Handbook of Operating Procedures

INFORMATION RESOURCES USE AND SECURITY

A. Purpose

The purpose of this policy is to:

1. establish standards regarding the use and safeguarding of The University of Texas Rio Grande Valley (UTRGV) Information Resources;
2. protect the privacy of individuals by preserving the confidentiality of Personally Identifiable Information (PII) entrusted to UTRGV;
3. ensure compliance with applicable policies and state and federal laws and regulations regarding the management of risks to and the security of Information Resources;
4. appropriately reduce the collection, use, or disclosure of social security numbers contained in any medium, including paper records;
5. establish accountability;
6. educate individuals regarding their responsibilities associated with use and management of UTRGV Information Resources; and
7. serve as the foundation for the UTRGV's Information Security Program, provide the Information Security Office the authority to implement Policies, Standards, and Procedures necessary to operate an effective Information Security Program in compliance with this Policy.

B. Persons and Resources Affected

This policy applies to:

1. all individuals accessing, using, holding, or managing UTRGV Information Resources on behalf of UTRGV;
2. all individuals associated with or on the premise of UTRGV, including without limitation employees, faculty, students, visitors, volunteers, contractors, or vendors;
3. all Information Resources owned, leased, operated, or under the custodial care of the University, organization, or facility;
4. all Information Resources owned, leased, operated, or under the custodial care of third parties operating on behalf of the University, organization, or facility; and
5. Information Resources owned by others, such as political subdivisions of the state or agencies of the state or federal government, in which there is a statutory, contractual, or fiduciary duty to protect the resources while in UTRGV custody. If the owner has a more restrictive policy than these policies, then the owner's policy will control.

C. Policy

1. UTRGV is committed to freedom of expression, free inquiry, open intellectual and scientific debate, and criticism of the accepted body of knowledge, regardless of the medium of

expression. However, the individual rights of expression or privacy may be impacted by the responsibility of UTRGV to protect the integrity of information technology resources, the rights of all users and the property of the University.

2. UTRGV Information Resources are strategic and vital assets belonging to the people of Texas, and access to these Information Resources is a privilege. Access to Information resources must be appropriately managed. To provide the greatest use of its computing and information technology resources for the entire University community, it is the policy of the University and responsibility of each individual to:

    a. Protect against risk of accidental or unauthorized access, disclosure, modification, or destruction of Information Resources;

    b. Complete required information security training and awareness activities;

    c. Maintain the confidentiality, integrity, and availability of Information Resources; and

    d. Apply appropriate physical and technical safeguards to conduct University business while meeting the guidelines of applicable state laws, federal laws, System guidelines, industry standards, UTRGV standards, and best practices of the information security program.

3. As assets of UTRGV, all UTRGV Information Resources are subject to access and monitoring without prior notice to the user at any time for any purpose consistent with the duties and missions of the institution, including without limitation responding to public information requests, court orders, subpoenas or litigation holds; conducting maintenance; or conducting inventories or investigations.

4. The Chief Information Security Officer (CISO) is responsible for UTRGV's Information Security and Cybersecurity Programs, and has the authority to establish, implement, and enforce policies, standards, and procedures necessary to oversee and manage an effective program. In addition to the duties of the CISO listed in UTS 165, the CISO will:

    a. provide leadership, strategic direction, and coordination for Cybersecurity, cyber-resilience activities, and the Information Security Program;

    b. provide leadership and direction for Information Security and Cybersecurity response operations; and

    c. ensure the continuing improvement and development of the Information Security and Cybersecurity Programs at UTRGV.

5. Individuals using UTRGV Information Resources are expected to familiarize themselves, cooperate, and comply with the policies, procedures, standards, expectations, or other requirements established by UTRGV regarding access and use of Information Resources.

D. Procedures

1. Protecting the integrity of UTRGV shared information resources and preserving access to them is a community effort that requires each member to act responsibly and guard against abuses. Both the UTRGV community and each individual user have an obligation to abide by the procedures, standards, protocols, and best practices of the information security program, as amended from time to time, that are outlined in this policy and in the published

procedures, standards, protocols, and best practices found on the UTRGV Information Security Office website.

2. UTRGV reserves the right to limit or restrict their use based on institutional priorities and financial considerations, as well as when presented with evidence of a violation of University policy, contractual agreements, or state/federal laws.

E. Definitions

The Information Security Office maintains a list of terms and definitions that apply to information security policies, procedures, standards, protocols, and best practices. This list can be accessed from the Information Security Website.

F. Related Statutes or Regulations, Rules, Policies, or Standards

Family Educational Rights and Privacy Act of 1974 (FERPA), as amended in 2000
Copyright Act of 1976, as amended
Foreign Corrupt Practices Act of 1977, as amended in 1988
Computer Fraud and Abuse Act of 1986, as amended in 1996
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
USA PATRIOT Act of 2001
The State of Texas Public Information Act
Texas Government Code, Section 441
Texas Administrative Code 1 TAC 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
University of Texas System Information Resources Use and Security Policy, UTS165

G. Dates Reviewed or Amended

July 13, 2022 - Reviewed and amended (non-substantive: updated responsible executive).