UTEP Standard 17: Security Monitoring

The purpose of the Security Monitoring Policy is to ensure that Information Resources security controls are in place, are effective, and are not being bypassed. Benefits of security monitoring include the early identification of security issues or new security vulnerabilities. Early identification can help prevent security issues or vulnerabilities before harm can be done, or to minimize the potential impact.

17.1 The Chief Information Security Officer (CISO) must ensure:

(a) that network traffic and use of Information Resources is monitored as authorized by applicable law and only for purposes of fulfilling a the University's mission related duty;

(b) server and network logs are reviewed manually or through automated processes on a scheduled basis based on Risk and regulation to ensure that Information Resources containing Confidential Data are not being inappropriately accessed;

(c) vulnerability assessments are performed annually, at minimum, to identify software and configuration weaknesses within information systems;

(d) professionally administered and reported external network penetration test is performed on an as needed basis; and

(e) that results of log reviews, vulnerability assessments, penetration tests, and IT audits are available to the CISO and that required remediation is implemented.

17.2 Two groups on campus are authorized to routinely monitor traffic on the University's networks. These groups are Telecommunications Infrastructure (Networking Team) and the Information Security Office. Additional campus IT staff may be approved to access and monitor specific traffic on specific networks for which they are responsible. Authorization must be attained from the CISO.

(a) TI-Networking and the ISO have the authority to discontinue service to any network or network device that:

i. is in violation of University Policies or Standards;

ii. has demonstrated an operation hindrance or threat to the University's network; or

iii. is a threat to the Internet community, in general

17.3 Monitoring may consist of activities such as, but not limited to, the review of:

- automated intrusion detection/prevention system logs
- firewall logs
- user account logs
- Internet traffic
- electronic mail traffic
- LAN traffic, protocols, and device inventory
- Network scanning logs
- application logs
- Data backup recovery logs
- Service Desk requests
- other log and error files

17.4 Any security issues discovered will be reported to the ISO for follow-up investigation.

(a) All security-related events on critical or confidential systems must be logged and audit trails saved as follows:

i. All security, system and application related logs will be retained online for a minimum of 90 days;

ii. Daily incremental tape backups will be retained for at least 1 month;

iii. Weekly full tape backups of logs will be retained for at least 3 months;

iv. Backups must be verified at least on a quarterly basis, either through automated verification, through customer restores, or through trial restores; and

v. Monthly full backups will be retained for a minimum of 90 days.

(b) Security-related events will be reported to the Information Security Office, which will review logs and report incidents as appropriate. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

i. port-scan attacks;

ii. evidence of unauthorized access to privileged or user accounts;

iii. anomalous occurrences that are not related to specific applications on the host;

iv. web defacement or compromised server;

v. potential intrusion detection;

vi. compromised user's account;

vii. data breach; or

viii. other security incident

17.5 Revision History

First Draft: April 4, 2002
Revised: September 19, 2002
Revised: December 13, 2011
Revised: May 31, 2017 (align with UTS165)
Approved: June 9, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer