General
Texas A&M International University (TAMIU) information resources are strategic assets which, as property of the State of Texas, must be managed as valuable State assets. The integrity and continued management of information resources is critical to the operation of the University. However, malicious code can disrupt normal operations of TAMIU’s Information Resources.

Applicability
The purpose of this SAP is to provide procedures and guidelines to improve preparation for, resistance to, and recovery from malicious code. It applies to all individuals who have access to TAMIU Information Resources.

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.

**Malicious Code:** Software which interferes with the normal operation of information resources. It includes, but is not limited to, viruses, worms, Trojan horses, backdoors, and attack scripts.

**Office of Information Technology (OIT):** The name of the TAMIU department responsible for computers, networking and data management.

**Rootkits:** A set of software tools used by a third party after gaining access to a computer system in order to conceal the altering of files, or processes being executed by the third party without the user's knowledge.
1. **Prevention and Detection**

1.1 Understand the risks associated with malicious code and preventative measures that can be reasonably deployed.

1.2 Be aware of and follow the procedures outlined in TAMIU OIT announcements (via web page or email), which will be used to communicate warnings of potential computer virus threats.

1.3 Treat viruses with urgency. Write down the name of the virus if provided by the virus detection software.

1.4 Contact the OIT Help Desk immediately when a computer virus is suspected and/or detected.

1.5 Never boot directly from an external drive until the drive has been scanned for viruses. By default, TAMIU’s antivirus program, Symantec Endpoint, is configured to automatically scan all external disks upon use.

1.6 Ensure files received from external sources are clean of viruses prior to use or distribution, and never use or introduce non-licensed software on any TAMIU computing device.

1.7 Back up critical data (i.e. student/employee information, data related to TAMIU operations, vital mission data, etc.) to a network drive on the server.

2. **Response and Recovery**

2.1 All reasonable efforts will be made to contain the effects of any system that is infected with malicious code. This may include disconnecting systems from the network or disabling email.

2.2 If malicious code is discovered, or believed to exist, OIT will remove or quarantine the malicious code using Symantec Endpoint.

2.3 If malicious code cannot be automatically quarantined or removed by Symantec Endpoint, the system will be disconnected from the network until it can be safely reconnected.

2.4 OIT will identify the source of infection and type of infection to prevent and prepare for future recurrence.

2.5 Any removable media recently used on an infected machine will be scanned prior to opening and/or executing any files contained therein.
2.6 All computers containing rootkits, Trojans, and worms will be re-formatted.

**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
SANS Institute InfoSec Reading Room

**Contact Office**

<table>
<thead>
<tr>
<th>Office of Information Technology</th>
<th>Information Security Officer</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>

<table>
<thead>
<tr>
<th>Office Hours</th>
<th>ITSecurity Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday - Friday: 7:30 AM - 6:00 PM</td>
<td><a href="mailto:itsecurity@tamiu.edu">itsecurity@tamiu.edu</a></td>
</tr>
<tr>
<td>Saturday - Sunday: Closed</td>
<td></td>
</tr>
</tbody>
</table>

Killam Library 257

Information Security Officer
Cuauhtemoc Barrios
cbarrios@tamiu.edu

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