Information and Communications Technology Unit
Risk Management Report

Potential Problem	Possible Causes	How Likely	Impact	Ways to limit risk/recommendation	Results of action taken
1.Major Information security breach/intrusion in our network infrastructure	Computer virus from unsecured servers; illegal/unauthorized intrusion	low	maximum	Ensure safe computer usage practice	With the following: -Implement appropriate network security measures by upgrading firewall to provide unified threat management capabilities, -installation of enterprise antivirus solutions from servers to workstations. Enterprise anti-virus system is constantly upgraded and/or change based on evaluation on its effectiveness and performance. -implementation of active directory in critical areas. -Implement DMZ for server resources such as databases and application servers -Separate internet lines between offices and wifi/laboratories :No major information security breach/intrusion in TUAs network

					infrastructure is experienced
2. major network breakdown	Force majeure; physical destruction of cables	low	maximum	consistent monitoring of network facilities	With the following: -Implement appropriate preventive maintenance of network infrastructure -Implement redundancy and backup measures on application servers and databases, especially for the enrollment system -Implement backup airconditioning unit for the data center :No major network breakdown is experienced
3.Major Information security breach/intrusion in the TUAPORTAL/TAIMS	Computer virus from unsecured servers; illegal/unauthorized intrusion	medium	maximum	Observe technical security principles fundamentals	With the following: -Implement DMZ for server resources such as databases and application servers -Separate internet lines between offices and wifi/laboratories -implement user credentials management :No major Information security breach/intrusion in the TUAPORTAL/TAIMS is experienced certificate infrastructure

4. Data breach or security incident under the Data Privacy Act Compliance	Ignorance of the Data Privacy Act Lack of mechanisms for the Data Privacy Act	medium	maximum	Creation of clear policies and procedures in adherence to the Data Privacy Act. Setup infrastructure and tools to protect the University's data.	With the following: ● Compliance to the phase 1 and phase 2 set by the national Privacy Commission ● Implement the recommended guidelines set by the national Privacy Commission such as Privacy Impact Assessment ● Conduct general orientation for the entire University constituents :TUA is in adherence with the Data Privacy Act
5. Unavailability of Information and Communications Systems such as telephony, internet, system applications (e.g. enrollment system): a. Due to power failure	Brownout/black out/power outage Service provider system failure Data center's equipment failure/Network infrastructure failure System software	low	maximum	Setup of power redundancy such as power generator and uninterrupted power supply in the data center Redundancy of telephony and internet facilities System and data backup Continuous update of application systems	With the following: -implement power generator equipment -implement an uninterrupted power supply equipment that will cover the entire work day -implement several lines of telephony from various providers -implement several lines of internet facilities from various providers

b. Due to system crash or error	failure				-conduct a regular preventive maintenance for network infrastructure and equipment -implement a regular backup procedure :Telephony, Internet and application systems are highly available majority of the time

Prepared by:	Reviewed and Endorsed by:	Approved by:
Randy D. Lagdaan Director, ICTU	Ms. Leonora N. Yngente Vice President for Administration and Finance	Dr. Wilfred U. Tiu University President