UTEP Standard 12: Security Incident Management

12.1 Reporting Requirements. Security Incidents will be reported as required by State and Federal law and University Policy including U.T. System Information Security Incident Reporting Requirements.

12.2 Incident Management Procedures. This section describes the procedures for computer security incidents. Security incidents include, but are not limited to, unauthorized use of Information Resources accounts, as well as complaints of improper use of Information Resources as outlined in UTEP Standard 2: Acceptable Use of Information Resources. The University will establish a Computer Incident Response Team (CIRT) that, in the event of a significant computer security incident, will initiate and follow the Incident Management Procedures. The members of this team will have defined roles and responsibilities that, based on the severity of the incident, may take priority over normal duties. Please refer to the Security Incident Management Process flow chart at the end of this section.

(a) Detection or Reported Incident – incidents involving computer security will be managed by the Information Security Office (ISO) and reported as required by Federal or State law or regulation. All faculty, staff, and/or students shall report promptly any unauthorized or inappropriate disclosure of confidential Digital Data, including Social Security Numbers, to the UTEP CISO (via security@utep.edu or 915-747-6324), their supervisors, and/or the University Institutional Compliance hotline (via 1-888-228-7713 or anonymously online at www.reportlineweb.com/utep).

(b) Response to Incident - the ISO will notify the CISO and respond by opening and Incident Report and following Incident Management Procedures to ensure that each incident is reported, documented, and resolved in a manner that restores operation quickly and, if required, maintains evidence for further disciplinary, legal, or law enforcement actions.

(c) Initial Incident Assessment - an Initial Incident Assessment will be performed to determine whether the incident is classified as Low, Medium, or High impact, as well as any potential damage to Information Resources, etc.

(d) Forensics/Data Gathering – the ISO will determine and preserve what physical and electronic evidence is to be gathered as part of the Incident Investigation, as well as documenting any actions taken to remediate.

(e) Assigning Responsibility for Investigating Incident – the CISO will assign responsibility for gathering, maintaining, and reporting detailed information regarding the incident to the appropriate team member(s). The technical resource is responsible for monitoring

and insuring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.

(f) Escalation – if the incident is deemed Low, the Incident is Resolved. If, however, the incident is deemed Medium or High, the CISO will escalate the Incident by notifying the appropriate UTEP and U.T. System CISO, residents of Texas, Data Owners, Federal and State agencies, and consumer reporting agencies as required by applicable State and Federal law and U.T. System Policy.

(g) Time Requirements – disclosure shall be made as quickly as possible upon the discovery or receipt of notification of the incident taking into consideration: 1) the time necessary to determine the scope of the incident and restore the reasonable integrity of operations; or 2) any request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that it will not compromise the investigation.

(h) Notification – The University shall disclose, in accordance with applicable Federal or State law, incidents involving computer security that compromise the security, confidentiality, and/or integrity of personal identifying information it maintains to Data Owners and any resident of Texas whose personal identifying information was, or is reasonably believed to have been, acquired without authorization.

12.3 Employee Reporting. All employees must promptly report unauthorized or inappropriate disclosure of Confidential, Controlled or Protected Data, regardless of medium (e.g., digital, paper, or any other format), to the UTEP Chief Information Security Officer, their supervisor, and/or the University's Institutional Compliance hotline [please refer to 12.2 (a) above].

12.4 Reporting to Information Security Office. Information Resources Owners, Custodians, and any supervisors, directors, or managers who become aware of a Security Incident are to report the incident to the UTEP Chief Information Security Officer, their supervisor, and/or the University's Institutional Compliance hotline [please refer to 12.2 (a) above].

12.5 Reporting Requirements to U.T. System. The UTEP CISO must report significant Security Incidents, as defined by the U.T. System Security Incident Reporting Requirements, to the U.T. System CISO. Security Incidents resulting in unauthorized disclosure of University Data must be reported immediately. The UTEP CISO must report Security Incidents to the U.T. System CISO prior to reporting to non-U.T. System agencies or organizations except as required by State or Federal law.

12.6 Monitoring Techniques and Procedures. Custodians must implement monitoring controls and Procedures for detecting, reporting, retaining, and investigating incidents.

12.7 Revision History

First Draft:	April 2, 2002
Revised:	September 11, 2002
Revised:	July 8, 2011
Revised:	May 12, 2017 (complete rewrite based on new UTS165)
Approved:	May 12, 2017 Gerard D. Cochrane Jr., Chief Information Security Officer

Security Incident Management Process