C2018/509

CYBER SECURITY POLICY DOCUMENT

Cyber Security Policy

Version No. 0.2

Contents

1. PURPOSE

This Cyber Security Policy is a formal set of rules by which those who are given access to the University's information systems and data must abide. The policy describes the technology and information assets that we must protect and identifies the threats to those assets, additionally aims to inform the University's users (i.e. employees, temporary staff, contractors, consultants and students) of their obligatory requirements for protecting the information systems and data. The Cyber Security Policy should be read in conjunction with the University's Information Security Policy, Acceptable Use Policy and Data Classification and Handling Policy, which will comprehensively describe the user's responsibilities and privileges in terms of information systems and data.

2. SCOPE

This policy shall apply to all information and information assets that are under the control of the University, irrespective of location, and apply to the entire University Community including entities affiliated to the University in which the University has a controlling interest. The Policy applies to all users of the University's information and information assets, including its employees, temporary staff, contractors, consultants and students.

Information assets including all computing equipment in the data centres, desktop and laptop computers, system software including operating systems, backup and restore software, database management systems, communication protocols, application software used by various departments within the University, custom or commercial, communication network hardware and software including routers, hubs, modems, switches, firewalls, network management software and tools.

3. CYBER SECURITY FRAMEWORK

For the detailed Cyber Security Framework, please see Addendum 01

4. PRINCIPLES

Cyber security spans across six key dimensions, which support the University's cyber security capabilities.

The dimensions covered by the Cyber Security Policy include:

- Leadership and governance
- Human capital

- Information risk management
- Business continuity
- Operations and technology
- Legal, compliance and audit.

The following precepts underpin these principles:

4.1 Risk based Approach that ensures that cyber risks are at acceptable level.

4.2 Generally accepted security controls should be in place.

4.3 Increased cyber resilience by implementing layered security to avoid single point of vulnerability.

4.4 Well defined cyber roles and responsibilities that include staff, students, suppliers and partners.

4.4 Maintenance of Business Continuity Planning processes.

4.5 Restricting access to University information and facilities to authorized users, processes and devices.

4.6 Monitoring and detection of anomalies on information systems.

4.7 Having a cyber-insurance policy for all information assets.

4.8 Access control to information and facilities with least privilege rights.

4.9 Compliance with the regulatory, contractual and legal requirements.

5. POLICY APPLICATION

Please see Policy Application – Addendum 02

Version	Date	Summary	Changed by
v.01	16/08/2018	Original Draft	Sue Tshoke/ Thokozani Dlamini
v.02	19/08/2018	Reviewed	Carol Crosley