Information Security Standard

date and place of birth, mother‘s maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

“Protected Health Information (ePHI)” is defined as any individually identifiable health information and is required to be protected through the Health Insurance Portability and Accountability Act (HIPAA).

“Workforce Member” includes, but is not limited to, faculty, staff, employees, guests, consultants, vendors, contractors, volunteers, interns, student workers or temporary workers associated with the University.

The Information Security and Privacy Committee (ISPC), as defined in University Policy 97, is responsible for the development, implementation, communication, and oversight of information security policies and standards. Internal Audit will periodically review policy compliance.

The standing membership of the IRT includes the CIO (IRT Leader), General Counsel, Chief Information Security Officer, Internal Audit, and University Police. These positions or their designee are responsible for implementing the referenced below.

Depending on the incident, General Counsel may choose to activate the campus Executive Crisis Management Team (ECMT). This team will work in conjunction with the IRT and coordinate all internal and external communications.

Department managers are responsible for ensuring all workforce members complete any assigned information security training, and for enforcing information security policies and standards.

All workforce members are responsible for reporting information security incidents and assisting the IRT in investigating and mitigating information security incidents.

As soon as an incident has been identified, the employee who discovered it must take immediate steps to report the incident to his or her supervisor. The supervisor must take immediate1 0 0 iETQ0.00000912 0 612 792 reW*nBT/F2 11.04 Tf1 0 0 1 161.3 177

Reporting a computer security incident maliciously or in bad faith may constitute an abuse of this policy and may result in disciplinary action against the person making the report.

.

The ISPC is to regularly review and revise this policy as may be appropriate, minimally every three years. There may be events that trigger additional reviews such as changes in laws or regulations, information security best practices, threat models, or changes in business processes.

International Standards Organization (ISO/IEC 27002:2022, Clause 5 Organizational Controls)

International Standards Organization (ISO/IEC 27002:2022, Clause 6 People Controls)

University Policy 117 Information Security

University Policy 97 Information Security and Privacy Governance

WCU Information Security Incident Response Plan

45 CFR Part 164, Subpart C – Security Standards for the Protection of Electronic Protected Health Information

Response and Reporting [164.308(a)(6)(ii)] (Required) - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

Security Incident Procedures [164.308(a)(6)(i)] (Standard) - Implement policies and procedures to address security incidents.