



# Standard Administrative Procedure (SAP)

## 29.01.99.L1.18 Security Awareness

**First Approved:** March 28, 2013  
**Revised:** June 22, 2017  
**Next Scheduled Review:** June 22, 2022

---

### Procedure Statement and Reason for Procedure

---

Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product-specific training. The philosophy of protection and specific security instructions need to be taught to computer users. In addition, security awareness and training information need to be continuously upgraded and reinforced.

The purpose of this SAP is to describe the requirements that ensure each user of Texas A&M International University (TAMIU) Information Resources receives adequate training on computer security issues. This SAP applies to all individuals who use TAMIU Information Resources. This SAP supplements *TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities* and *TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*.

---

### Procedures and Responsibilities

---

1. Security Training
  - 1.1 TAMIU will use the "New Employee Orientation" to educate new employees about Texas A&M University System (TAMUS) policies and regulations and TAMIU rules and standard administrative procedures regarding information resources.
  - 1.2 Annual security awareness training will be required of all employees who access TAMIU Information Resources. The Office of Human Resources and the Information Security Officer (ISO) will be responsible for compliance with this SAP.

- 1.3 Required training for employees is assigned and tracked through the TAMUS TrainTraQ system.
- 1.4 Employees are responsible for keeping up-to-date on rule and procedural changes in TAMIU rules and standard administrative procedures regarding Information Resources.

---

## Related Statutes, Policies, Regulations, or Rules

---

[Texas Administrative Code 202, Subchapter C – Information Security Standards for Institutions of Higher Education](#)

*TAMIU Rule 24.99.01.L1, Security of Electronic Information Resources*

*TAMIU Rule 29.01.99.L1, Use of Information Resources and Facilities*

---

## Appendix

---

### References:

Copyright Act of 1976

Foreign Corrupt Practices Act of 1977

Computer Fraud and Abuse Act of 1986

Computer Security Act of 1987

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The State of Texas Information Act

Texas Government Code, Section 441

Texas Administrative Code, Chapter 202

IRM Act, 2054.075(b)

The State of Texas Penal Code, Chapters 33 and 33A

DIR Practices for Protecting Information Resources Assets

DIR Standards Review and Recommendations Publications

---

## Contact Office

---

Office of Information Technology, 956-326-2310