Information Security Policy

Version 1.0
December 2016

Version Number: 1.0
Version Date: December 12, 2016
Version Status: Final

TABLE OF CONTENTS

1.0 INTRODUCTION

The University of the West Indies ("UWI" or "the University") is recognised as the leading tertiary level institution in the English-speaking Caribbean. In order to advance education delivery and knowledge creation, UWI, like other leading institutions, must properly manage its information infrastructure. UWI considers information to be a strategic asset, one that is essential to its mission and business operations. To this end, UWI must maintain the confidentiality, integrity and accessibility of the information it generates, collects, stores, and disseminates.

This policy defines information security as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction. This protection in turn ensures the confidentiality, integrity, and availability of information in the University space. Information security addresses the protection of information throughout the life cycle of this information and covers all information assets and processes, whether these involve people, or technology.

1.1 PURPOSE

This Policy is an update and replacement of The Information and Communication Technology Security Policy (2008) and has been developed to inform members of the UWI community, including visitors, of UWI's stance, as well as the rights and obligations of UWI community members in matters related to information security. This Policy adapts best practices, from the wider information security space, to the UWI context. The content within this Policy represents the basic requirements that each campus must meet. However, each campus retains the liberty to draft its own Information Security Policy customised to its local circumstance.

1.2 SCOPE

This Policy contains the requirements for protecting the confidentiality, availability, and integrity of UWI's information. This Policy covers all campuses of the University and supersedes any campus-specific policy where there is a conflict between this and any campus-specific policy.

1.3 AUTHORITY

The Office of the University CIO, in conjunction with the University-wide IT group, has the authority to draft University-wide ICT policies. These polices are then ratified as outlined by the governance process in section 1.7.

1.4 REVIEW

This Policy is scheduled for review by January 2017 or no later than 24 months after it has been accepted for promulgation by the relevant University committee.

1.5 COMPLEMENTARY DOCUMENTS

1.5.1 THE INFORMATION SECURITY POLICY GUIDELINES

Guidelines have been produced to assist members of the University community and those using UWI ICT facilities to secure UWI information assets. The guidelines complement UWI's Information Security Policy and should be read in conjunction with it.

1.5.2 GUIDELINES FOR MARKING AND HANDLING UNIVERSITY INFORMATION

It is necessary to classify information so that every individual that comes in contact with it knows how to properly handle and/or protect it. These guidelines have been produced to assist members of the University community and those using UWI ICT facilities to secure UWI information assets. These guidelines complement UWI's Information Security Policy and should be read in conjunction with it.

1.6 INFORMATION SECURITY GOVERNANCE

This Policy is enacted at the University-level and guides the information security process across UWI. Implementation of this Policy will be done at the campus-level by the respective roles identified in section 2.4.

The governance process involves the following steps:

- drafting initial policy by the Policy unit of the Office of the University CIO;
- circulating to members of the University-wide ICT team for feedback;
- circulating to members of the wider University for feedback;
- tabling at a meeting of the ICT Steering Committee at each campus;
- tabling at a meeting of the University ICT Steering Committee for initial acceptance;
- presenting to the University Finance and General Purposes Committee for ratification.

  (Policy ratification is done by the University Finance and General Purposes Committee on behalf of University Council.)

- monitoring and evaluation will be conducted by the University ICT Steering Committee, through the Relevant IT Authorities across the University.

1.7 KEY DEFINITIONS

Campus IT Services (CITS)	The generic description for the department, at each campus, that provides information technology and related services to the campus (and UWI affiliated units at that campus). All centre departments, that is, departments which operate at the regional level, are affiliated with a campus and are therefore serviced by the CITS at the campus with which it is affiliated.
Critical Information Infrastructure	Any Information system (including all hardware and software) that might halt University operations if interrupted or damaged.
Information Asset	Any data, device, or any other component of the environment, that supports information-related activities.
Information Owner	The individual with decision-making authority for data, as well as any forms, files, and records, regardless of their format, used to conduct UWI business. The Information Owner is normally the head of a department, Dean, or Registrar.
Information Security Metrics	Measurements that are compared with a specific baseline/benchmark of what should be expected.
Information Security Awareness Programme	A set of coordinated activities aimed at educating persons to defend information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction.
Malware	Any computer software that is used to compromise systems, destroy data, gather information, restrict access to systems, and gain unauthorised control of hardware and software. They may be represented by, but not limited to viruses, Trojans, worms and spyware.

Relevant IT Authority	The Chief Information Officer at the respective Campus or Centre (or his/her designate with responsibility for information security).
Remote access	Any access to a UWI information system by a user communicating through an external network such as the Internet.
Security Task Force	Any group of selected staff responsible for monitoring the Critical Information Infrastructure.

2.0 POLICY STATEMENTS

2.1 APPLICABLE LAWS

All UWI staff shall, as best as they are able, adhere to the applicable national or international laws, within their jurisdiction, concerning information security.

2.2 INTERNATIONAL GUIDELINES AND BEST PRACTICE

UWI shall use, but not be limited to, the following standards to protect its information assets:

- The International Organization for standardization (ISO) ISO/IEC 27001 suite;
- The National Information Standards and Technology (NIST) 800-100 Information Security Handbook: A Guide for Managers;
- The National Information Standards and Technology (NIST) 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems;
- The International Organization for standardization (ISO) ISO/IEC 31010:2009 Risk Assessment Techniques;
- The National Information Standards and Technology NIST 800-30 rev. 1 Guide for conducting Risk Assessments;
- SANS Institute's Top 20 Critical Security Controls.

2.3 COMPLIANCE WITH OTHER UNIVERSITY POLICIES

The protection of information assets shall also conform to the following UWI policies:

a. Policy on Intellectual Property (1998);
b. Policy on Release of Information about Students (1997);
c. Revised Procedures for Handling Confidential and Highly Restricted Documents (2013);

d. Statement of Principles/Code of Ethics for Academic and Senior Administrative Staff (1998);
e. The Acceptable Use Policy, Information and Communication Technology (2014);
f. The Code of Principles and Responsibilities for Students (2001);
g. The University Archives and Records Management Policy (2012).

2.4 KEY ROLES AND RESPONSIBILITIES

This section outlines the roles and responsibilities of all members of the UWI community and several critical participants in the information security process.

2.4.1 General

All members of the UWI community, including visitors, share in the responsibility of protecting any UWI information asset to which they have access, or for which they have custody.

2.4.2 Heads of Department shall:

- convey to staff within, and visitors to, their department the general responsibility to protect UWI information assets;
- ensure that all staff members participate in security awareness programmes whenever such programmes are held.

2.4.3 Information owners shall:

- establish administrative procedures for accessing and using information under their jurisdiction;
- document requests for information and ensure that this documentation is available for future reference;
- report any breach in the processing or dissemination of information to the Relevant IT Authority.

2.4.4 The Relevant IT Authority shall:

- participate in the review and update of this Policy;
- ensure that information security initiatives are integrated with strategic and operational planning initiatives;
- be responsible for communicating information security initiatives to staff members;
- establish (or assist in establishing) and maintain an Information Security Awareness Programme;
- establish monitoring measures to detect and correct information security breaches;

- provide periodic reports to the respective ICT Steering Committee and Executive Management, either directly or through a designate, on the status of information security programmes;
- report, to the respective ICT Steering Committee and Executive Management, either directly or through a designate, material information on security incidents;
- participate in the design and implementation of Business Continuity and Disaster Recovery procedures.

2.4.5 Campus IT Services shall:

- oversee the campus' Information Security, through a competent IT Officer (or Officers);
- implement security monitoring and prevention strategies for UWI's Critical Information Infrastructure;
    - manage domain user accounts, including activation, deactivation, changes, and audits;
    - authorise, document, and monitor all remote access capabilities;
    - develop formal procedures for authorised individuals to access UWI information systems from remote systems;
        - ensure that all remote access connections that utilise a shared infrastructure, such as the Internet, use some form of encryption for the transmission of data and authentication information;
        - ensure that Virtual Private Network (VPN), or equivalent, technology is used when remotely accessing information systems;
- promote security awareness programmes focused on the protection of UWI's information assets;
- ensure that visitors, both physical and virtual, to a UWI location (campus/site), such as vendors, scholars and other non-staff members, are aware of the Policy;
- draft procedures to promote compliance with this Policy or to the respective campus-specific information security policy;
- draft procedures for handling information security breaches *(See sample Information Security Incident Form – Appendix I)*;
- on a periodic basis, report to Campus Management, through the relevant ICT Steering Committee, on the status of Information Security at the campus;
- collaborate with the University Enterprise Risk Manager on initiatives to manage risks that, if realised, might have severe business impact on UWI;
- design an Information Repository that will house information about information security plans, breaches, remediation processes, upgrades and tacit information.

- collaborate with other higher education institutions and/or organisations on information security strategies and best practices;
- periodically, at least once per academic year, test business continuity, incident response and disaster recovery procedures;
- develop secure configuration settings for all hardware and software *(refer to 2.6.2 Information Security Baseline);*
- ensure that all IT personnel who are a part of the processing of information have clearly defined roles and responsibilities.

2.4.6 The University Enterprise Risk Manager shall:

- ensure that all Heads of Department, through the University Registrar and respective Campus Registrar, are aware of the ICT risks faced by their respective department;
- assist in creating an awareness of the implications of the risks that face each department;
- provide guidance on managing the risks identified.

2.5 INFORMATION SECURITY RISK ASSESSMENT

Risk assessment identifies, quantifies, and prioritises risks based on risk acceptance and the objectives of the University. The assessment results guide the determination of appropriate management action and priorities for managing information security risks as well as highlighting the deficiencies in the controls which should be in place to guard against these risks.

2.5.1 Each campus, through the Relevant IT Authority and CITS and with the assistance of The University Risk Manager, shall conduct periodic risk assessments (at least once per academic year).

2.5.2 Risk assessments shall utilise a tested and proven information security framework/standard such as:

- NIST 800 series publications;
- ISO 27001;
- COBIT Information Security;
- ITIL.

2.6 SECURITY CONTROLS AND MONITORING

The University's critical information infrastructure comprises all systems which are vital to the function and operations of UWI. The following categories are to be used to establish critical security controls to protect this infrastructure.

Asset Management

2.6.1.1 **Inventory of Assets**

CITS shall maintain an inventory of IT assets organised as outlined below:

Information Assets: databases and data files, system documentation, user manuals, training material, operational or support procedures, disaster recovery plans, archived information.

Software Assets: application software, system software, development tools, utilities, virtual servers.

Physical Assets: critical computer equipment (routers, switches, physical servers, security devices), communication equipment (PBXs), Uninterruptible Power Supplies.

Services: Service catalogue

2.6.1.2 CITS shall ensure that all hardware and software systems maintain a secure baseline configuration at all times *(refer to 2.6.2 Information Security Baseline)*.

2.6.1.3 **Information Classification**

Information should be classified by Information Owners according to its sensitivity, that is, the effect unauthorised access might have on members of the University community. Access to information is then determined by its classification as outlined in the table below.

Classification	Definition
Open	Information which may, or must, be open to the general public. This information has no existing local, national, or international legal restrictions on access. ***Example:*** *Course Catalogue.*
Confidential (Restricted)	Information protected by statutes, policies or regulations. These protections delimit its use. The Information Owner may exercise his/her right to restrict access. ***Example:*** *Student academic*
Sensitive	Information for which access must be guarded due to proprietary, ethical or privacy considerations. Unauthorised access, whether from members of the University community, may lead to damage to individuals, the University or their interests. ***Example:*** *Date of Birth, gender.*

Note: *Two documents provide details on the treatment of Confidential Information*

i. *Guidelines for Marking and Handling University Information; and*
ii. *The Revised Procedures for Handling Confidential and Highly Restricted Documents.*

2.6.2 INFORMATION SECURITY BASELINE

An Information Security Baseline is the minimum required to protect the confidentiality, integrity and availability of information assets. CITS shall employ baseline requirements in the following areas.

2.6.2.1 Network Security

All interconnections should be guarded by, but not limited to, intrusion detection and protection systems and firewalls.

2.6.2.2 Secure Endpoints

All endpoints shall be configured using industry standard practices to protect their integrity and confidentiality.

2.6.2.3 Application Development Security

Application development shall follow international best practices and standards such as ISO/IEC 27034:2011

2.6.2.4 Access Control

Only authorised devices and systems shall be given access, and unauthorised and unmanaged devices and systems shall be found and prevented from gaining access. It is therefore necessary to:

- manage user accounts, including activation, deactivation, changes and audits;
- ensure that the granting of access to all electronic information must be documented and signed off by the Information Owner;
- identify, document and approve specific user actions that can be performed without identification or authentication;
- ensure that all roles and responsibilities are clear and the appropriate access granted.

2.6.2.5 Physical Security

Ensure physical protection of all communication equipment and peripherals, data transmission media, storage and power systems including the spaces they occupy.

2.6.2.6 Malware Protection

All systems both hardware and software shall be protected against the potential risks posed by malicious software by the installation of internet security software and applying patches to address security vulnerabilities.

A member of the IT staff should be assigned the responsibility of monitoring the release of security updates and patches by software vendors.

2.7 INCIDENT RESPONSE

Compromises in security can potentially occur at all levels, from a desktop computer to a server in the data centre. An incident can be an accidental incursion or a deliberate attempt to break into systems and can be categorised from benign to malicious in purpose or consequence. Regardless of intent, each incident will require a careful response commensurate with its potential impact to the security of individuals and the campus as a whole.

- All incidents shall be documented as soon as possible after they have been discovered. *(See sample Information Security Incident Form – Appendix I)*
- Once an incident has been reported, the response to it should be based on a pre-defined process. *(This pre-defined process shall be determined by each CITS unit and documented.)*

3.0 INFORMATION SECURITY AWARENESS

This is the knowledge and attitude of members of the UWI community and visitors concerning the protection of the University's information assets. Developing a security awareness plan is a major initiative to not only educate but to craft a defence strategy against information security breaches.

- The Relevant IT Authority and CITS at each campus shall conduct an Information Security Awareness Programme at least once every academic year.
- The awareness programme should educate all staff members on self-protection strategies and mitigation techniques.

4.0 PENALTIES FOR MISUSE

Where there is evidence of misuse of UWI Information assets, UWI may restrict or prohibit the use of these resources.

UWI members who breach this Policy may face disciplinary action under the University statutes and ordinances which includes termination of employment in the case of staff members; and suspension or expulsion in the case of students. Violation may also constitute a breach of national law

5.0 LOCALISED POLICIES

Notwithstanding the broad elements of this policy, campus units may establish or seek to establish complementary policies, standards, guidelines or procedures that refine or extend the provisions of this policy and to meet local needs. All such extensions shall comply with University Regulations, Ordinances and national laws.

6.0 PRIVACY AND CONFIDENTIALITY

The University requires that the architecture, processes and procedures surrounding software applications be such that privacy of University data and information is protected. Users of University-supplied or supported applications should be advised of the procedures required to maintain privacy of University data and information.

6.1 RIGHT TO MONITOR ICT SYSTEMS

Notwithstanding the UWI's acknowledgement of an inherent right to privacy by users of the University-provided ICT systems, the University reserves the right to monitor, audit and interdict all data traversing its networks or stored on its systems in furtherance of its duty to secure and retain the confidentiality and integrity of its data and information resources.

7.0 STATEMENT OF LIABILITY

The University of the West Indies (UWI) shall not be liable for any errors, omissions, loss or damage claimed or incurred due to any use of any University information asset that does not comply with this Policy or the policies cited herein.

8.0 USER ACCEPTANCE

All users of UWI's information and communication technologies are required to sign this document, or otherwise signify acceptance of this Policy, and thereby commit to abide by its provisions. Those who log in to UWI's data network, by entering the username and

password provided by the Campus IT services at one of the four UWI campuses, signifies acceptance of this Policy.

8.1 USER ACCEPTANCE STATEMENT SIGNING SHEET

I understand that UWI provides, operates and maintains its ICT resources to support its teaching, research, and administrative activities.

I understand that my assigned access credentials (including user names, passwords and PINs) identify and allow my access to UWI's ICT resources and that I am accountable for the secrecy of my access credentials. I also accept and agree that I am responsible for all actions committed through the use of my access credentials.

I will comply with the UWI's Information Security Policy and accept that as a user of the UWI's ICT resources I have a responsibility for the security of those resources.

To the best of my ability I will protect the UWI's ICT resources from unauthorised use, modification, destruction or disclosure, whether accidental or intentional. I agree to be bound by the current version of UWI's Information Security Policy and the Information Security Policy Guidelines, which will be freely available to the UWI community.

I understand that failure to comply with these requirements, and others which may be declared in the future, may result in disciplinary and/or legal action.

Persons found in violation of this Policy may be liable to disciplinary action under University statutes and ordinances. Violation may also constitute a breach of national law.

I hereby acknowledge that I have read and understand UWI's Information Security Policy and the Information Security Policy Guidelines.

Name:	Date:
Signature:	Student/Staff ID No:
Position:	Campus:
Office/Faculty:	Department/Unit:

APPENDIX I: SAMPLE INFORMATION SECURITY INCIDENT REPORTING FORM

Information Security Incident Reporting Form

Campus:
Department:
Date and time of Incident:
Point of Contact
Name: **Phone:**
Incident Details (Please tick (√) the appropriate section below).

	Incident Category		Incident discovery method
	Unauthorised access		Anti-virus
	Denial of Service		Log Audit
	Malicious Code		Intrusion Detection (IPS/IDS)
	Improper Usage		User Complaint
			System Administrator
			Other (Specify):

Source of Incident

IP Address Port # Protocol

Destination

IP Address Port #

Affected System:

System Function (e.g., DNS, Web server etc.) _____

Operating System Version Date of Latest Updates

Antivirus Installed Version Date of Latest Updates

Briefly describe the incident including its impact.

What actions were taken to reduce the risk of this type of incident happening again?

REFERENCES

Woodbeck, D. (2014). Outline of Model Security Policy Elements. Available at: https://wiki.internet2.edu/confluence/display/itsg2/Outline+of+Model+Security+Policy+Elements. (Accessed October 13, 2014).

Brotby, W.K. and The IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management.* 2nd Ed. [ONLINE] Available at: http://www.isaca.org/Knowledge-Center/Research/Documents/InfoSecGuidanceDirectorsExecMgt.pdf