I. POLICY STATEMENT

The University will protect the Information Resources assets of the State of Texas in accordance with TAC, Chapter 202 and as authorized by the Information Resources Management Act, Texas Government Code, Chapter 2054. The University will apply policies, procedures, practice standards, and guidelines to protect its IR functions from internal data or programming errors and from misuse by individuals within or outside the University. This is to protect the University from the risk of compromising the integrity of programs, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety. All University Information Resources security programs will be responsive and adaptable to changing technologies affecting Information Resources.

II. PURPOSE AND SCOPE

The Information Resources ("IR") Security Standards Policy applies to all information obtained, created, or maintained by Texas Southern University's automated Information Resources. These policy standards are based on the interpretation of Texas Administrative Code ("TAC"), Chapter 202 and Industry Best Practices and apply equally to all personnel including, but not limited to, all University's employees, students, agents, consultants, volunteers, and all other authorized users granted access to Information Resources. Further, these Policy Standards apply to all information generated by the University's Information Resources functions through the time of its transfer to ownership external to the University or its proper disposal/destruction. In the event of a conflict, this policy shall be interpreted in a manner consistent with applicable law and governing University policies.

III. DEFINITIONS

A. Data Classification Categories:

In accordance with **Texas Administrative Code (TAC) §202**, the University classifies Information Resources based on the risk and impact of unauthorized disclosure as follows:

- **Category I – Confidential:** Information protected by law (e.g., HIPAA, FERPA) or contract. Unauthorized disclosure requires notification and may result in significant legal or financial penalties.
- **Category II – Sensitive:** Information not protected by law but intended for internal University use. Unauthorized disclosure could cause moderate risk or operational harm.
- **Category III – Public:** Information that has been approved for public release and may be distributed without restriction.

B. Authorized User:
Any individual or entity granted explicit permission by the University to access and use Information Resources.

C. Custodian:
The department or personnel responsible for providing the technical infrastructure, maintenance, and security controls for Information Resources as directed by the Owner.

D. Information Resources (IR):
The procedures, equipment, and software designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

E. Owner:
The University manager or administrator who has primary responsibility for a business function and determines the classification and access rights for the data supporting that function.

F. Security Incident:
An event that results in the accidental or intentional unauthorized access, loss, disclosure, modification, disruption, or destruction of Information Resources.

G. Sensitive Data:

A collective term for data categorized as either Confidential or Sensitive that requires protection beyond what is afforded to Public information..

IV. POLICY PROVISIONS

1. Violations

Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of IR constitutes a breach of security and confidentiality. Violations may include, but are not limited to any act that:

1.1. Exposes the University to actual or potential monetary loss through the compromise of Information Resources security;

1.2. Involves the disclosure of sensitive or confidential information or the unauthorized use of University data or resources;

1.3. Involves the use of Information Resources for personal gain, unethical, harmful, or illicit purposes; and/or

1.4. Results in reputational harm to the University arising from unauthorized or improper use of Information Resources.

2. Incident Response and Breach Management

In accordance with Texas Administrative Code §202.73, the University shall maintain and follow formal incident response procedures for all suspected or confirmed security incidents involving Information Resources.

2.2 Reporting.

All users must promptly report suspected or confirmed security incidents to the Office of Information Technology or the University Information Security Officer in accordance with University procedures.

2.3 Compliance

The University shall comply with all applicable notification requirements to the Texas Department of Information Resources (DIR), the Office of the Attorney General, and other regulatory authorities, as required by law.

2.4 Implementation

The Office of Information Technology, in coordination with the Information Security Officer, shall be responsible for implementing and maintaining these procedures, including processes for investigation, documentation, and appropriate evidence preservation.

2.5 Cooperation

All users are expected to cooperate with incident response and investigative activities. Failure to comply may result in disciplinary action in accordance with University policy.

2.6 Additional Provision (Recommended)

Detailed incident response timelines and operational procedures are maintained by the Office of Information Technology and may be updated as necessary to remain consistent with applicable law and industry standards.

3. Disciplinary Action

Violation of the Policy Standards may result in immediate disciplinary action pursuant to University policy (MAPP 02.05.03 – Discipline & Termination Policy).

4. Security Standards

All employees are responsible for reviewing and adhering to all Security Standards as described in this policy as well as the provisions in the Security Standards addendum (Addendum A):

	STANDARD	SOURCE
1	IR Security controls must not be bypassed or disabled.	Control Standard Catalog
2	Security awareness of personnel must be continually emphasized and reinforced.	TAC §202.8(d) and (e)
3	All personnel are responsible for managing their use of IR and are accountable for their actions relating to IR security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management. Security incidents meeting reporting thresholds under TAC §202.73 must be reported to the Texas Department of Information Resources (DIR) in accordance with state incident reporting requirements.	TAC §20272
4	Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and other computer systems security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner or to department management.	TAC §202.72

5	Access to, and use of IR must be strictly controlled and secured. Information access authority for each user must be reviewed on a regular basis and any changes to the configuration or software of an Information Resource must be documented and approved. . Access must be promptly and appropriately adjusted or revoked following a change in job status, such as a transfer, promotion, demotion, or termination of service.	TAC §202.72(1)B
6	The use of IR must be for officially authorized business purposes only. Users should not expect personal privacy when using University Information Resources, which may be monitored in accordance with applicable law and University policy. The use of these electronic communications tools may be monitored to fulfill complaint or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of IR utilization, the establishment of effective use, and reporting of performance to management.	TAC §202.72
7	Any data used in an IR system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement of keeping it confidential and secure. Rather, the type of information or the information itself are the basis for determining whether the data must be kept confidential and secure. Furthermore, data must still be protected as confidential and secured regardless of whether it is stored in a paper or electronic format or copied, printed, or electronically transmitted.	TAC §202.76
8	All computer software programs, applications, source code, object code, documentation and data shall be guarded and protected as state property.	TAC §202.70(1)

9	On termination of the relationship with the University, users must surrender all property and IR managed or owned by the University. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. These obligations survive termination until all University property and access are properly returned or revoked.	TAC §202.72(1)(B)

10	The owner must engage the Information Resource Manager or designee at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development and operation of computer hardware and applications must be authorized by appropriate management. Management and the requesting department must act within their delegated approval limits in accordance with the University authorization policy. A list of standard software and hardware that may be obtained without specific, individual approval will be published.	Industry Best Practices
11	The department that requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by or acquired for computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.	TAC §202.72
12	The IR network is owned by the State of Texas and controlled by OIT. Approval must be obtained from OIT before connecting a device that does not comply with published guidelines to the network. OIT reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.	Industry Best Practices
13	The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with state law and University policies and procedures.	Industry Best Practices

14	The integrity of general use software, utilities, operating systems, networks, and respective data files is the responsibility of the custodian department. Data for test and research purposes must be depersonalized prior to release to testers unless each individual involved in the testing has authorized access to the data.	Control Standard Catalog
15	All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.	Control Standard Catalog, TAC §202.76
16	Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuse in accordance with the needs defined by owner departments. Access must be properly documented, authorized and controlled.	Control Standard Catalog, TAC §202.76
17	All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure or loss of the data for which they are responsible.. **Security risk assessments shall be conducted at a frequency determined by the Office of Information Technology (OIT) based on the classification of the data and the risk to the University. The Information Security Officer (ISO) shall maintain the central documentation of all risk analyses. Through the use of monitoring systems, departments must ensure the University is protected from damage, monetary or otherwise.** Owner and custodian departments must maintain appropriate backup and contingency plans for disaster recovery based on these risk assessment and business requirements.	TAC §202.75
18	All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized University officer and must contain terms approved as to form by the Office of General Counsel, advising vendors of the University's retained proprietary rights with respect to information sytems, programs, and data. Such agreements shall include appropriate provisions addressing data security, maintenance, protection, and the return or destruction of University data upon termination of the agreement. In accordance with Texas Government Code §2054.0593,	Industry Best Practices

	vendors providing cloud computing services to the University must demonstrate and maintain Texas Risk and Authorization Management Program (TX-RAMP) certification at a level appropriate to the classification of data being processed, as applicable.	
19	IR computer systems and/or associated equipment used for University business that is conducted and managed outside of University control must meet contractual requirements and be subject to monitoring.	TAC §202.71(c)(2)
20	External access to and from IR must meet appropriate published University security guidelines.	Industry Best Practices
21	All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. The IRM through OIT reserves the right to remove any unlicensed software from any computer system.	Control Standard Catalog
22	The IRM through OIT reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to games, instant messengers, pop email, music files, image files, freeware, and shareware.	Industry Best Practices
23	Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.	Industry Best Practices