., cabling, routers, switches, wireless access points, access methods, and prot

(qq) **Non-University Owned Computing Device**: Any device that is capable of receiving, transmitting, and/or storing electronic data, and that is not owned, leased, or under the management of an Institution including personally owned devices.

(rr) **Password**: A string of characters used to verify or "authenticate" a person's identity.

(bbb) **Research**: Systematic investigation designed to develop and contribute to knowledge and may include all stages of development, testing and evaluation.

(ccc) **Researcher**: Faculty, staff, graduate students, postdoctoral fellows, residents, visiting/affiliated scientists or lead researchers who are engaged in or responsible for Research activities.

(ddd) **Risk**: A function of the likelihood that a threat will exploit a vulnerability and the resulting impact to University missions, functions, image, reputation, assets, or constituencies if such an exploit were to occur.

(eee) **Scheduled Change**: A change to an Information Resource made under normal working conditions following formally prescribed change management control processes as defined in UTS 165 Standard 7 - Change Management.

(fff) **Security Incident**: An event that results in unauthorized access, loss, disclosure, modification, disruption, or destruction of Information Resources whether accidental or deliberate.

(ggg) **Server**: A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.

(hhh) **Social Media**: A forum or media for social interaction, using highly accessible and scalable communication techniques. Examples include but are not limited to wikis (e.g., Wikia, Wikimedia); blogs and microblogs (e.g., Blogger, Twitter); content communities (e.g., Flickr, YouTube); social networking sites (e.g., Facebook, MySpace, Linsh-pace,nsh-e.