STUDENT ID: 816003952

STUDENT NAME: TENEIL RODRIGUEZ

COURSE: INFO 2604 INFORMATION SYSTEMS SECURITY

PART 3

Policies

Internet use policy

purpose

The purpose of this policy is to establish the appropriate use of the internet by the Students at U.W.I in the DCIT computer labs. Effective implementation of this policy to prevent the students from misusing of the lab equipment which will prevent hardware/software malfunctions.

Scope

The internet policy applies to the usage of the internet by all users who gain access through computers or networking resources within the DCIT computer labs. All Internet users are expected understand and are expected to comply with this policy.

Security assessment

Accessing the internet can leave you venerable malicious code such as viruses, worms, trojans etc. These malicious codes can corrupt computer network and can even be cause loss/ theft of restricted and confidential information from the DCIT department. They may also cause system failure in the department. The following policies have been developed to prevent against these threats.

* The access to the internet must be consistent with the academic objective of the student such as research. Student will only gain access to computer network resources via their distinct university user name and password.
* Attempts to access restricted sites, servers, databases, etc are strictly prohibited. If a student is caught attempting such action they shall be penalised appropriately.
* The downloading of unauthorised software (such games) on the systems is prohibited.
* The use of the system for (unauthorized) online gaming, multi-user internet gaming is prohibited.
* The use of audio broadcast or video streaming for non-academic purposes is prohibited.
* The use of the internet non-university related commercial purposes, financial gain, personal business, product advertisement, or political lobbying is prohibited.
* If a student identifies a security/system problem, they are required to notify the lab personnel immediately and not exercise their own problem-solving skills by trying to fix it themselves.
* The removal or disconnection of lab equipment is prohibited.

Disaster recovery policy

Purpose

The purpose of this policy is to establish a strategic plan for safeguarding the vital software and hardware managed by the DCIT department at U.W.I. the successful implementation of this policy will ensure that the effects of a disaster is minimised.

Scope

The Disaster recovery policy is geared toward having a systematic approach to protecting the software and hardware that is vital to the performance of the DCIT department at U.W.I. The head of the department along with the key members of the department are required to be familiar with the policy.

Loss software and hardware due damages caused disaster can disable the DCIT department from functioning due to loss of vital files such as student records and teaching resources. The loss of student records would have a major effect as this information Is vital as it contains the student’s academic record for their degree. The following policy have been developed to prevent against these threats.

* (prior to disaster) Value assessment of the vital hardware and software with in the department regularly.
* Budget assessment for possible recovery of vital hardware and software in case of disaster.
* Every DCIT lab must be equipped with a fire extinguisher, smoke detectors and a fire alarm.
* All vital software must be backed-up daily at a specifically scheduled time.
* Back-ups shall be taken to a safe/secure location.
* A log of the backups should be kept, and the log must be checked to ensure successful backup was made.
* (prior to disaster) Hardware component should be elevated from the floor.
* A complete assessment of the damager should be made.
* Temporary space should be allocated to house classes while repair and being made.
* Restore vital system with backup.
* Assess the likely duration required to fix the damages and restore systems that have been affected.
* Seek financial assistance if necessary or possible.

Antivirus policy

Purpose

The purpose of this policy is to establish appropriate antivirus requirements for the DCIT department to ensure effective virus detection and prevention.

Scope

This policy must be applied to all the computers and networks within the DCIT department to be able to protect the system from viruses that will cause failure to the computer systems within the department.

Security assessment

Virus affected computer are usually much slower and programs launch takes longer as well as increase freezing and crashing of the computer. The data in the DCIT department that may become affected by a virus can become corrupted. This is either through the virus rendering the files unusable in a process or destroying the data. Files and folders can be deleted or become inaccessible. The following policy have been developed to prevent against these threats.

* All DCIT labs computer must have high quality standard antivirus software installed.
* This software must be regularly updated to ensure that the antivirus software is up to date.
* Computer that have been affected by a virus must be removed from the system until the problem has been rectified through the removal of the virus and an update of the computers antivirus software.
* Regular system test should be performed on the computer to ensure no viruses have infiltrated the system.
* All files in the computer shall be scanned systematically for viruses.