Wharton County Junior College	ADMINISTRATIVE PROCEDURE	
WCJC Title: Cyber Incident Response Plan	Section C: Business and Support Services	Pages: 5
Policy Title: Information Security	Policy: CS	
Subtitle: N/A	Date Adopted: 03/31/2026	

Purpose

This document serves to establish cyber incident response regulations and procedures. The purpose of these regulations and procedures is to improve Wharton County Junior College's ("WCJC" or "College") capability to identify, respond to, and manage cyber incidents, which may occur across the College environment. The scope of these regulations and procedures is applicable to all Information Resources owned or operated by WCJC. All Users are responsible for adhering to these regulations and procedures. If needed or appropriate, information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

Definitions

Cyber Incident: A cyber incident occurs when there is a breach of explicit or implied digital security administrative procedure that requires corrective action because it threatens the confidentiality, availability, and integrity of an information system or the information the system processes, stores, or transmits. Examples include, but are not limited to:

- Denial of service attacks (DoS) that affect system or service availability
- Virus or malware outbreak (including ransomware)
- Compromise or disclosure of sensitive information (private or restricted)
- Compromise of network credentials or an email account

Data Breach: Unauthorized access to sensitive or personally identifiable information.

Employee: Any individual at WCJC who is hired in a full-time, part-time, or temporary capacity in a faculty or staff position, or in a position where the individual is required to be a student as a condition of employment.

Information Resources: The systems, tools, and services that enable the storage, processing, transmission, and use of data. This includes:

- Digital content: Electronic, Audiovisual, and Multimedia
- Hardware and software that handle information ressources
    - Servers
    - Computers and/or mobile devices
    - Cloud services
    - Medical or lab equipment

- Related communication tools
    - Email
    - Telephones and Fax Machines
    - Printers
    - Networks

It also covers the procedures and facilities used to create, manage, and deliver information.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Student: A person taking courses at WCJC, a person who is not currently enrolled in courses but who has a continuing academic relationship with WCJC, or a person who has been admitted or readmitted to WCJC

College Affiliate: Any individual associated with WCJC in a capacity other than as a student or employee who has access to WCJC resources through a contractual arrangement or other association. This includes:

- WCJC Trustees
- Contractors and vendors
- Employee of a governmental agency
- Employee of a WCJC-affiliated institution
- Pre-employment individual
- Other individual or entity affiliated with WCJC

Information Spillage: The transfer or disclosure of sensitive, confidential, or restricted information to an information system, network, media, or individual that is not authorized to access, process, or store that information. This includes both intentional and inadvertent releases of protected data to unauthorized locations or recipients.

User: WCJC employees, contractors, vendors, or other individuals using a WCJC Information Resource.

Information System Owner: The individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Procedure

This administrative procedure is applicable to WCJC employees, students, and college affiliates.

1. Security Standards
    a. Incident Response Training
        i. *WCJC IT Department:* Implements and maintains incident response training for assigned users with incident response roles and responsibilities.
        ii. *Incident Response Training Update:* Incident response training content

shall be updated periodically and following significant changes to the information system.

iii. *Assigned Users:* Shall complete incident response training within 30 days of their assigned incident response role or as assigned in response to changes in the information system, and shall complete a refresher course annually thereafter.

b. Incident Response Testing: The effectiveness of the incident response capability for the information system shall be tested annually using tabletop exercises, simulations, and/or real-world incident response circumstances.

c. Incident Handling: WCJC IT Department maintains a document called the "WCJC Cyber Incident Response Plan Process" which:
   i. Addresses incident preparation, detection and analysis, containment, eradication, and recovery;
   ii. Coordinates incident handling activities with information system recovery and reconstitution planning activities;
   iii. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly; and
   iv. Ensures the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the college.

d. Incident Monitoring: WCJC Information Security tracks and records cyber incidents using several methods. This includes but is not limited to incidents reported through Team Dynamix, antivirus systems, and network security systems.

e. Incident Reporting
   i. *Users:* Shall immediately report suspected or known cyber incidents to immediate supervisors and the Information Security team by reporting the suspicious activity to ITSupport@wcjc.edu or via Team Dynamix.
   ii. *Information System Owner:* Shall report cyber incidents to the Texas Department of Information Resources for events that are assessed to:
      1. Propagate to other state systems;
      2. Result in criminal violations that shall be reported to law enforcement;
      3. Involve the unauthorized disclosure or modification of confidential information (e.g., sensitive personal information as defined in §521.002(a)(2), Business and Commerce Code, and other applicable laws that may require public notification).
   iii. *Criminal Activity Response:* If the cyber incident is assessed to involve suspected criminal activity (e.g., including but not limited to violations of Chapter 33 or Chapter 33A Texas Penal Code), the cyber incident shall be investigated, reported, and documented in a manner that restores

operation promptly while meeting the legal requirements for handling of evidence.

f. Incident Response Assistance: WCJC Information Security shall provide an Incident Response Plan as a support resource that offers advice and assistance to users of the information system for the handling and reporting of cyber incidents. Users may request assistance via ITSupport@wcjc.edu.

g. Incident Response Plan: The WCJC Incident Response Plan (IRP) is distributed to personnel with incident response roles and responsibilities, and all changes are timely communicated to the appropriate staff.
    i. *WCJC IT Department:* Maintains the WCJC IRP that:
        1. Provides the college with a roadmap for implementing its incident response capability;
        2. Describes the structure and organization of the incident response capability;
        3. Provides a high-level approach for how the incident response capability fits into the overall operations of the college;
        4. Meets the unique requirements of the college, which relate to mission, size, structure, and functions;
        5. Defines reportable incidents;
        6. Provides metrics for measuring the incident response capability within the college;
        7. Defines the resources and management support needed to effectively maintain and further develop an incident response capability;
        8. Addresses the sharing of incident information;
        9. Explicitly designates responsibility for incident response to the ISO; and
        10. Is protected from unauthorized disclosure and modification.
    ii. *WCJC Information Security:* The WCJC IRP is created, maintained, and tested annually by WCJC Information Security.
    iii. *Information System Owner:* The WCJC IRP is reviewed and updated annually by the ISO.
    iv. *Vice President of Information Technology:* The WCJC IRP is approved annually by the Vice President of Information Technology.

h. Information Spillage Response: Information system owners are responsible for responding to information spills by:
    i. Identifying the specific information involved in the information system contamination;
    ii. Alerting WCJC Information Security by reporting the information spillage via ITSupport@wcjc.edu or a method of communication not associated with the spill;
    iii. Isolating the contaminated information system or information system

component;

iv. Eradicating the information from the contaminated information system or information system component;
v. Identifying other information systems or components of information systems that may have been subsequently contaminated; and
vi. Perform any other additional actions deemed necessary during the incident response process.

2. Regulatory Compliance
   The State of Texas has chosen to adopt the Incident Response ("IR") principles established in the National Institute of Standards and Technology (NIST) SP 800-53 "Incident Response" guidelines. The NIST IR controls have been assigned a number. The following subsections outline the IR standards included in WCJC's regulations and procedures: IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, IR-9.

3. Compliance
   Employees who violate this administrative procedure are subject to corrective and disciplinary actions. WCJC may also take corrective action against interns, volunteers, contractors, consultants, trustees, or members of the public who violate this administrative procedure, including up to termination of WCJC's relations or access to college resources for that individual or entity. Students who violate this administrative procedure are subject to corrective and disciplinary action.

4. Review

   This administrative procedure will remain in effect and published until it is reviewed, updated, or archived. This administrative procedure is to be reviewed annually. An interim review may be required as a result of updates to federal and state law or regulations, administrative procedures, or internal processes or procedures.

5. References
   - National Institute of Standards and Technology
   - WCJC Incident Response Plan Process
   - Texas Administrative Code Chapter 202
   - Texas Department of Information Resources
   - Texas Business and Commerce Code § 512.053
   - Texas Government Code § 2054.518
   - Texas Government Code § 2054.1125

Date Prepared/Revised: 02/01/2026 (KV)