General
Electronic backups are business requirements that enable the recovery of data and applications in case of events such as natural disasters, system disk drive failures, data entry errors, or system operations errors.

Applicability
The purpose of this SAP is to establish the rules for the backup and storage of electronic information. It applies to all individuals within Texas A&M International University (TAMIU) who are responsible for the installation and support of Information Resources, individuals charged with Information Resources security and data owners.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of system loss.

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.

Offsite Storage: A geographically different location from the University campus that does not share the same disaster threats. Based on an assessment of the data backed up and its criticality, removing the backup media from the building and storing it in another secured location on the University campus may be appropriate.

Recovery: retrieving data from hard drives, solid-state drives, storage tapes, and other media internal or external that is corrupted, inaccessible or damaged physically or logically.
1. **Backup/Recovery**

1.1 Recovery process is outlined in the Disaster Recovery Plan.

1.2 The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk.

1.3 TAMU’s Information Resources backup and recovery process for each system must be documented and reviewed at least annually.

1.4 To verify the success of the backup, a work order must be established in the Track-IT system, including any logs generated by the backup application.

1.5 Backups must be periodically tested to ensure that they are recoverable in accordance with the **Backup Verification Standard Operating Procedure**.

1.6 A full backup of the systems must be performed and stored offsite at least once a month.

1.7 Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest University sensitivity level of information stored.

1.8 University servers are backed up on a scheduled basis as listed below:

- **Nightly** - Incremental backups are performed and retained until the next full backup is performed.
- **Weekly** - Full data backups are performed and retained for five weeks.
- **Monthly** - Full data backups are performed and retained one year from the date of the backup.

1.9 Institutional shared drives are limited in physical size. Therefore, personal data should not be saved on those resources.

1.10 Users are responsible for creating backups of their own data. OIT can assist data owners in creating a backup process. Owners, however, need to assess the following:

- Value of the data,
- Security and or encryption requirements for the data,
- Reason why the data is not stored on an institutional shared resource,
- Identify the specific path to the directories where the data is stored separately from the program files and operating system files,
- Define the time period to retain the backup, and
- Specific needs or requirement for repetition of the backup.
1.11 Email Backups:

- Nightly - Incremental backups are performed and retained until the next full backup is performed.
- Weekly - Full data backups are performed and retained for five weeks.

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

TAC 202.75 Security Standards for Institutions of Higher Education

**Appendix**

**References**
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
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>

<table>
<thead>
<tr>
<th><strong>Office Hours</strong></th>
<th><strong>ITSecurity Group</strong></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>