What needs to be incorporated into a *Cyber Security Policy* for a Higher Education Institution

Greg Whateley and Tom O'Connor

September 2025

A comprehensive and informed cyber security policy is critical for higher education institutions to safeguard sensitive data, support academic operations, and maintain trust among students, staff, and stakeholders. A policy of this nature is also an essential part of academic integrity.

Purpose and Scope

It is important to clearly state the objectives of the policy - such as protecting institutional data; ensuring compliance with legal and regulatory requirements; and supporting the university's mission. It is best to define the scope - specifying who and what systems the policy applies to - such as staff, students, contractors, all devices connected to the network.

Roles and Responsibilities

Roles and responsibilities need to be clearly outlined. Some simple examples would include – **IT Security Team** – to be responsible for implementing and monitoring security measures; **Staff** – who need to comply with security practices and report incidents; **Students** - who will be expected to follow acceptable use policies and report suspicious activity; and **Executive Leadership (Management)** – who are clearly accountable for reviewing and endorsing the policy on an ongoing basis. *Training* will be imperative here – especially for the non-IT minded.

Use of the policy

Set out clear expectations for the acceptable use of institutional IT resources, including computers, networks, and software. Addressing issues such as personal use, prohibited activities, and consequences for violations must be clearly stated and reinforced – *almost ad nauseam.*

Data Protection and Privacy

There are certain key issues that must be addressed including - classification of data such as public, internal, confidential, restricted; guidelines for handling, storing, and transmitting sensitive information (including student records, research data, and financial information); and of course, compliance with relevant privacy laws.

Control of access

To ensure security and avoid breaches some simple controls can be put in place including - users should only have access necessary for their roles; authentication requirements such as strong passwords, multi-factor authentication; and formal procedures for granting, modifying, and revoking access.

Network and System Security

Best practice would suggest security configurations for devices and servers be put in place; network segmentation and firewall policies and procedures be embedded; and regular (ongoing) vulnerability assessments be instigated.

Responding to and Reporting incidents

This aspect is best endorsed with identifying, reporting, and responding to security incidents; easy access to contact information for the IT security team; and embedding procedures for preserving evidence and notifying affected/impacted parties.

Device Management

A most sensible approach would be to insist on guidelines for the use of personal devices (BYOD), including security controls and monitoring. In addition - procedures for lost and stolen devices would also be a key consideration.

Backup and Recovery

An important element of cyber security would be regular data backups and of course - secure storage. Testing of disaster recovery and business continuity plans is also imperative.

By incorporating these components (and there are numerous others not highlighted) any higher education institution can put in place robust cyber security policies and protocols that address the challenges of the academic environment while ensuring the protection of its digital assets and – community at large.

Emeritus Professor Greg Whataley is currently Chief Executive and Executive Dean at the *Australian Guild of Education* (Melbourne)

Associate Professor Tom O'Connor is currently Academic Director at the *Australian Guild of Education* (Melbourne)