THE UNIVERSITY OF THE WEST INDIES
Information & Communication Technology Security Policy

1. Introduction

In accordance with its broader strategic objectives, The University of the West Indies, [hereinafter "the UWI"] has procured and implemented at various locations, Information and Communication Technologies (ICTs) that are used to create, process, store, share and disseminate data and information. These assets represent a significant economic investment by the UWI. The data and information resources they create, store and disseminate could well be priceless and irreplaceable. Their continued availability in furtherance of the UWI's business is of paramount importance, hence, there is a compelling need to secure and control access to them.

Users of university electronic information systems and other stakeholders have an expectation of privacy for their personal data gathered by the UWI in the normal course of its business. Therefore, there is a reasonable expectation from users that the UWI would institute controls to conserve the privacy of personal information. Confidentiality of information is demanded by the common law, national statute as well as university ordinances, regulations and convention. Since the UWI operates on an international stage offering higher education services in a global marketplace, misuse of the institution's ICT assets could degrade its goodwill and reputation.

The UWI acknowledges that there is a well-founded requirement to maintain the integrity and confidentiality of its electronic data and information. Such assets must be protected from unauthorized access and intrusions, malicious misuse, inadvertent compromise and intentional damage or destruction. Accordingly, the UWI is obliged to ensure that appropriate security measures are enacted for all electronic data and information, as well as ICT equipment and processes in its domain of ownership and control.

1.1 <u>Purpose</u>

This policy is prepared for the direction and use of personnel engaged in the implementation and support of the UWI's ICT systems and the services delivered thereon. It is intended to inform:

- the development and implementation of rules, guidelines and a code of practice to secure the UWI's ICT systems and services;

- the development of mechanisms that will help the University to reduce its legal risk brought about by an increasingly interconnected world;
- the UWI community about the rules and practices pertaining to confidentiality and security of the University's ICT resources;
- custodians of University ICT systems and services about their responsibilities with respect to the preservation of these systems and the sanctions for non-compliance.

1.2 Scope

This policy outlines the requirements for securing UWI's data and information assets and provides the groundwork for the development of local policies, guidelines and best practices insofar as it is practical. This policy applies to the mitigation of the following categories of risk:

- Computer system availability
- Conservation of University ICT assets
- Integrity of University data and information
- The confidentiality of University information
- Efficient use of University ICT resources

It covers the following security domains:

- The physical security of all computing and communication premises, computers, communication equipment and appliances, transmission paths and computer peripherals.
- The physical security of all storage media for data, system software, application software and documentation.
- The physical security of power systems supplying electrical power to network communication and computer systems.
- The logical security of data, information and information processing resources such as databases, computer programs, email records, servers, routers, switches and other network appliances.

2. Roles and Responsibilities

ICTs are provided and deployed by the UWI to support the operational and administrative functions of Teaching, Learning, Research, and the management of its business. They are intended to be used primarily as business tools and to provide other support services.

2.1 General

The ICTs deployed are University facilities. All such technologies are and remain the property of the UWI, certain assigned Intellectual Property rights excepted.

2.2 Roles

Campus ICT Services Departments shall:

- Account for all ICTs and information resources in their area of jurisdiction that is connected to campus networks by one or other means.
- Provide and maintain a database of unique identifiers for all network-connected ICT assets.
- Assess the security risk of all ICT systems and apply such security systems and processes as are consistent with the mitigation of this risk.
- Provide and/or commission the physical security of all enterprise servers, databases, backbone network switches and ICT management, teaching and learning platforms.
- Procure, implement and maintain the logical security systems as are necessary to protect University electronic data and information assets from misuse, damage, loss or unauthorized access.
- Develop, document and publish the ICT security guidelines in accordance with and informed by best practice.
- Promote a security awareness campaign for users of University ICT systems and collaborate with functional departments to design and deliver end user ICT security awareness training.

Heads of Departments with functional ownership of data and information resources shall:

- Assess the security risk to data and information resources developed, generated and produced in their operations
- Determine the confidentiality requirements for data and information resources developed, generated and produced by their departments
- Collaborate with University and Campus ICT management to develop and implement procedures that establish and manage privilege to access confidential data and information resources
- Ensure every user in their jurisdiction and span of control is informed of the security requirements

2.3 Responsibilities

a) The Campus Information Technology Services department at each campus [hereinafter the Competent Authority] is responsible and accountable for all aspects of the design, implementation, administration and maintenance of all ICT security systems and the processes and procedures by which these operate. The Competent Authority has the duty to immediately suspend privilege, access and service to any user in breach of this policy pending further enquiry. Such restrictions as applied are subject to review by the appropriate superior university authority

b) Users of the services are responsible for maintaining the security of their interfaces to University-owned ICTs, data and information resources by complying with Campus and University policies, the applicable University statutes and ordinances, and related national and international laws. Persons found to be 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.

c) Functional Managers and Heads of Departments are responsible for enforcing the application of the security policies covering ICTs, data and information resources as set out in local guidelines and practice documents

3. Qualifying Users

Users of University ICTs, data and information resources shall be limited to UWI students, faculty, staff and other approved persons, for purposes that advance the objectives of teaching, learning, research, outreach and administration. These classes of users must be known to and defined in the existing gateway systems such as one or other of Enterprise Resource Planning (ERP), Human Resource Management Information System (HRMIS), Student Administration System (SAS) or teaching and learning platforms. Any exception must be authorized by the Chief Information Officer in conjunction with a Head of Department.

4. Physical Security & Integrity of Systems

Appropriate barriers and controls governing the physical access to, and the maintenance of, the integrity of critical University ICT assets must be deployed commensurate with the risk identified. These risks include identified natural and environmental hazards. Barriers and controls include, but are not limited to, electronic access control to servers and critical network infrastructure, installations of grillwork surrounding and enclosing video systems, fire suppression, and power management systems. Physical ICT assets include but are not limited to multifunction devices, servers, communication switches, personal computers, cameras, printers, plotters, multimedia projectors, media management platforms, scanners, media containing software, books and manuals.

5. Logical Security & Integrity of Systems

Authentication and authorization functions must be employed for all users of University electronic data and information resources. A central authentication database shall be established for all users. Procedures to manage access, authentication and authorization shall be developed to support and manage these activities. Such processes and procedures include but shall not be limited to user passwords for network and application access, biometric access mechanism, tokens and electronic key devices. For the purposes of this paragraph, computer and other electronic processes are deemed to be users.

5.1 Software and Firmware upgrades

All computers, switches, routers and other network-attached devices shall have the most recent approved and released software and firmware security patches installed as soon as they are generally available.

5.2 Malware control

Malware is a common feature of globally connected networks. Personnel engaged in the implementation and support of the UWI's ICT systems shall take all appropriate steps to protect its ICT assets from damage, compromise or loss of confidentiality. For the purposes of this policy, malware is defined as software agents that by their action deny users the maximum capabilities of the ICT systems, compromise the security and confidentiality of university data and information or destroy or damage university ICT assets. Malware may be represented by but is not limited to spyware, viruses, worms and spam.

5.3 Network Interconnections

Interconnections among networks are unavoidable in the ordinary course of business. These interconnections are portals for unauthorized access and entry to University networks and pose significant risk to the security of University data and information resources. Therefore all network interconnections shall be guarded, and audited by processes and such perimeter defence and intrusion detection systems, as are appropriate to manage and mitigate these risks.

5.3.1 Access to Business Critical systems

The University is dependent on several of its major systems for its daily operations. Breaches to their integrity, or their unavailability for any significant period of time, could reduce the service delivery capability or place the institution in disrepute. Such systems may include the Student Administration System, online teaching and learning platforms, the financial management system, the enterprise planning and/or human resource management information system. Notwithstanding the general security safeguards enunciated before, these business-critical systems shall be provided with an elevated level of security. These additional measures shall include, but are not limited to, internal firewalls, secondary access challenges and biometric access controls. When the security requirements are stringent enough, internal isolation of the network segment to which such systems are attached is the final consideration.

6. Privacy and Confidentiality

The University requires that the architecture, processes and procedures surrounding applications must be such that privacy of University data and information is protected. Users of University-supplied or supported applications must 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 electronic payloads traversing its networks or stored on its systems in furtherance of its duty to secure and retain the confidentiality of its data and information resources.

7. 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 specific local needs. In any event, such extensions shall comply with university regulations, ordinances and national laws.