UTEP Standard 1: Information Resources Security Requirements and Accountability

1.1 Designation of Responsibility. All Institutions and any U.T. System governing body having oversight of Information Resources must have designated and documented roles and responsibilities for the information security function.

1.2 Chancellor. The Chancellor shall:

(a) designate an individual to serve as U.T. System Chief Information Security Officer (CISO);

(b) budget sufficient resources to fund ongoing information security remediation, implementation, and compliance activities that reduce compliance Risk to an acceptable level; and

(c) ensure that appropriate corrective and disciplinary action is taken in the event of noncompliance.

1.3 Chief Administrative Officers (CAO). The Chief Administrative Officers at each Institution shall:

(a) ensure the Institution's compliance with this Policy and associated Standards;

(b) designate an individual to serve as the Chief Information Security Officer (CISO) who shall:

i. serve in the capacity as required by 1 Texas Administrative Code 202.71 (b) with authority for that entire Institution;

ii. report to the President or to a senior executive, other than the Chief Information Officer or Information Resources Manager, who reports to the President; and

iii. have a dotted line reporting relationship to the UTEP Compliance Officer and the UT System Chief Information Security Officer;

(c) budget sufficient resources to fund ongoing information security remediation, implementation, and compliance activities (e.g., staffing, training, tools, and monitoring activities) that reduce compliance Risk to documented acceptable levels;

(d) approve the Institution's Information Security Program; and

(e) ensure appropriate corrective and disciplinary action is taken in the event of noncompliance.

1.4 Information Resources Manager (IRM). The IRM shall:

(a) implement security controls in accordance with UTEP's Information Security Program; and

(b) review and approve or disallow the purchase or deployment of new Decentralized IT Information Systems or services (e.g., electronic mail/web/file servers, file/system backup, storage, etc.) that duplicate services provided by Centralized IT.

1.5 U.T. System Chief Information Security Officer (U.T. System CISO). The U.T. System Chief Information Security Officer shall:

(a) provide leadership, strategic direction, and coordination for the U. T. Systemwide Information Security Program including issuing of Policies, Standards, Procedures, and Guidelines;

(b) chair and hold meetings of the U.T. System CISO Council at least quarterly;

(c) develop and oversee the U.T. Systemwide Information Security Compliance Program;

(d) provide guidance relating to Institutional and Common Use Infrastructures Information Security Programs regarding organizational duties and responsibilities, covered activities, authority to act, terminology definitions, standard methodologies, and minimum Standards;

(e) define the Risk management process to be used for U.T. System information security Risk management activities, and ensure performance of Risk assessment for systemwide systems that will process or store Confidential Data;

(f) explore and recommend the acquisition of cybersecurity tools, resources, and services that can be utilized by multiple U.T. Institutions and for ways to share expertise among Institutions;

(g) establish reporting requirements, metrics, and timelines and monitor effectiveness of security strategies at each Institution;

(h) apprise the Chancellor, the U.T. System Executive Compliance Committee, and the Board of Regents on the status and effectiveness of the Information Security Compliance Programs;

(i) oversee and/or monitor deployment of information security initiatives funded or sponsored through the U.T. System, and manage contracts with service providers;

(j) establish processes for assessing information security proposals for U.T. System sponsorship, and oversee procurements; and

(k) appoint an Information Security Officer for Common Use Infrastructures.

1.6 Information Security Officer for Common Use Infrastructures. The Information Security Officer for Common Use Infrastructures is responsible for defining, implementing, and managing an Information Security Program encompassing the U. T. System Common Use Infrastructures in accordance with requirements of the U. T. Systemwide Information Security Program and shall:

(a) develop and maintain a current and comprehensive Information Security Program, that includes Risk assessment, metrics, action plans, training plans, monitoring plans, and adoption of Policies, Standards, Procedures, and/or Guidelines as needed;

(b) coordinate with Institutional Information Security Officers, Information Resource Managers, facilities management, and governance groups to ensure appropriate Policies, Standards, Procedures, and/or Guidelines are established, and responsible parties are assigned;

(c) monitor the effectiveness of security controls and submit required reports to the U.T. System Chief Information Security Officer; and

(d) serve as a member of the U.T. System Chief Information Security Officer Council, and perform other tasks similar in nature to an Institutional Information Security Officer.

1.7 UTEP Chief Information Security Officer (CISO). The UTEP CISO is the individual responsible for UTEP's Information Security Program and shall:

(a) work in partnership with the University community, constituency groups, and leadership to establish effective and secure processes and information systems and to promote information security as a core institutional value;

(b) provide information security oversight for all Centralized and Decentralized IT Information Resources;

(c) develop and maintain a current and comprehensive Information Security Program, that includes risk assessment, action plans, training plans, monitoring plans, and specific risk mitigation

strategies to be used by Owners and Custodians of Mission Critical Information Resources to manage identified risks;

(d) develop Institutional Policies, Standards, Procedures, and/or Guidelines to ensure that the protection of Information Resources is considered during the development or purchase of new computer applications or services;

(e) develop or adopt a Data Classification Standard that conforms or maps to UTS165 Standard 9 – Data Classification;

(f) coordinate Risk assessments required by UT System to be reported to the UT System Executive Compliance Committee or Board of Regents, and ensure that annual information security risk assessments are performed and documented by Owners of Mission Critical Information Resources and Information Resources containing Confidential Data in accordance with UTEP Standard 10: Risk Management;

(g) ensure that each Owner of Mission Critical Information Resources has designated an Information Security Administrator (ISA);

(h) establish an Institutional Information Security Working Group composed of ISAs (ISA Working Group) and convene meetings at least quarterly;

(i) approve and document any exceptions to information security Policies or Standards, other than UTEP Standard 2: Acceptable Use of Information Resources, within the Institution in accordance with UTEP Standard 23: Security Control Exceptions;

(j) document and justify, in collaboration with the Owners, exceptions to specific elements of the program required due to circumstances within a specific organizational unit(s) within an Institution, and include such exceptions in the annual report to the Chief Administrative Officer;

(k) establish reporting requirements, metrics, and timelines, and monitor effectiveness of security strategies implemented in both Centralized and Decentralized IT;

(l) perform, at minimum, an annual vulnerability assessment of Information Resources maintained in both Centralized and Decentralized IT and track implementation of any remediation required as a result of the assessment;

(m) ensure that an annual external network penetration test is performed and track implementation of needed risk remediation;

(n) specify and require use of appropriate security software such as antimalware, firewall, configuration management, and other security related software on Computing Devices owned, leased, or under the custody of any department, operating unit, employee, or other individual providing services to the Institution;

(o) establish and communicate security configuration requirements and Guidelines;

(p) ensure Computing Devices are administered by appropriately trained staff and in accordance with Policies, Standards, and Procedures;

(q) review the security requirements, specifications, and, third-party risk assessments of any new computer applications or services that receive, maintain, and/or share Confidential Data;

(r) approve security requirements for the purchase of Information Technology hardware, software, and systems development services;

(s) ensure all employees receive periodic information security training appropriate to the security role (such as Owner or ISA) of the employee, including high-level information security awareness training as part of each employee's first-time compliance training;

(t) communicate instances of noncompliance to appropriate administrative officers for corrective, restorative, and/or disciplinary action;

(u) investigate Security Incidents and inform the CAO of incidents posing significant risk to individuals, the Institution, or other organizations;

(v) report significant information security incidents, as defined by the UT System Security Incident Reporting Requirements, to the UT System CISO;

(w) participate in the UT System CISO Council meetings, workgroups, and related activities;

(x) report to the UT System CISO in accordance with Program reporting guidance and metrics;

(y) provide updates to the Institutional Compliance Committee regarding information security risks and issues; and

(z) provide a report, at least annually, to the CAO with copies to the Institution's CIO and Compliance Officer and the UT System CISO on the status and effectiveness of Information Resources security controls for the whole Institution in accordance with reporting instructions provided by the UT System CISO.

1.8 Department Heads and Lead Researchers. Department Heads and Lead Researchers at UTEP shall classify and appropriately secure Data under their control including Data held in relation to subcontracts for projects in which the prime award is at another Institution or Agency.

1.9 Information Resources Owners. For Information Resources and Data under their authority, Owners shall:

(a) grant access to Information Systems and Data;

(b) control and monitor access to data based on data sensitivity and risk;

(c) classify data based on the Institution's Data Classification Standard;

(d) conduct risk assessments that identify the Information Resources under their authority and the level of risk associated with the Information Resources and the vulnerabilities, if any, to the Institution's information security environment;

(e) define, recommend, and document acceptable risk levels for Information Resources and risk mitigation strategies;

(f) document and justify, in collaboration with the ISO, any exceptions to specific program requirements due to extenuating circumstances within the Owner's area of responsibility;

(g) ensure data is securely backed up in accordance with risk management decisions;

(h) ensure data is maintained in accordance with the applicable University records retention schedule and procedures;

(i) provide documented permission and justification for any User who is to store Confidential University Data on a Portable Computing Device or a Non-University Owned Computing Device;

(j) ensure that High Risk Computing Devices and Confidential Data are encrypted in accordance with requirements specified in UTS165 Standard 11 - Safeguarding Data;

(k) ensure that Information Resources under their authority are administered by qualified Information Resources Custodians;

(l) ensure that a risk assessment is performed prior to purchase of any software that has not been previously assessed by the Institution for use under similar circumstances;

(m) ensure that a third-party risk assessment is performed prior to purchase of Vendor services involving or accessing University Data; and

(n) ensure contracts involving products or services that impact Information Resources contain information security language appropriate to the risk.

1.10 Owner of Mission Critical Information Resources. For Information Resources under the Owner's authority, the Owner shall:

(a) designate an individual to serve as an Information Security Administrator (ISA) to implement information security Policies and Procedures and to report incidents to the ISO;

(b) provide for appropriate training for ISAs to ensure effective security practices;

(c) perform an annual information security risk assessment that identifies Information Resources, levels of associated risk, and any vulnerabilities to those Information Resources;

(d) define, recommend, and document acceptable risk levels for Information Resources and risk mitigation strategies as needed; and

(e) adopt a disaster recovery plan for Information Resources and ensure testing is performed in accordance with the requirements of UTEP Standard 6 – Backup and Disaster Recovery.

1.11 Information Resources Custodians. Information Resources Custodians shall:

(a) implement approved risk mitigation strategies and adhere to Information Security Policies and Procedures to manage risk levels for Information Resources under their care;

(b) implement monitoring controls for detecting and reporting incidents;

(c) control and monitor access to Information Resources under the Custodian's care based on sensitivity and risk;

(d) implement and adhere to approved UTEP change management processes to ensure secure, reliable, and stable operations;

(e) encrypt High Risk Computing Devices and Confidential Data in accordance with requirements specified in UTEP Standard 11 - Safeguarding Data;

(f) provide appropriate technical training to employees providing information technology, security, help-desk, or technical support for Information Resources under their responsibility; and

(g) ensure that technical staff under their authority are qualified to perform their assigned duties.

1.12 Information Security Administrator (ISA). Information Security Administrator shall:

(a) implement and comply with all UTEP Policies and Procedures relating to assigned Information Systems;

(b) assist Owners in performing annual information security Risk assessments;

(c) report general computing and Security Incidents to the ISO;

(d) as a member of the ISA Work Group, assist the ISO in developing, implementing, and monitoring the Information Security Program, and in establishing reporting guidance, metrics, and timelines for the ISO to monitor effectiveness of security strategies; and

(e) report at least annually to the ISO about the status and effectiveness of Information Resources security controls.

(f) provide assistance to individuals responsible for the information security function;

(g) assist with acquisition and maintenance of system hardware/software;

(h) assist with identification of vulnerabilities;

(i) develop / maintain access control rules; and

(j) maintain user lists, password control, encryption keys, etc.

1.13 Institutional Offices with Designated Responsibility for Account Management. Each office within the Institution responsible for account management shall manage accounts in accordance with this Policy and all

other applicable UTEP Information Security Policies, Standards, Procedures, and Guidelines.

1.14 Institutional Office Designated with Responsibility for Network Infrastructure. Each office so designated shall be responsible for:

(a) configuring and managing network resources in accordance with this Policy and all other applicable UTEP Information Security Policies, Standards, Procedures, and Guidelines;

(b) segmenting the UTEP network physically or logically to reduce the scope of potential exposure of Information Resources in the event of a security incident;

(c) separating Internet facing applications from internal applications;

(d) maintaining appropriate access to the Network Infrastructure in accordance with this Policy and all other applicable UTEP Information Security Policies, Standards, Procedures, and Guidelines;

(e) managing, testing, and updating operating systems and applications for network equipment for which it is responsible; and

(f) approving all access methods, installation of all network hardware connected to the local-area network and methods and requirements for attachment of any non-UTEP owned computer systems or devices to the UTEP network.

1.15 Information Resources and Planning Charged with Supporting Information Resources. The office so designated shall be responsible for:

(a) Formalizing best Practice Change Management processes into Practice Standards;

(b) Requiring compliance from all individuals who manage information Systems and applications; and

(c) Providing support, guidance, and problem resolution to Owners, including Department Heads and lead Researchers, and Users with respect to this Policy and applicable Standards, Polices, Procedures and Guidelines.

1.16 Users.

(a) All Users must comply with this Policy. Users who fail to comply are subject to disciplinary action in accordance with UTEP Standard 24–Disciplinary Actions.

(b) All Users who are University employees, including student employees, or who are otherwise serving as an agent or are working on behalf of the University must formally acknowledge and comply with UTEP's Information Resources Acceptable Use and Security Policy Standard 2 – Acceptable Use of Information Resources.

1.17 Revision History

Complete Rewrite based on UTS165: May 9, 2017

Approved: May 9, 2017

Gerard D. Cochrane Jr., Chief Information Security Officer