WCU
WEST CHESTER
UNIVERSITY

— UNIVERSITY POLICY —

Incident Response Policy

Accommodations for individuals with disabilities in accessing these policies are available upon request by emailing accessiblepolicy@wcupa.edu

Purpose and Scope

The Incident Response Policy for West Chester University Information Services & Technology computing facilities, systems and resources applies to all members of the University community, including faculty, students, staff, contractors, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access service or eduroam access, and to those who register their computers and other devices through Conference Services programs or through other offices, for use of the campus network.

Policy Statement

The purpose of this policy is to clearly define the roles and responsibilities during the investigation and response of a computer security incident or data breach as well as establish the criteria for what constitutes an "incident."

This policy applies to all members of the West Chester University community, such as faculty, staff, students, vendors, contractors, associates, volunteers, and guests ("Users") who utilize West Chester University computing resources or access the campus network, whether locally or remotely.

While information security is the responsibility of every user at West Chester University, suspected incidents or possible data breaches should be immediately reported directly to Information Services & Technology (IS&T) through phone call (610-436-3350) or email (helpdesk@wcupa.edu) to the IS&T Help Desk.

The Computer Security Incident Response Team (CSIRT), a subset of IS&T, is responsible for the coordination and leadership of response to reported or discovered incidents. In addition, the CSIRT will spearhead the University's security readiness, threat analysis, and remedial efforts.

Policy Framework

The CSIRT detects and investigates security events to determine whether an incident has occurred, and the extent, cause, and damage of incidents. The CSIRT directs the recovery, containment, and remediation of security incidents and may authorize and expedite changes to information systems necessary to do so. The CSIRT coordinates the response with external parties when existing agreements place responsibility for incident investigations on the external party.

During the conduct of security incident investigations, the CSIRT may utilize applicable logs, login session data, communications, or other relevant records of specific WCU users or information systems. These and other types of retrievable electronic data, or computer systems, may be gathered and utilized during an investigation without notice or further approval, as stated in the Acceptable Use Policy. Any external disclosure of confidential user data or information regarding security incidents must be reviewed and approved by the CISO, Deputy CIO, or CIO and may be required to consult with University Legal Counsel, University Communications & Marketing, and other University stakeholders as appropriate.

The CSIRT will coordinate with law enforcement, government agencies, peer CSIRTs and relevant Information Sharing and Analysis Centers (ISACs) in the identification and investigation of security incidents. The CSIRT is authorized to share external threat and incident information with these organizations that does not identify any member of West Chester University. Up-to-date processes, procedures, communication matrix, and CSIRT members can be found in the IS&T Incident Response Plan.

Definitions

Computer Security Incident Response Team (CSIRT) – A subset of the Information Security Office and IS&T, responsible for receiving, reviewing, and coordinating the response to reported computer security incident events and activity involving West Chester University data and/or information systems.

Data Breach – Unauthorized access, acquisition, use or transmission of University Data. Data breach notifications are subject to regulatory requirements following an investigation or risk assessment.

Incident – An event (electronic or physical) that negatively impacts the confidentiality, integrity or availability of West Chester University data or information Systems. Actions or events that violate West Chester University privacy or acceptable use policies.

References

Acceptable Use Policy (http://www.wcupa.edu/policies/documents/Acceptable%20Uses%20of%20Electronic%20Signatures%20Policy.pdf)

Reviewed by: Information Services & Technology

Policy Owner: **Stephen Safranek**

Chief Information Security Officer
Information Services & Technology

Office of Labor Relations Review: Review completed December 27, 2022

Approved by:

JT Singh

Senior Associate VP & CIO
Information Services & Technology
Date: October 13, 2023

Effective Date: **November 15, 2023**

Next Review Date: October 13, 2027

History:

Initial Draft: 11/1/2022

Initial Approval: 12/27/2022

Review Dates: 11/1/2022, 10/23/2023, 11/14/2023

Amended: