Standard Administrative Procedure

29.01.00.L1.34  Risk Assessment Guidelines
Approval date: 03/28/13
Revision date: 01/24/13
Next scheduled review date: 01/24/15
Author: Office of Information Technology

Standard Administrative Procedure Statement

General
Information security risk assessments are a vital process for identifying Information Resources that require protection from the loss of information confidentiality, integrity and/or availability.

Applicability
This SAP applies to all users and administrators of Texas A&M International University (TAMIU) Information Resources who perform, approve, or make risk management decisions on information security risk assessments. The purpose of this SAP is to establish guidelines that will assist Information Security Administrators in conducting risk assessments effectively.

Definitions

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Security Administrator: The person responsible for monitoring and implementing security controls and procedures for a system.

ISAAC - Information Security Assessment Awareness and Compliance: This system provides an information security risk assessment methodology and reporting function for individual departments and TAMIU.

Procedures and Responsibilities

1. Guidelines and Procedures
1.1 Risk assessments must be performed annually by the ISAs of each department. Each department head will designate an ISA to perform the risk assessment.

1.2 The IT Security group will schedule meetings with appropriate personnel from TAMIU departments to review their departmental information security risk assessment(s).

1.3 IT Security group will answer any questions departmental personnel have regarding the risk assessment process with the goal of promoting a better understanding and effective use of the ISAAC Risk Assessment process. IT Security group will seek suggestions that may benefit the department regarding clarification and improvement of the risk assessment process and tool(s).

1.4 Upon completion and analysis of the review, IT Security group will provide a report to the department head or director and to any departmental personnel designated by the department head or director.

1.5 System failure scenarios must be included in the disaster recovery plan for each critical server.

**Related Statutes, Policies, Regulations, Rules or Requirements**

TAC 202.75 Security Standards for Institutions of Higher Education

**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**

<table>
<thead>
<tr>
<th><strong>Office of Information Technology</strong></th>
<th><strong>Information Security Officer</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotline: (956) 326-2310</td>
<td>Cuauhtemoc Barrios</td>
</tr>
<tr>
<td>Killam Library 257</td>
<td><a href="mailto:cbarrios@tamiu.edu">cbarrios@tamiu.edu</a></td>
</tr>
</tbody>
</table>

**Office Hours**  
Monday - Friday: 7:30 AM - 6:00 PM  
Saturday - Sunday: Closed  

**IT Security Group**  
itsecurity@tamiu.edu