UNIVERSITY OF WAH

IT Policy

January 10, 2014

Document Revision History

Revision No	Revision Date	Description	Page No

Table of Contents

Introduction

Introduction

The exponential growth in Information Technology, since 1950, has influenced every aspect of our lives at home as well as at work. One of the most stimulated being the Higher Education sector. Information technology offers increased opportunities for communication and collaboration and has changed the way we conduct business as a university. Institutions have made major investments in the new technologies, distributing computing capacity across their campuses, linking faculty with students as well as with one another, and generally providing the necessary IT infrastructure that is a precondition to faculty involvement and educational management system. The demand for IT-based teaching and learning programs will grow substantially, probably exponentially, over the next decade. In an economy that is itself increasingly knowledge-based; the new information technologies offer an economical means of providing the continuous education. IT will change teaching and learning profoundly, no matter what the response of traditional higher education institutions. IT offers great potential but in order to reap the benefits, institutions will have to transform themselves in fundamental ways. Our task is to understand these changes in terms that are both practical and operational. Perhaps IT's most widely known potential, through such tools as the Internet and the various online databases, is access to enormous quantities of information. As systems become increasingly sophisticated, IT will provide a growing capacity to navigate among such information resources at low cost. In the future, students will be able to access any desired information without moving from their chairs. In the past, libraries held the keys to research and knowledge; in the future, networked desktops will allow much of the same access when and where the user desires it.

Purpose

Any organization that uses computers, email, the internet, and software on a daily basis should have information technology (IT) policies in place. It is important for users to know what is expected and required of them when using the technology provided by an organization, and it is critical for an institution to protect itself by having policies to govern areas related to IT use. The purpose of this document is to create a well-written IT policies and procedures Manual that improves performance by enhancing consistency and establishing clear criteria for computer, network, software, IT security, and IT vendors. The University provides the IT Resources for the advancement of the University's educational, research, service, and business objectives. Any access or use of IT Resources that interferes, interrupts, or conflicts with these purposes is not acceptable and will be considered a violation of this Policy Statement (referred to hereafter as "IT Policy"). The goals of this policy are to maintain the confidentiality, integrity, and availability of the university's network infrastructure and information assets to all stakeholders. The major areas addressed are:

1. **Security Issues:** Guidelines for passwords, levels of access to the network, virus protection, confidentiality, and the usage of data.

2. **Users Responsibility:** Users Guidelines for the use of computers, fax machines, telephones, internet, email, and voicemail and the consequences for misuse.

3. **Network Policy**: Guidelines regarding how the network is configured, how to add new employees to the network, permission levels for employees, and licensing of software.

4. **Technology Standards**: Guidelines to determine the type of software, hardware, and systems will be purchased and used at the University, including those that are prohibited (for example, instant messenger or mp3 music download software).

5. **IT Services**: Guidelines to determine how technology needs and problems will be addressed, who in the organization is responsible for employee technical support, maintenance, installation, and long-term technology planning.

6. **Disaster Recovery:** Guidelines for data recovery in the event of a disaster, and data backup methods

Policy Statement

Information Technology is provided to support the teaching, learning, research and administrative activities of University of Wah (referred to hereafter as UW). The data held on the network forms part of its critical assets and are subject to security breaches that may compromise confidential information and expose university to losses and other legal risks. These University of Wah guidelines and policies change from time to time; therefore users are encouraged to refer to on-line versions of this and other university policies on the web site. Any infringement of these regulations may be subject to penalties under civil or criminal law, and such law may be invoked by the University of Wah. Any infringement of these regulations constitutes a disciplinary offence under university’s procedures and may be treated as such regardless of legal proceedings. Abuse of the regulations may result in the user’s account(s) being suspended. These regulations are periodically reviewed by the IT Department.

Scope

This policy applies to all IT Custodians and IT Owners of department or enterprise information technology resources (including, but not limited to, any networking devices, network monitoring devices, computers acting as network monitoring devices, intrusion detection systems, other packet sniffing devices, logs of other devices such as firewalls, and flow detectors monitoring network activity) operating on a university network. This IT Policy shall also apply to any and every member of the University community including, but not limited to, faculty, students, administrative officials, staff, and independent contractors who uses, accesses, or otherwise employs, locally or remotely, the University's IT Resources, whether individually controlled, shared, stand-alone, or networked.

Structure

University information resources consist of the computer devices, data, applications, and the supporting networking infrastructure. Users of these services include but not limited to:

- All students, faculty, and staff use e-mail services
- All members of the university can obtain wireless connectivity
- Every campus dormitory room has a connection to the Internet
- Students submit assignments via the Internet
- Admission at university and associated institution uses internet services

These are but a few of the many examples of how information resources are connected to many activities at the university.

Security Issues

1. Security Issues

Security issues perhaps constitute the most important aspect of IT Policy. Security threats presented in this document are selected based on their occurrence and significance. The threat resource is categorized into four main groups:

- Environmental/physical threats
- Human threats
- Natural threats and
- Technical threats.

The categories list is not exhaustive. It is developed as a guide for identification of threats and vulnerabilities. As conditions and technology change, other categories not included here could apply to the system under review.

Out of numbers of types of threats two categories namely; human threats and technical threats pose the biggest challenge to the network administrative.

- Human Threats may include:

  Arson, Data Entry Errors or Omissions, Espionage Impersonation. Improper Disposal of Sensitive Media, Acts or Carelessness, Omissions, Procedural Violation, Theft, Sabotage, Vandalism, or Physical Intrusions, User Abuse or Fraud.

- Examples of Technical threats:

  Unintentional data-related or intelligence-bearing signals, Corruption by System, System Errors, or Failures, Data/System Contamination, Eavesdropping, Hardware / Equipment Failure, Impersonation, Insertion of Malicious Code or Software, or Unauthorized Modification of a Database Installation Errors, Intrusion or Unauthorized Access to System Resources, Jamming (Telecommunications), Misuse of Known Software Weaknesses.

1.1 Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. The following levels are to be used when classifying information:

1.1.1 Sensitive Information (Examination record.)

i. Credibility of a university is critically dependent on integrity, reliability and accuracy of examination data such as: transcript record, CGPA obtained, personal data that permits identification of the individual or could reasonably be used to identify the individual (registration No. etc.)

ii. Unauthorized or improper disclosure, modification, or destruction of this information could cause serious damage to the university and its students or research interests.

1.1.2 Confidential Information

i. Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Examples of Confidential Information may include: personnel information, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys.

ii. Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations, or may cause significant problems for the University, its students, or its business partners. Decisions about the provision of access to this information must always be cleared through the information owner.

1.1.3 Internal Information

i. Internal Information is intended for unrestricted use within University, and its affiliated organizations such as Wah Engineering College (WEC). This type of information is already widely-distributed within University, or it could be so distributed within the organization without advance permission from the information owner. Examples of Internal Information may include: personnel directories, internal policies and procedures, most internal electronic mail messages.

ii. Any information not explicitly classified as Confidential or Public will, by default, be classified as Internal Information.

iii. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

1.1.4 Public Information

i. Public Information has been specifically approved for public release by a designated authority within each entity of the University. Examples of Public Information may include prospectus, admission policy, marketing brochures and material posted to the University's Internet web pages.

ii. This information may be disclosed outside of The University.

1.2 Information Security Responsibilities

1.2.1 Chief IT Administrative:

The chief administrative of information is generally responsible for the processing and storage of the information. The administrative is responsible for the administration of controls as specified by the owner. Responsibilities may include:

i. Providing and/or recommending physical safeguards.

ii. Providing and/or recommending procedural safeguards.

iii. Administering access to information.

iv. Releasing information as authorized by the Information Owner and/or the head of the institution for use and disclosure using procedures that protect the privacy of the information.

v. Evaluating the cost effectiveness of controls.

vi. Maintaining information security policies, procedures and standards as appropriate and in consultation with the competent authority.

vii. Promoting employee, faculty and student's education and awareness by utilizing programs approved by the competent authority, where appropriate.

viii. Reporting promptly to the concerned authority the loss or misuse of the University information.

ix. Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

1.2.2 User Administrative:

The University management who supervise users as defined below. User management is responsible for overseeing the use of information, including:

i. Reviewing and approving all requests for their employee's access authorizations.

ii. Initiating security change requests to keep employees' security record current with their positions and job functions.

iii. Promptly informing appropriate parties of employee terminations and transfers, in accordance with local entity termination procedures.

iv. Revoking physical access to terminated employees, i.e., confiscating keys, changing combination locks, etc.

v. Providing employees with the opportunity for training needed to properly use the computer systems.

vi. Reporting promptly to the Chief Administrative the loss or misuse of University information.

vii. Initiating corrective actions when problems are identified.

viii. Following existing approval processes of the University for the Selection, budgeting, purchase, and implementation of any computer system/software to manage information.

1.3 Internet Usage Policy

Internet access shall be provided on "need to use" basis. Anyone who requires it shall be given access after appropriate authorization. Such access shall be reviewed periodically by the competent authority Internet facility shall be provided only through proxy server and university reserves every right to monitor, examine, block or delete any/all incoming or outgoing Internet connections on the university's network. Users shall not use modem / wireless data card / any other media to access internet while being connected to the University network. Internet usage policy is highlighted below:

1.3.1 Use of personal Instant messenger and chat is prohibited

Very selectively when instant communication is necessary over the internet to perform certain activities because of business demands, Instant messenger shall be made available.

1.3.2 By default access to the following shall be denied

i. Access to download executable files.

ii. Access to sites related to sports, finance, news and HR (jobs).

iii. Users with internet access shall not use company's facilities to download entertainment software or games, or play games over the internet.

iv. Images or videos unless there is an explicit business-related use for the material. Or display any kind of sexually explicit image or document on any system. In addition, sexually explicit material shall not be accessed, attempted to be accessed, archived, stored, distributed, edited, or recorded using University network or computing resources.

v. Freeware / shareware / unlicensed software or tools without prior consent from authorized personnel.

vi. Users with internet access shall not upload any software which is a property of the university, data owned or licensed by the university and documents classified as Proprietary, Confidential or Internal Use, without explicit authorization.

vii. Users shall not carry out any objectionable, frivolous or illegal activity on the internet that shall damage the university's business or its image.

viii. Users shall not attempt to circumvent or subvert security measures on either the network resources or any other system connected to or accessible through internet.

ix. Users shall not post to public discussion groups, chat rooms or other public forums representing the institution on the Internet unless preauthorized by the competent authority.

x. Users shall not send on internet, any information the disclosure of which may in any case cause harm or loss to either the university's or its customers' reputation.

xi. All proxies shall be configured as per the web filter policy defined and implemented from time to time. (a specimen is attached at appendix-II)

1.4 Taking down information published on the internet in accordance with Terrorism laws

1.4.1 UW takes all breaches of the IT Policy very seriously but this issue is exceptional because the University is expected to act immediately upon receiving the notice from the Police/Court.

1.4.2 Sections 6, 8 and 11A of the Anti-Terrorism Act (ATA) 1997 makes it an offence to encourage terrorism and also to distribute information that is deemed to perpetuate terrorism through any media.

1.4.3 Section 11 of the aforementioned Act dictates that any organisation that refuses to remove any information covered by the act without any reasonable excuse will be seen as endorsing the materials and information and so leaves itself liable to prosecution. Section 11 of the Act gives the police the right to serve a notice on the University of Wah as a provider of electronic communications to remove materials that directly or indirectly promote or disseminate terrorism.

1.4.4 UW will comply with notices to take down information that may be deemed as glorifying terrorism in response to a request by the police/court under a Section 11 notice.

1.4.5 Notices under Section 11 of the Terrorism Act should normally be given in writing or email to Vice Chancellor and/or Registrar identifying the materials to be removed. UW will deal with Section 11 notices issued by the police by using the IT Policy as it would with other IT violations.

1.4.6 If asked by the police to retain the information for prosecution, the IT Department will preserve a snapshot of the website and the backup discs in conformity with the stipulations of the Pakistan Telecommunication (Re-organization) Act 1996 which covers the interception of communication.

1.4.7 UW will deal with any request to remove materials that that may be deemed as glorifying terrorism or which directly or indirectly promote or disseminate terrorism by invoking the IT Policy. IT Department will investigate and respond to such a request under IT Policy as it would with other IT violations.

Users Responsibilities

2. Users Responsibility

The user is any person who has been authorized to read, enter, or update information. The IT policy is based on the following principles:

a) Information Technology is a tool to accomplish and support the essential mission of the university and the use of resources must be oriented towards that objective.

b) Users are expected to use information resources with courtesy, respect, and integrity.

c) The infrastructure developed for the Information resources is designed for the entire University and its associated institutions. It follows the product life cycle like any other product and needs to be replaced. It is therefore not too much to expect responsible behavior from users.

d) Simply because an action is easy to do technically does not mean it is legal or even appropriate

2.1 Users are expected to observe the following guidelines:

i. Do not allow unauthorized access of your computer or associated accessories assigned for your exclusive use.

ii. Safeguard your password and do not share it with anyone. Remember that an insecure account may provide an access point for the entire computer system.

iii. University encourages every user to use electronic communication for university related activities such as submission of assignments, conducting exams, submitting projects , conducting research , making announcements the list could be exhaustive. People who use university communication services (such as e-mail) are expected to use them in an ethical and responsible manner, following general guidelines based on common sense, common decency, and civility applied to the networked computing environment. It is based upon a respect for individuals as well as a desire to learn from others.

2.1.1 Users are required:

i. NEVER TO GIVE YOUR PASSWORD TO ANYONE ELSE.

ii. Not to give others access to university information resources unless they are authorized and authenticated to do so.

iii. Not to promote any commercial activity using university information resources.

iv. Never to use any university-provided information resource to do something illegal, threatening, or deliberately destructive—not even as a joke.

v. Never deliberately install any unauthorized or malicious software on any system.

vi. You cannot be exempted from the law because you are "just a student," "you were conducting research," or you were "just playing around."

vii. Not to send rude or harassing correspondence.

viii. Not to communicate with anyone without his or her accord.

2.1.2 Users are forbidden:

i. Spamming the network.

ii. Misuse of peer-to-peer applications.

iii. Falsifying your identity or enable others to falsify identity using university information resources. This type of forgery can result in serious criminal penalties and disciplinary action.

iv. Infringe upon someone else's copyright.

v. Trying to circumvent login procedures on any computer system or otherwise attempt to gain access where you are not allowed. Never deliberately scan or probe any information resource without prior authorization. Such activities are not acceptable under any circumstances and can result in serious consequences,

vi. Disclosing data that is otherwise confidential or restricted, without appropriate authorization.

2.1.3 Password Control Standards

Users are responsible for complying with the following password standards:

i. Passwords must never be shared with another person, unless the person is a designated security manager.

ii. Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed)

iii. Passwords must, where possible, have a minimum length of six characters.

iv. Passwords must never be saved when prompted by any application.

v. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.

vi. When creating a password, it is important not to use words that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc.). Combinations of alpha and numeric characters are more difficult to guess.

2.2 Disciplinary Actions

Punishment for violations includes, but is not limited to:

i. Verbal warnings

ii. Revocation of access privileges

iii. Disciplinary probation

iv. Suspension from the university

v. Criminal prosecution.

2.3 Reporting Security Incidents

All users of IT facilities at UW are encouraged to note and report any observed or suspected security incidents, security weaknesses in or threats to systems and services. Such incidents should be reported to the IT Department.

All external complaints against UW must be reported via email addresses shown below. All reports of unsolicited emails including spam should be reported to the IT Department or via email.

	University of Wah	**Wah Engineering College**
Telephone	+92 (0)51 9055 22255-56	+92 (0)51 931 4419-20
Email	info@wecuw.edu.pk	info@wecuw.edu.pk
Website	http://www.uow.edu.pk	http://www.wecuw.edu.pk

Network Policy

3. Network Policy

Monitoring a network is a very delicate affair. It necessitates the constitution of dedicated staff with authentication from the Vice-chancellor to perform and generate reports on all aspect of network security. Authorized personnel must demonstrate a need for and an understanding of the operation of network monitoring devices.

a) Authorized staff shall use network monitoring devices only to detect:

  i. known patterns of attack or compromise;

  ii. the improper release of confidential employee or student data;

  iii. or to troubleshoot and analyze network-based problems.

b) Authorized staff may also analyze certain network-based anomalies to determine the security risk to the university and conduct statistical/operational studies. All monitoring shall be as narrow in scope as possible.

c) Authorized staff may not exceed specified scope of monitoring (for example, users, address ranges, protocols, signatures).

d) Personnel authorized to analyze network traffic shall not disclose any information realized in the process without approval of the respective Vice Chancellor.

e) No authorized personnel shall use network monitoring devices to monitor employee electronic transmissions for job performance evaluation, or as part of an unofficial investigation, without first receiving signed approval from the Office of the Vice Chancellor for Employee.

f) All monitoring points will be architected, approved, and configured Networking Manager. Responsible staff shall maintain written records of all monitoring points, architectures, and agreements.

g) Monitoring data stores and logs may not be accessible from the public Internet. All personnel must show due care in protection, handling, and storage of all monitored data and logs.

h) Misuse or destruction of information technology resources can vary in severity and appropriate disciplinary actions should be taken in proportion to the severity of the incident. It is not the role of Information Technology professionals to carry out disciplinary actions as the result of an incident, but it is their role to monitor resources, to identify potential incidents and to bring such incidents to the attention of the competent authority.

i) Issues of departmental non-compliance may be reported to the respective executive management.

3.1 Server Related Policy

Any and all servers providing services to one or more users, and hosted on a Microsoft Windows platform, and variations of Linux, Unix and platforms. Servers can be defined, in terms of risk assessment, into three categories, such as:

- Critical servers, including servers hosting data of corporate sensitivity, including web services, financial, student or staff information.
- User account services or servers hosting user accounts and passwords.
- Non-Core Research and Teaching Servers used for research and teaching activities.

For all servers connected to the University network, the following minimum server standards and procedures are suggested.

- Access requirements and function of server are to be documented (to ensure firewall rules and IP address allocation can be used to best protect device).
- The physical location of server is confirmed to be sufficient (power, air-conditioning, physical security of device, WHS requirements).
- Specific technical staff is nominated with sufficient technical skills in server management to ensure that the server can be supported post-production. This may or may not include third party support arrangements.
- The appointed technical staff member must have an appropriate level of server training and experience in supporting the server platform.
- Entry to server room should be restricted to authorized personals only. Log of all entries is the kept.

Technology Standards

4. Technology Standards

All involved systems and information are assets of the University and are expected to be protected from misuse, unauthorized manipulation, and destruction. These protection measures may be physical and/or software based.

a. Ownership of Software

All computer software developed by the University employees or contract personnel on behalf of the University or licensed for University use is the property of the University and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

b. Installed Software

All software packages that reside on computers and networks within the University must comply with applicable licensing agreements and restrictions and must comply with the University acquisition of software policies.

c. Virus Protection

Virus checking systems approved by the IT Manager and Information Services must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus checking systems.

d. Access Controls

Physical and electronic access to Confidential and Internal information and computing resources is controlled. To ensure appropriate levels of access by internal workers, a variety of security measures will be instituted as recommended by the Information Technology manager and approved by the University Mechanisms to control access to Confidential and Internal information include (but are not limited to) the following methods:

4.1 Authorization

Access will be granted on a “need to know” basis and must be authorized by the immediate supervisor and application owner with the assistance of the IT manager. Any of the following methods are acceptable for providing access under this policy:

4.1.1 Context-based access

Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external” factors might include time of day, location of the user, strength of user authentication, etc.

4.1.2 Role-based access

An alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

4.1.3 User-based access

A security mechanism used to grant users of a system access based upon the identity of the user.

4.2 Identification/Authentication

Unique user identification (user id) and authentication is required for all systems that maintain or access Confidential and/or Internal Information. Users will be held accountable for all actions performed on the system with their user id.

4.2.1 At least one of the following authentication methods must be implemented:

i. strictly controlled passwords.

ii. biometric identification, and/or

iii. Tokens in conjunction with a PIN.

4.2.2 The user must secure his/her authentication control (e.g. password, token) such that it is known only to that user and possibly a designated security manager.

4.2.3 An automatic timeout re-authentication must be required after a certain period of no activity (maximum 15 minutes).

4.2.4 The user must log off or secure the system when leaving it.

4.3 Data Integrity

The University must be able to provide validation that Confidential, and Internal Information has not been altered or destroyed in an unauthorized manner. Listed below are some methods that support data integrity:

i. transaction audit

ii. disk redundancy (RAID)

iii. ECC (Error Correcting Memory)

iv. checksums (file integrity)

v. encryption of data in storage

vi. digital signatures

4.4 Transmission Security

Technical security mechanisms must be put in place to guard against unauthorized access to data that is transmitted over a communications network, including wireless networks. The following features must be implemented:

i. integrity controls and

ii. encryption, where deemed appropriate

4.5 Remote Access

Access into the University network from outside will be granted using the University approved devices and pathways on an individual user and application basis. All other network access options are strictly prohibited. Further Confidential and/or Internal Information that is stored or accessed remotely must maintain the same level of protections as information stored and accessed within the University network.

4.6 Physical Access

Access to areas in which information processing is carried out must be restricted to only appropriately authorized individuals.

The following physical controls must be in place:

i. The main computer systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.

ii. File servers containing Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.

iii. Workstations or personal computers (PC) must be secured against use by unauthorized individuals. Local procedures and standards must be developed on secure and appropriate workstation use and physical safeguards which must include procedures that will:

a. Position workstations to minimize unauthorized viewing of protected sensitive information.

b. Grant workstation access only to those who need it in order to perform their job function.

c. Establish workstation location criteria to eliminate or minimize the possibility of unauthorized access to protected examination related information.

d. Employ physical safeguards as determined by risk analysis, such as locating workstations in controlled access areas or installing covers or enclosures to preclude passerby access to critical data

e. Use automatic screen savers with passwords to protect unattended machines.

4.7

Facility access controls must be implemented to limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed. Local policies and procedures must be developed to address the following facility access control requirements:

i. Contingency Operations – Documented procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

ii. Facility Security Plan – Documented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

iii. Access Control and Validation – Documented procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

iv. Maintenance records – Documented policies and procedures to document repairs and modifications to the physical components of the facility which are related to security (for example, hardware, walls, doors, and locks).

4.8 Software and Hardware auditing

i. UW has an obligation to ensure that only legal software is used on UW owned equipment and to support this, appropriate technology may be used to audit UW owned software on UW owned equipment without staff permission.

ii. Note that this will not include privately owned software.

iii. The HoD, Dean, Vice Chancellor, Registrar and/or IT Manager may be notified of any illegal software discovered as part of the audit process.

4.9 Removal of Equipment

iv. No equipment or other electronic communication facility may be borrowed, removed or moved from a designated location, without the explicit permission of Vice Chancellor, Dean, Registrar or IT Manager or their representative, as appropriate.

v. No equipment other than equipment designed to be portable and used outside the University can be taken out of the UW premises without the explicit permission of Vice Chancellor, Dean, Registrar or IT Manager or their representative, as appropriate. For permission to be granted, the necessary forms detailing the purpose of the removal of the equipment and the equipment details must be filled by the applicant and countersigned by the appropriate HoD or owner as mentioned above.

4.10 Emergency Access

i. Each entity is required to establish a mechanism to provide emergency access to systems and applications in the event that the assigned manager or owner is unavailable during an emergency.

ii. Procedures must be documented to address:

a. Authorization,

b. Implementation, and

c. Revocation

4.11 Equipment and Media Controls

The disposal of information must ensure the continued protection of Confidential and Internal Information. Each entity must develop and implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain data into and out of a facility, and the movement of these items within the facility. The following specification must be addressed:

1. **Information Disposal / Media Re-Use of:**

   i. Hard copy (paper and microfilm/fiche)

   ii. Magnetic media (floppy disks, hard drives, zip disks, etc.) and

   iii. CD ROM Disks

2. **Accountability:**

   Each entity must maintain a record of the movements of hardware and electronic media and any person responsible therefore.

3. **Data backup and Storage:**

   When needed, create a retrievable, exact copy of electronic record before movement of equipment.

4.12 Other Media Controls

1. Examinations and Confidential Information stored on external media (diskettes, CD-ROMs, portable storage, memory sticks, etc.) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as **exam** or Confidential Information. Further, external media containing Exam and Confidential Information must never be left unattended in unsecured areas.

2. Sensitive and Confidential Information must never be stored on mobile computing devices (laptops, personal digital assistants (PDA), smart phones, tablet PC's, etc.) unless the devices have the following minimum security requirements implemented:

   i. Power-on passwords

ii. Auto logoff or screen saver with password

iii. Encryption of stored data or other acceptable safeguards approved by Information Security Officer

Further, mobile computing devices must never be left unattended in unsecured areas.

3. If Confidential Information is stored on external medium or mobile computing devices and there is a breach of confidentiality as a result, then the owner of the medium/device will be held personally accountable and is subject to the terms and conditions of university Information Security Policies and Confidentiality Statement signed as a condition of employment or affiliation with the University.

4.13 Data Transfer/Printing

1. Electronic Mass Data Transfers: Downloading and uploading Confidential, and Internal Information between systems must be strictly controlled. Requests for mass download of, or individual requests for, information for research purposes that include admission , financial statistics be approved by the competent authority

2. Other Electronic Data Transfers and Printing: Confidential and Internal Information must be stored in a manner inaccessible to unauthorized individuals. Confidential information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

4.14 Loss and Damage

4.14.1 Save as set out below, UW (including its faculty, officers, staff and employees) accepts no liability to users (whether in contract, tort (including negligence), breach of statutory duty, restitution or otherwise) for:

i. Any loss or damage incurred by a user as a result of personal use of UW IT facilities. Users should not rely on personal use of UW electronic communications facilities for communications that might be sensitive with regard to timing, financial effect, privacy or confidentiality.

ii. The malfunctioning of any IT facility, or for the loss of any data or software, or the failure of any security or privacy mechanism, whether caused by any defect in the resources of UW or by any act or neglect of UW (including its faculty, officers, staff and employees) or howsoever otherwise.

iii. For the acts or omissions of other providers of telecommunications services or for faults in or failures of their networks and equipment;

iv. For any injury, death, damage, or direct, indirect or consequential loss (all three of which terms include, without limitation, pure economic loss, loss of profits, loss of business, loss of data, loss of opportunity, depletion of goodwill and like loss) howsoever caused arising out of or in connection with the use of the UW's IT facilities.

4.14.2 UW does not exclude its liability under this Policy (if any) to users:

i. For personal injury or death resulting from UW's negligence;

ii. For any matter which it would be illegal for UW to exclude or to attempt to exclude its liability;

iii. For fraudulent misrepresentation.

4.14.3 Users agree not to cause any form of damage to UW's IT facilities, or to any accommodation associated with them. Should such damage arise UW shall be entitled to recover from such user, by way of indemnity, any and all losses, costs, damages and/or expenses that UW incurs or suffers as a result of such damage.

4.15 Contingency Plan

Controls must ensure that the University can recover from any damage to computer equipment or files within a reasonable period of time. Each entity is required to develop and maintain a plan for responding to a system emergency or other occurrence (for example, fire, vandalism, system failure and natural disaster) that damages systems that contain Confidential, or Internal Information. This will include developing policies and procedures to address the following:

4.15.1 Data Backup Plan

i. A data backup plan must be documented and routinely updated to create and maintain, for a specific period of time, retrievable exact copies of information.

ii. Backup data must be stored in an off-site location and protected from physical damage.

iii. Backup data must be provided the same level of protection as the original data.

4.15.2 Information Retention

i. Information shall not be retained any longer than the business requires it to be retained. This reduces the window of time that data can potentially be available for misuse. Controls should be implemented to delete data that exceeds required retention time.

ii. Electronic member data shall be retained for up to five (5) years.

Portable IT Equipment Policy

5. Portable IT Equipment Policy

5.1 The Policy

This policy is to ensure the proper control of the use and issue of Laptop, OHPs, Multimedia Projectors and other Portable IT Equipment (i.e., Cameras, Presenters and related accessories etc.) in the most efficient, secure and cost effective manner. Security and confidentiality matters are also addressed.

5.2 Criteria for Issue

5.2.1 Faculty/Staff who have a need to use a computer, or access computer data whilst away from the office will be considered for the issue of a Laptop, PC or other Portable IT Equipment.

The faculty/staff should note that mobile devices have a higher life-cycle cost of ownership. They are inherently expensive to buy, have limited upgradeability, and are less robust than desktops. They are also more vulnerable to theft and damage. Additionally they may contain sensitive information.

5.2.2 HODs will need to take account of these issues in deciding whether to support the issue of portable equipment to their faculty/staff. HODs are reminded that it is their duty to ensure that their staff comply with university policies.

5.2.3 Users will be required sign the document at Annex A, accepting responsibility for the portable IT equipment and any additional equipment handed over at the time.

5.2.4 Data security is the responsibility of all faculty/staff as individuals, and failure to observe appropriate security measures and policies will be treated as Gross Misconduct/Gross Professional Misconduct.

5.2.5 The equipment reserved by any member of staff or faculty can be issued to their student representative on their behalf.

5.3 Equipment Available

A range of portable equipment is available for use by faculty/staff/students at the university. This includes laptops, audio-visual aids such as OHPs, multimedia projectors, and other small items.

5.3.1 Laptops and Multimedia PCs

These are standard laptops & PCs, installed with Microsoft Windows 7 Starter and Microsoft Office 2010. They are internet ready and can be plugged into any University Network socket for immediate connection (if required). Video output sockets can be used to connect the laptop to any fixed or portable data projectors and screens for a larger image. The laptops and all associated power supplies, cables, etc., are supplied in a soft carry case.

5.3.2 Multimedia Projectors/OHPs/Projection Screen

Multimedia Projectors are suitable for projecting images from a computer, DVD player, or other VGA/composite video source. They are easy to operate, and are supplied with remote controls and cables in a carry case. OHPs are suitable for displaying transparencies. If you are not familiar with connecting and using these projectors then we recommend that you include 30 minutes in your reservation time to read through the instructions and set the equipment up.

5.3.3 Wireless Presenters

A wireless 'presenter' (remote control for advancing through slides) and wireless keyboard/mouse are also available.

5.3.4 Photography Equipment

A basic digital camera, camcorder, tripod and memory to store several hundred full-resolution images. The photography equipment is supplied with the cables for connecting to a computer via USB.

5.4 Making a Reservation

5.4.1 The equipment can be reserved by any faculty member, or member of staff, for bona fide university purposes (academic or business). Reservations can be made by contacting the IT Department. The equipment will be available from the IT Department’s Office, and should be returned to the same office by the end of the reservation period to ensure that the equipment is ready for other users.

5.4.2 The reserved equipment can be delivered/installed at any required location within university premises. In such cases IT Department should be informed well before time for necessary arrangements. The closing time of an event must also be notified for removal of equipment.

5.4.3 All of this equipment is serviced once a term to ensure that everything is present and in working order. With any important event it is still a good idea to run a full test beforehand, to ensure that a previous user has left the equipment in good condition and that the user requesting the equipment is familiar with its use.

5.4.4 If there are any items of equipment that a staff or faculty find particularly useful, but which are not currently available, then please let the IT team know so that we can factor this into our future provisioning.

5.5 Security Issues Particularly Pertinent to Portable Equipment

Laptops and other Portable IT Equipment are particularly vulnerable to both opportunist and planned theft. This may entail inconvenience, cost of replacement, and breach of confidentiality. Where loss has occurred due to negligence on behalf of the user this will be addressed in accordance with the University of Wah Disciplinary Policy.

5.6 Data Security

5.6.1 All laptops and PCs will be issued with software to encrypt all data held on the hard drive.

5.6.2 Until the individual’s laptop, PC or PDA is encrypted with encryption software, users must not copy any PID (Personally Identifiable Data) or confidential data onto the laptop. This includes data held in offline folders created as a result of:

i. Synchronisation of any network drives

ii. Synchronisation of any Microsoft Outlook, the standard folder structure within Microsoft Outlook and Personal Folders linked to Microsoft Outlook.

Additionally, all confidential information should be kept in password protected files. Both Microsoft Word and Excel can be set up to require a password to open them.

5.7 Physical Security

5.7.1 Users are required to take every reasonable precaution for the physical security of issued laptops, PCs and other portable IT equipment.

5.7.2 If the device is to be left in the user's normal workplace, it should be placed in a secure cupboard or drawer when not in use.

5.7.3 At all other times when it is in the user's custody, apart from when it is actually in use, it should be kept switched off, and as securely as possible.

5.7.4 Ideally equipment should not be left in cars, but when unavoidable it should be secured out of sight in the boot preferably before starting the journey.

[All equipment will be security etched with University's Address, Contact Numbers and Inventory Number.]

5.8 Insurance

Laptops, PCs and Portable IT Equipment are not covered by any insurance. If loss of the equipment is found to be due to negligence then the person accepting the equipment might be held liable for the cost of a replacement. Users may wish to consider insurance to cover the equipment whilst in their care.

Email Policy

6. Email Policy

6.1 The University of Wah provides electronic mail services (“email”) to support the teaching, learning, research and administrative mission of the University and which is maintained by the IT Department for use by staff, students, faculty, alumni and associates affiliated with University.

6.2 Email is a critical means of communication at University and many official communications are transmitted between staff and students.

6.3 This policy applies to users (academic, professional support staff, faculty, students and others extended access privileges) and has been established to provide guidelines for the acceptable use of the email service.

6.4 **Staff Email:** All official University of Wah email communication to UW staff will be delivered to their official UW account and should not be automatically forwarded to any other email accounts.

6.5 The University of Wah in collaboration with Google, has introduced Google Apps for Education, a service that allows institutions and individuals to use Google's communication and collaboration applications under their own domain names. These services are hosted by Google offsite and provide a convenient solution to store or share information which is accessible from any computer device connected anywhere to the Internet. Any use of Google Mail by staff is governed by this UW Email Policy.

6.6 Staff have also been given Google accounts by default which allows them to use Google Mail as well all the applications in the Google environment.

6.7 Email is not a secure method of communication and staff should not send or forward confidential, personal or sensitive business information to non UW email accounts or through the UW Google email service.

6.8 Information Services do not backup any emails stored in the Google environment so users are individually responsible for keeping backups of any stored in the Google environment.

6.9 All email communication from staff should display the following disclaimer.

“This e-mail and its attachments are intended for the above named only and may be confidential. If they have come to you in error you must not copy or show them to anyone, nor should you take any action based on them, other than to notify the error by replying to the sender”.

6.10 **Confidentiality:** Communication between staff is considered a business record and some emails may have attachments that may contain confidential and personal information. UW has a duty of care to prevent the leakage of confidential data from its systems. In addition to that, restrictions may also be applied to certain research projects that may forbid the storage of research data on non-UW owned systems. Any such data that is deemed confidential should not be shared in the Google environment and should only be shared on UW owned systems and with authorized staff.

6.11 **Student Email:** Undergraduate and Postgraduate students have been given Google accounts on their individual requests which allows them to use the authorized applications in the Google environment. Any use of Google Mail is governed by this UW Email Policy.

6.12 Users of the UW IT facilities shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of UW or any department of UW unless appropriately authorized (explicitly or implicitly) to do so. While it is permissible to indicate one's affiliation with UW, unless it is clear from the context that the author is not representing UW, an explicit disclaimer must be included. An appropriate disclaimer may take the form:

"These statements are my own, not those of the University of Wah".

6.13 Users of the UW IT facilities must not send email on behalf of another person, or impersonate another user when sending email, except when authorized by that person to do so.

6.14 Users of the UW IT facilities may only send mass communications in support of the UW's business and in accordance with policies on sending bulk messages and guidance from the Registrar.

6.15 In general, UW cannot and does not wish to be the arbiter of the contents of electronic communications. Neither can UW, in general, protect users from receiving electronic communications they might find offensive.

6.16 Users of the UW IT facilities are strongly encouraged to use the same personal and professional courtesies and considerations in emails as they would in other forms of communication.

6.17 The email service must not be used to send emails that are intimidating or harassing. Disciplinary action will be taken against any user who sends threatening, intimidating or threatening emails.

6.18 The email service must not be used to inappropriately distribute works protected by Intellectual Property Rights belonging to others.

Google Collaborative Applications

7. Google Collaborative Applications

7.1 Introduction

7.1.1 The University of Wah in collaboration with Google, has introduced Google Apps for Education, a service that allows institutions and individuals to use Google's communication and collaboration applications under their own domain names. These services are hosted by Google offsite and provide a convenient solution to store or share information which is accessible from any computer device connected anywhere to the Internet.

7.1.2 The Google Apps package includes the following services and is available for students and faculty. Administrative Staff have also been given Google accounts by default which allows them to use all the applications in the Google environment:

- **Gmail** – email including instant messaging; any use of Google Mail, whether by faculty, staff or students, is governed by the UW Email Policy.

- **Google Calendar** – an online calendar & time-management application;

- **Google Sites** – Create, share and publish websites, Google Sites is a structured wiki- and web page-creation tool offered by Google as part of the Google Apps Productivity suite. The goal of Google Sites is for anyone to be able to create a team-oriented site where multiple people can collaborate and share files.

- **Google Talk/Hangouts** – allows users make PC-to-PC free voice calls, send instant messages and share files;

- **Google Docs/Google Drive** – allows users to create exchange and collaborate on documents with different users within the University.

- **Google Mobile** – Google Sync for Mobile, Google Apps Mobile Management lets administrators enforce device policies over their mobile fleet using their Google Admin console, without the need for an on premise device management server.

7.1.3 The access summary for all major Google apps services by different users is as follows,

Service	Students	Faculty	Admin Staff
Gmail	✓	✓	✓
Google Calendar	**x**	✓	✓
Google Sites	**O**	✓	✓
Google Talk/Hangouts	✓	✓	✓
Google Docs/Google Drive	**O**	✓	✓
Google Mobile	**X**	**X**	**X**

✓ = Full Access **X** = No Access **O** = Restricted Access

7.2 Purpose

7.2.1 This policy is to establish the appropriate use of Google Apps to protect UW business records and to limit the exposure of the University to data and IPR risks by specifying the appropriate conditions under which the Google service may be used. Use of Google Mail, whether by faculty, staff or students, is governed by the UW Email Policy.

7.3 Policy

Google provides the Google Apps service on behalf of UW and users are expected to adhere to the UW IT Policy such that the same standards of behaviour and adherence are expected in the use of the Google Apps as in the use of all UW systems.

7.3.1 Ownership/Intellectual Property Rights (IPR): Users must only collaborate on documents to which they own the intellectual property rights or where they have the expressed permission for the contemplated use from the intellectual property owner.

7.3.2 Confidentiality: Communication between staff is considered a business record and some emails may have attachments that may contain confidential and personal information. UW has a duty of care to prevent the leakage of confidential data from its systems. In addition to that, restrictions may also be applied to certain research projects that may forbid the storage of research data on non-UW owned systems. Any such data that is deemed confidential should not be shared in the Google environment and should only be shared on UW owned systems and with authorized staff.

7.3.3 Every current document on Google Apps must have a named owner and if there are joint collaborators on a document it is the responsibility of the departing owner to transfer the ownership of the document.

7.3.4 Management Information Systems such as WECMIS and other UW IS do not backup any documents or emails stored in the Google environment so users are individually responsible for keeping backups of any documents stored in the Google environment.

7.3.5 Personal and sensitive information: In accordance with the Electronic Data Protection Act 2005, the following information must not be placed in the Google environment when collaborating or working on draft documents, even when collaborating or working with other UW staff:

- Personal information
- Date of birth
- Financial information
- Examination record
- Payment & bank details
- Username & passwords
- Medical records
- Alumni Information
- Any other information that the staff member knows or is expected to know that it is confidential.

Disposal of Old Equipment

8. Disposal of Old Equipment

8.1 Introduction

8.1.1 The frequently changing IT environment means that computing equipment (personal computers, laptops and peripherals such as printers) periodically becomes surplus to requirements or reaches the end of its useful life. Computers are usually passed on to other departments (redeployed), sold on to members of staff, given to charity organisations or disposed of.

8.1.2 The University is bound by statutory obligations such as Data Protection Act 2005 to ensure that the data stored on these computers is securely removed prior to disposal. Any University data which is discovered by a later owner may cause University of Wah adverse publicity or controversy.

8.2 Policy

Options for the disposal of IT equipment.

8.2.1 The following order of priority should be applied to computers and other IT related equipment when they become redundant:

- Redeployment to another department within the University.
- Subject to UW Financial Regulations, equipment with a residual value may be offered to members of staff for a nominal fee, after the completion of the **Removal of Equipment Form**.
- Donation to a UW approved charitable organisation, which must guarantee the secure destruction of the data and the environmentally friendly recycling or disposal of the equipment.
- Disposal/recycling.

Note: Procedures for each of these options are detailed below. In all cases asset and inventory records of the serial number(s) must be accurately updated before the equipment is disposed of.

8.3 Removal of data and software

8.3.1 All traces of the data contained on computer equipment must be removed by the IT Department and destroyed prior to their disposal.

8.3.2 Care must be taken to meet the requirements of the Data Protection Act regarding the security of data as well as the Copyright (Amendment) Act 1992 to ensure that software and licensing regulations are not infringed during the disposal process.

8.3.3 Merely deleting the file or reformatting the hard drive does not remove traces of all data or prevent its recovery.

8.3.4 Specialized "disk wiping" utilities should be used to erase to entire contents of the disk. However in cases where the redundant computer was previously an open access lab machine, repartitioning or reformatting the disk will effectively remove the software licenses.

8.4 Procedures

8.4.1 Redeploying a computer to another department

i. Unless the recipient has a business requirement for the transfer of some of the data, IT Department must remove all the data from the computer.

ii. The Vice Chancellor, Registrar, Dean, HoD or their representative must give their explicit authorization before the data is transferred.

iii. If the information held on the computer relates to personal information as defined by the Data Protection Act 2005 (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life and criminal convictions), the disk should be erased with a secure disk wiping utility.

iv. Software or licenses must only be retained or transferred to a new owner if UW holds a license and where there is a business requirement to transfer the license.

8.4.2 Offering equipment to member of staff

i. All data and software must be removed using a secure disk wiping utility.

ii. To comply with licences and copyright laws, IT Department must ensure that all software is removed properly.

iii. If the computer is to be used for personal purposes, the user would be offered the opportunity to purchase their own software license(s).

8.4.3 Donating to an outside body

i. Donating redundant computer equipment should only be considered when it has been agreed by IT Department to be redundant in relation to University requirements.

ii. All software and data must be securely removed using a secure disk wiping utility.

iii. UW licensed software must not be transferred to a third-party.

iv. The recipients of the computer equipment must be made aware that University of Wah cannot guarantee the safety or suitability of the equipment and resigns all responsibility for its maintenance.

v. Records should be kept of computer equipment donated to third parties, as evidence that University of Wah is committed to increasing the rate of recycling of all appropriate materials.

8.4.4 Disposal in an environmentally-friendly manner.

i. Older computer monitors are defined as hazardous waste and proper arrangements for their disposal must be made.

ii. University of Wah aims to minimize the impact of electrical and electronic equipment on the environment both during their life time and when they become waste. It encourages and sets criteria for the collection, treatment, recycling and recovery of waste equipment.

iii. Redundant equipment that cannot be redeployed, sold or donated to charity should be disposed of in an environmentally friendly manner.

Backup Retention and Archive Policy

9. Backup Retention and Archive Policy

9.1 Purpose

The purpose of this policy is to establish the structures that exist around the management of data; backups; retention; destruction and retrieval of data, documents and digital content held on UW infrastructure. It also highlights limitations and exclusions to the retrieval of data. This does not replace the University's records management and related policies and can be considered a practical guide to good data management practices.

9.2 Scope

The audience of this policy includes University users of all University systems and includes academic staff, research staff and other knowledge workers, professional support staff, students and third parties with contractual obligations to the University.

9.3 Policy

9.3.1 System Classifications

IT Department operates a tiered system for University corporate services and where necessary, operate different granularity for backup retention and retrieval:

- **Tier 0** – enabling systems which are necessary for the provision of corporate systems e.g. Microsoft Active Directory, DNS etc.
- **Tier 1** – corporate applications such as Student Record Systems, Finance Systems, Library Management System, Email intranet / Internet.
- **Tier 2** – applications which are not used across the University but which play a crucial role within specific departments.

9.3.2 Infrastructure description:

The IT Department has embraced newer techniques based on data replication and virtual technologies and these include:

- **Data Replication -** the process of copying data from one server to another using inbuilt "on-the-fly" techniques which do not rely on proactive management and monitoring

- **Log Shipping -** the process of automatically copying and restoring a production server's transaction logs to a standby server in the same or separate data centre

- **SANs (Storage Area Network) -** the ability to harness large amounts of space from a confederation of smaller physical drives which provide improvements in speed and greater redundancy

- **Off Site Backups -** the process of making copies of key data to external locations on a daily and weekly basis.

9.3.3 Type of systems

(The IT Department operates different policies for different services based on the complexity of each system)

- **Transactional Systems -** these are systems, which are database driven such as IS (Information System).

  Where the architecture permits, and depending on the degree of criticality, replication, log shipping and virtualisation techniques are deployed as the primary method for data availability and resilience. Rigorous off-site backup and restore procedures are also used but are not the primary method for data recovery. Most Tier 1 systems rely on these types of backups.

- **File Storage**

  This covers those systems which rely on storing digital content on file stores such as Microsoft AD (home areas and various shares), NTFS file storage and card system security images. Rigorous on- and off-site backup and restore procedures are used as the primary method for data recovery. These mostly apply to Tier 2 applications.

- **Externally managed and hosted systems**

  The University has contractual agreements with a number of third parties to manage a number of its corporate systems. Where such an arrangement exists, the third party supplier is responsible for ensuring that regular backups of the systems are maintained in line with the University Backup, Retention and Archive Policy

- **Systems**

  Systems are the databases, web and application servers which configuration data only. The backing up of such configuration files is necessary for the total restoration of the system in the event of major failure.

9.4 Frequency and Timing of Backups

- A full backup of transactional systems is automatically taken every day.
- A full backup of file storage systems is automatically taken every day.
- Externally managed systems should be backed up daily.
- System backups are taken daily, however separate backup routines may exist for certain systems.

9.5 Verification

The backup logs are checked daily by the IT Department and the system administrator of each service is informed in the event of a backup failure. Persistent backup failures are noted and investigated immediately.

9.6 Roles and Responsibilities:

Roles	Responsibilities
Design and execution of the log shipping, replication and virtualization	The responsibility resides with Systems manager with escalation to the IT Manager.
Data integrity for restores (quality assurance)	The responsibility for date verification for restores resides with manager responsible for the system(s) including the IT Manager.
Locally held data	The responsibility for the backups for data held on local hardware, flash drives, Google Apps resides with the user.
Hosted system	The responsibility for the data backups resides with the data owner within the University.
Managed Service	The responsibility for data backups is as defined in the Service Contract. The primary contact is the business owner with escalation to the Systems Manager and Applications Manager.

9.7 Service Backup Levels

Service	Tier	Freq	Freq	Backup Type	Backup Retention
Infrastructure	0			Data Configuration	Log files for > 3 months As File Systems (below)
Web	1	Daily	Daily	Data	Up to 3 Months
Applications (General)	1	Daily Yearly	Daily Yearly	Data Data	Up to 3 Months Up to 3 Years
Applications (Finance)	1	Daily Yearly	Daily Yearly	Data Data	Up to 3 Months Up to 7 years
File Systems	1	Daily	Daily	Data	All active files - last 3 versions Deleted files - final version for 2 years
Web	2	Daily	Daily	Data	Up to 1 Months
Applications	2	Daily		Data	Up to 1 Months
Workstations and removable storage (PCs, Flash Drives)	3	Never		None	Never

Disaster Recovery Plan

10. Disaster Recovery Plan

A disaster recovery plan must be developed and documented which contains a process enabling the entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.

10.1 Emergency Mode Operation Plan

A plan must be developed and documented which contains a process enabling the entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.

10.2 Testing and Revision Procedures

Procedures should be developed and documented requiring periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary.

10.3 Applications and Data Analysis

The criticality of specific applications and data in support of other contingency plan components must be assessed and documented.

Appendixes

Appendix A: External Acts

The use of computer and network resources at UW is subject without limitation to the following Statutes and Regulations.

- Anti-Terrorism Act (ATA) 1997
- Data Protection Act 2005
- Copyright (Amendment) Act 1992
- Pakistan Telecommunication (Re-organization) Act 1996
- Pakistan Nuclear Regulatory Authority Ordinance 2001
- Fair Trial Bill 2012 (Proposed)
- Official Secrets Act 1923
- Prevention of Anti-National Activities 1974
- Security of Pakistan Act 1952
- Prohibition of Private Armies Act 1974
- National Command Authority Act 2010
- ePrivacy Regulations 2011
- ePrivacy Directive 2002
- Foreign Data Security and Protection Act 2004