SECTION: Information Technology **Policy 04.06.22**
AREA: Information Security

SUBJECT: Security Standards Policy

I. 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. To the extent these Policy Standards conflict with existing University policy, the existing policy is superseded by this policy.

II. APPLICATION OF POLICY STANDARDS

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.

III. 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:

A. Exposes the University to actual or potential monetary loss through the

compromise of Information Resources security;

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

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

D. Results in public embarrassment to the University.

IV. DISCIPLINARY ACTION

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

V. 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.	TAC 202.70(1)
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.	TAC 202,70(3), TAC 202.71(c)(3)
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 202.70(3), TAC 202.71(c)(3)
5	Access to and change and use of IR must be strictly secured. Information access authority for each user must be reviewed on a regular basis. Job status change such as a transfer, promotion, demotion, or termination of service must also be reviewed on a regular basis.	TAC 202.71(c)(1)(A),(H) TAC 202.75 (3)(A)

6	The use of IR must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to email, Web browsing and other electronic discussion tools. 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 202.70(3), TAC 202.75(h)(O)
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 202.70(1), TAC 202.71(c)(3), TAC 202.75(2)
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. Further, this policy survives the terminated relationship.	TAC 202.75(3)(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 202.71(c)(1)

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 de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.	TAC 202.71(c)(2), TAC 202.75(6)(A)
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.	TAC 202.71(c)(1)
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.	TAC 202.71(c)(2)
17	All departments must carefully assess the risk of unauthorized alteration, unauthorized disclosure or loss of the data for which they are responsible and ensure through the use of monitoring systems that the University is protected from damage, monetary or otherwise. Owner and custodian departments must have appropriate backup and contingency plans for disaster recovery based on risk assessment and business requirements.	TAC 202.70(1), TAC 202.70(5), TAC 202.72 (a), TAC 202.74 (a)(5),(b), TAC 202.75(8)(D),(I),(P), TAC 202.75(9)(A)
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 General Counsel, advising vendors of the University's IR retained proprietary rights and acquired rights with respect to its information systems, programs and data requirements for computer systems security, including data maintenance and return.	Industry Best Practices
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.	TAC 202.75(7)(S), Section 117 of the Copyright Act
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.	TAC 202.75(7)(S), 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

VI. REVIEW AND RESPONSIBILITIES

Responsible Party: Chief Information Officer Billy Ratliff

Review: Every year, on or before September 1

VII. APPROVAL

Jim McShan

Vice President of Finance

President

2/18/11

Effective Date

ADDENDUM "A"
Security Standards Definitions

ADDENDUM A

DEFINITIONS

1. Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

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

3. Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that information technology resources are protected against improper modification before, during, and after system implementation. Change includes: A. Any implementation of new functionality, B. Any interruption of service, C. Any repair of existing functionality, and D. Any removal of existing functionality.

4. Change Classification:

- Change Category: Whereas the priority of a change indicates how urgently a change is required to be implemented, the category of a change is used to define the change's impact on the infrastructure, users, or business. For example, does the change affect one user, a department, or every user in the organization? Does the change involve updating a single switch, or is it a complete overhaul of the network? The answers to such questions determine the category of the change. As with priorities, the decision of what constitutes each category of change is determined by the individual organization. As a suggestion, the following categories have been used effectively in other organizations.

  > *Major.* A change where the impact on the group could be massive—for example, a departmental or corporate-wide change, or a network-wide or service-wide change.
  > *Significant.* A change where the effect is widespread, but not massive—for example, a change affecting a group within a department. *Minor.* A change affecting small numbers of individuals—for example, a change to a printer used by a department consisting of just a few members. *Standard.* A change that has been performed before and is part of the operational practice of the business—for example, an update to a user profile.

- Change Priority: As mentioned previously, priority is derived from the need for the change. The priority rating is used to decide how quickly changes will be evaluated and implemented. Although each organization can define its own priority levels, the following table further illustrates the four-level classification system summarized in the change request phase.

Emergency. Causing loss of service or severe usability problems to a large number of users, a mission-critical system, or some equally serious problem. Immediate action required. Emergency meetings of the CAB or CAB/EC may need to be convened. Resources may need to be immediately allocated to deploy such authorized changes.

High. Severely affecting some users or having an impact upon a large number of users. To be given highest priority for change building, testing, and implementation resources.

Medium. No severe impact, but rectification of an incident cannot be deferred until the next scheduled upgrade, for example. To be allocated medium priority for resources.

Low. A change is justified and necessary, but can wait until the next scheduled release or upgrade. To be allocated resources accordingly

5. CIRT (Computer Incident Response Team): Personnel responsible for coordinating the response to computer security incidents in an organization.

6. Custodian: Guardian or caretaker; the holder of data. Also, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The custodian is normally a provider of services.

7. Email: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application

8. Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

9. Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

10. Emergency Change: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

11. Firewall: An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

12. Host: A computer system that provides computer service for a number of users.

13. Information Attack: An attempt to bypass the physical or information security measures and controls protecting an automated information system. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

14. Information Operations: Actions taken to affect adversary information and information systems while defending one's own information and information systems.

15. IR&T (Information Resources &Technology): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, 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, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is 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.

16. IRM (Information Resources Manager): Responsible to the State of Texas for management of the University's information resources. The designation of a University information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state entities' information activities, and ensure greater visibility of such activities within and between state entities. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Information Resources of the University. If the University does not designate an IRM, the title defaults to the University President, and the President is responsible for adhering to the duties and requirements of an IRM.

17. ISO (Information Security Officer): Responsible to the executive management for administering the information security function within the University. The ISO is the University's internal and external point of contact for all information security matters.

18. Internal Auditor: Ensures that the University's information resources are being adequately secured based on risk management as directed by the IRM and acting on delegated authority for risk management decisions.

19. Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present —information super highway.‖

20. Intranet: A private network for communications and sharing of information that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

21. LAN (Local Area Network): A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.
TSU Information Technology Security Policies Approved by the Board of Regents on November 30, 2007 Page 7 of 34

22. OIT (Office of Information Technology): The University department responsible for computers, networking and data management

23. Offsite Storage: Based on data criticality, offsite storage should be in a geographically different location from the University campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location on the University Campus may be appropriate.

24. Owner: The manager or agent responsible for the function that is supported by the resource. Also, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

25. Password: A string of characters which serves as authentication of a person's identity which may be used to grant, or deny, access to private or shared data.

26. Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from IR. These include, but are not limited to, notebook computers, handheld computers, PDA's, pagers, and cell phones.

27. Production System: The hardware, software, physical, procedural, and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

28. Program Manager: Assigned IR ownership. Is responsible for the information used in carrying out program(s) under his or her direction and provides appropriate direction to implement defined security controls and procedures.

29. Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

30. Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system. Whereas the University will have one Information Security Officer, technical management may designate a number of security administrators.

31. Security Incident: In information operations, an assessed event of attempted entry, unauthorized entry or information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input,

processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

32. Server: A computer program that provides services to other computer programs in the same or another computer. A computer running a server program is frequently referred to as a server although it may also be running other client (and server) programs.

33. Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of
TSU Information Technology Security Policies Approved by the Board of Regents on November 30, 2007 Page 8 of 34
a sequence of characters, numbers, and special characters depending on the capabilities of the operating system. Typically the longer the password the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about you such as a birth date, social security number, and so on.

34. System Administrator: The person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls to enforce an organization's security policy.

35. System Development Life Cycle (SDLC): A set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance and acceptance testing.

36. TAC (Texas Administrative Code): Rules and regulations promulgated by state agencies under the authority of the Texas Legislature; have the same authority as state law.

37. Technical Manager: Assigned custodian of IR. Provides technical facilities and support services to owners and users of information. Assists the University in the selection of cost effective controls to be used to protect information resources. Is charged with executing the monitoring techniques and procedures for detecting, reporting, and investigating breaches in information asset security.

38. Trojan Horse: Destructive programs, usually viruses or worms, that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

39. Unscheduled / Mission critical Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of security vulnerability.

40. User: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules. Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive

information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.

41. Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.

42. Vendor: A person or company that exchanges goods or services for money.

43. Web server: A computer that delivers (serves up) web pages.

44. Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

45. World Wide Web: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contain links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Netscape, Navigator, and Microsoft Internet Explorer.

46. Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network, using otherwise-unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.