UNIVERSITY OF WEST LONDON
Connected.

INFORMATION SECURITY POLICY

"Information, whether financial or about people and systems, is the lifeblood of any organization." GCHQ, 2012

Foreword to the Information Security Policy

The University of West London (UWL) has an ethical, legal and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity and availability. In other words, the information UWL is responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it. This information security policy sets out its approach to information security management.

In today's highly connected, highly electronic world, information is generated and used everywhere from the point at which a prospective student first makes contact with UWL and the right the way through the student journey to alumni. Data can underpin research and intellectual property. It also supports the management of the institution. Sharing data is easier than it ever has been and more and more people chose to access systems (and therefore data) through personal devices.

UWL considers information to be a strategic asset that is essential to its core mission and objectives. It has a responsibility to manage effectively the risks around protecting the confidentiality, integrity and availability of its data and in complying with all statutory, regulatory and legal requirements.

The Information Security Policy set out bellow is an important milestone in the journey towards effective and efficient information security management. It sets out the responsibilities we have as an institution, as managers and as individuals. It has, therefore, my full support and I expect all UWL staff, students and anyone else who has access to UWL information to read it and abide by it.

Professor Peter John
Vice Chancellor & Chief Executive
University of West London
December 2014

1. DOCUMENT CONTROL

Document owner	Flavius Plesu Information Security Manager
Prepared by	Flavius Plesu Information Security Manager
Reviewed by	Adrian Ellison Director of IT Services
Approved by	Peter John Vice Chancellor
Approved on	16th of December 2014
Revision date	4th of December 2017
Reference	POL_ITS_001: Information Security Policy
Version	1.0
Classification	Public

Distribution list	
VCE	To approve and authorise
ISG	To review and update
All Department / Function / School Heads	To understand and comply

Communication	The Information Security Policy is communicated to all members of staff, students and third parties via email, UWL intranet, UWL website, HR handbook, student handbook and information security awareness training.

2. TABLE OF CONTENTS

3. INTRODUCTION

The University of West London (UWL) has an ethical, legal and professional duty to ensure the information it holds conforms to the principles of confidentiality, integrity and availability. In other words, the information UWL is responsible for is safeguarded where necessary against inappropriate disclosure, is accurate, timely and attributable, and is available to those who should be able to access it.

This information security policy outlines UWL's approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the University's information systems.

Under that umbrella, supporting policies, procedures and guidelines provide further detail on how to implement those information security arrangements.

4. STATEMENT OF INTENT

The main purpose of this policy is to describe the minimum level of protection that UWL expects of all UWL's information systems to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

A secondary but very relevant purpose of this policy is to ensure that all users understand their responsibilities for protecting the confidentiality and integrity of the data that they handle, including making users aware of relevant legislation.

The directives set in this policy were defined in the context of the information security programme, which has the overarching objectives:

- To support the Institutional business objectives in a flexible and effective way
- To maintain adequate regulatory compliance
- To protect UWL's information assets
- To maintain business continuity

The policy of the UWL is to protect information systems from unauthorised access, use, disclosure, destruction, modification, disruption or distribution.

The UWL Senior Management Group will ensure business, legal, regulatory requirements and contractual information security obligations are met.

The information security management system will be monitored regularly with regular reporting of the status and effectiveness at all levels.

This policy is the cornerstone of UWL's on-going commitment to establish and maintain our information security procedures. It has, in consequence, my full support, and I ask all UWL staff, students and anyone else who has access to UWL data and/or systems to read it and abide by it in the course of their work.

5. SCOPE

This policy is applicable, and will be communicated to all staff, students, other members of the UWL and third parties who interact with information held by the UWL and the information systems used to store and process it. This includes, but is not limited to, any systems or data attached to the UWL data or telephone networks, systems managed by UWL, mobile and personal devices used to connect to UWL networks or hold UWL data, data over which UWL holds the intellectual property rights, data over which UWL is the data owner or data custodian, communications sent to or from the UWL.

6. ROLES AND RESPONSIBILITIES

6.1 RESPONSIBILITIES OF EVERY USER OF UWL IT RESOURCES, INCLUDING THIRD PARTY SERVICE PROVIDERS

6.1.1 Appropriate use of IT resources

Staff, Students and -in general- users of UWL IT resources are expected to meet the acceptable usage policies and related terms and conditions of the services provided by UWL and by any third party on our behalf (e.g. Janet, Microsoft software licensing agreements).

The University will provide tools to create and store data, connect to the Internet and other networks. Users must apply these in a legal and appropriate manner, to protect the personal safety of themselves and their peers and to ask the University staff for advice or assistance in case of doubt or concerns. The IT Service Desk should be the first point of contact.

6.1.2 Confidentiality of passwords

Users must manage passwords with care and processes should be in place to ensure confidentiality from the initial creation, storage in applications, communication and day to day usage.

6.2 RESPONSIBILITIES SPECIFIC TO EVERY STAFF MEMBER OF UWL

6.2.1 Appropriate use of IT resources

All employees and third parties using UWL systems are accountable for understanding and following UWL's information security policies, as well as promoting safe practices within their teams and monitor compliance.

6.2.2 Asking for help, reporting a concern

All employees and third parties are responsible for asking for assistance when in doubt about how to proceed or interpret a policy and also to report any concern or suspect activity encountered. Depending on the nature of the concern, the first point of contact should be one of these: the line manager, IT Service Desk, the Information Security Manager or Human Resources.

6.3 RESPONSIBILTIES SPECIFIC TO MANAGERS

6.3.1 Fully understand the data, people, systems and processes that he/she is accountable for its safeguard

UWL managers are expected to identify the data and systems under their remit and accept accountability for its protection. Individual "custodians" (also referred as "owners") of the data will be identified. They will be accountable for it and will make informed decisions on risks and appropriate levels of protection, on behalf of the University.

6.3.2 Strategic support to open networks

UWL managers should not exclusively rely on perimeter controls, but also implement (or fund) security on each individual system. In an open and dynamic organisation such as UWL, having a clear strategy of providing flexible and seamless mobile access, it is no longer effective to rely on broad "Internet vs internal" networks, or physical access to the campus or on user ignorance of our estate or IT tools, to protect UWL from accidental or intentional misuse.

6.3.3 Fund secure systems

UWL managers that sponsor a system to process UWL data are accountable for commissioning one that meets the information security policy, applying deliberate and verifiable risk management. Security measures need to be identified, designed, resourced and delivered from the start of any initiative alongside any other business functionality and maintained for the entire lifecycle of the process or IT system, up to the data and system disposal.

6.3.4 Support services to deliver their services securely and be custodian/gatekeepers of the systems

Central functions such as IT Services, Human Resources, Legal and Finance will support the delivery of security on an "internal service provider" model. These functions will have also the mandate to monitor compliance and where appropriate will have accountability for the custodianship/gatekeeping in maintaining the practices agreed/accepted by Vice-Chancellor's Executive.

6.3.5 Setup resilient business processes, with a combination of controls to avoid single points of failure

UWL managers should ensure that the risks of concentrating functions on a single control ("single point of failure") -whether performed by individuals or systems- are well understood and actively managed. Managers need to choose and implement the combination of preventative and monitoring controls that best meet the business objectives.

6.3.6 Ensure their teams are security savvy

UWL managers should ensure their teams have the necessary skills and should communicate their responsibilities regarding protecting systems and data.

6.3.7 Oversee their teams and systems are effective

UWL managers should actively, regularly and demonstrably verify what their reports are doing and how systems under his/her supervision are functioning (with the assistance of IT where appropriate).

6.3.8 Monitor the third party with access to UWL systems and data

UWL managers should ensure any subcontractor employed for a particular function will meet the requirements specified (on selection and on an ongoing basis) and accept responsibility for their actions.

6.4 RESPONSIBILTIES OF SENIOR MANAGEMENT

6.4.1 Risk ownership

The Vice-chancellor's Executive owns the overall risk management process, and the prioritisation and acceptance of risks. Risks are identified "bottom up" from each department and "top down" from the Vice-Chancellor's Executive in a two-way flow.

6.4.2 Risk Acceptance

Head of Schools, individually or via governing bodies have the accountability for taking a stance on risks within their authority (or escalating if exceeds it) and ensuring the business operates in line with the Vice-Chancellor's Executive expectations.

6.4.3 Risk Treatment

Governance arrangements, such as the Audit & Risk committee of the Board of Governors and the Internal Audit programme, will help to identify risks to the University. The Vice Chancellor's Executive will take advice from these and other sources, including the University's own Risk Register. Ultimately the responsibility for risk lies with the Vice-Chancellor's Executive.

6.5 RESPONSIBILITIES OF THE INFORMATION SECURITY MANAGER

6.5.1 Risk management

Identify threats to the University's information assets and advise the Risk Committee on impact and recommended remediation. Scope includes risks related to information, data, technology & related regulatory requirements.

6.5.2 Policies and education

Communicate acceptable levels of risk and mitigation practices throughout the University via policy, standards and awareness programs. Central initiatives to communicate, facilitate/enable the adoption of secure practices.

6.5.3 Measuring progress and compliance

The information security programme will perform validation of compliance directly on the processes or verifying the management controls.

6.5.4 Incident response

Develop central capabilities to effectively respond to significant information security related incidents.

6.5.5 Service delivery

There may be central services delivered by the Information Security Manager, for example on demand pen testing, or some diagnostics/checks.

6.6 RESPONSIBILITIES SPECIFIC TO THIRD PARTY PROVIDERS

6.6.1 Meeting terms of service/contract agreements, right to audit.

Third party shall adhere to the IT acceptable usage policy as well as any other requirements specified in the service contract.

6.6.2 Security and incident response tests.

Third party working for UWL are expected to participate in incident response tests or drills as any other member of staff, when using UWL resources and/or premises. Specific audit/reviews/checks might be undertaken on external service providers, due to the dynamic nature of such relationships.

7. POLICY

7.1 ORGANIZATION OF INFORMATION SECURITY

7.1.1 Ultimate accountability for security

The Vice-chancellor Executive has the ultimate accountability for implementing information security at UWL.

7.1.2 Information security Programme

An Information security programme shall be established and led by the Information Security Manager. The programme will be funded within IT Services with distinct budget allocation. It will be updated annually, with a 3 year rolling plan.

7.1.3 Information security steering group (ISG)

A steering group with Vice-Chancellor's Executive representation will provide senior management direction. The Steering group will decide on risk prioritisation and acceptance, and approve the programme plan, the security policy set and specific mitigation activities where appropriate.

7.1.4 Information Security Forum

A collaborative team will be established with representation from all support and academic departments to provide cross functional skills and communications, chaired by the Information Security Manager. The information security Forum will provide assistance to the programme team to deliver policy, awareness raising and incident response capabilities.

7.1.5 Information Security Manager

The information Security Manager leads the information security programme and has remit across the University. He/She will support departments to require evidence or perform direct validation of compliance against policy. Specific sign-off requirements by the Information Security Manager may be established in policies or operational procedures.

7.1.6 Contact with special interest groups

Appropriate contacts with industry groups or other specialist security forums and professional associations should be maintained. Leverage of UWL own academic expertise should be sought, where appropriate.

7.1.7 Segregation of duties

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

7.2 POLICY MANAGEMENT, EDUCATION AND AWARENESS

7.2.1 Policies as minimum expectation, need for risk management

Managing risks is an essential part of the business activity at all levels of the organisation. The information security policies are only the minimum expectation to address information security risks according to well established practice. Management should assess the business, legal, contractual and corporate social responsibility risks and requirements in each relevant jurisdiction to decide on the need for additional controls or exceptions, and be able to justify and be accountable for these decisions. The risks management process will follow the UWL risk management policy, and be reviewed formally at least annually.

7.2.2 Policy issuing, communication and updating

A set of policies and procedures for information security will be maintained, approved by management, published and communicated to employees and relevant external parties. These policies should follow the overarching framework for policy approval and review defined at UWL level. In particular, policies should be reviewed and updated at least annually.

7.2.3 Trust, but verify

The policy statements are necessary but not sufficient on its own. There needs to be controls in place to provide comfort that policies are being followed. Furthermore, those controls should not be transactional or preventative only; Managers should perform demonstrable "controls over the controls" at an appropriate level of detail to reasonably conclude they are effective.

7.2.4 Awareness and education on policies and procedures

Managers should ensure staff and external parties working with UWL systems and data are formally aware of and educated on the policies and procedures they must be compliant with. This is a fundamental step to establishing any individual's accountability.

7.3 HUMAN RESOURCE SECURITY

7.3.1 Acceptable use of UWL resources

Every employee and third party granted access to UWL systems and/or data has a responsibility to use the systems and data in a secure manner, for UWL business purposes, following UWL policies and applying good judgment. Only approved hardware, software and data should be used to perform UWL business. The extent and exceptions to this policy, including personal use of UWL resources is defined in the "Acceptable Usage Policy" and the "Student Handbook".

7.3.2 Responsibility for reporting non compliance

Users are responsible for reporting any concern on how the security processes are performing, any suspected or confirmed incident regarding unauthorized or incorrect use to their manager or IT Service Desk or the Information Security Manager or Human Resources.

7.3.3 Management responsibility for security

Management is responsible for requiring their teams of employees and contractors to apply information security according to established policies and procedures, and to monitor use within his/her teams, leading by example and ensuring their direct reports have been educated on policies and security practices.

7.3.4 Background checks on employees

Background verification checks on candidates for employment, employees or contractors, as established by Human Resources, shall consider explicitly the sensitivity of the information to be accessed and the perceived risks when defining the nature and timing of those checks.

7.3.5 Terms and condition of employment and termination or change of responsibilities

The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security including those that remain after termination or change of functions. Detail procedures should be documented and communicated to the employee or contractor, and enforced.

7.3.6 Enforcement of information security policies

The HR department is responsible for defining and communicating the disciplinary process applicable to employees who have committed an information security breach.

7.4 DATA/ASSETS MANAGEMENT

7.4.1 Data classification

Each department manager must identify the data being used for fulfilling their duties and adopt controls to protect the information according to its risk. Assigning ownership and a sensitivity classification is a highly recommended method of protecting assets efficiently. If no formal classification is used, the department should work on the assumption that all information is as critical as the most critical information they possess.

7.4.2 Retention of information

UWL will have processes in place to safely dispose of information as required by law or, within legal compliance, when is no longer cost effective to retain. Based on their remit, Managers, assisted by legal counsel, is responsible for defining the acceptable retention period for the various kinds of data they hold. Managers are also responsible for establishing the controls to ensure these criteria are followed.

7.4.3 Safe storage and disposal of electronic media and surplus hardware

IT services will define a formal procedures in place for the safe acceptance, storage and disposal of surplus technology hardware (including electronic storage media). UWL only accepts new, vendor guaranteed equipment and destroys surplus/failed equipment/media/paper securely, compliant with the law, and (then) in an environmentally friendly way. Other arrangements need to be dealt on a case by case with business and technical signoff.

7.4.4 Safe storage and disposal of paper

Property Services will define a formal procedures in place for the safe storage, retrieval and disposal of paper files.

7.4.5 Logs retention policy

As a general rule, any logging activity should be kept for at least one year, of which three (3) months should be online immediately accessible upon request from a governing body or external inspection. Management needs to familiarise with local contractual/legal requirements applicable to each business to determine if additional requirements apply, or a shorter retention is acceptable.

7.4.6 Physical security, controlled areas

UWL assets, including systems and media need to be protected against intentional or accidental physical damage. For that, they will be located in an area with restricted access and protected against environmental hazards, under full control of UWL.

7.5 SECURITY BY DESIGN, SECURE ARCHITECTURE, ACQUISITION AND DEVELOPMENT

7.5.1 Governance on approved technology and security design principles

IT Services will establish the approved technologies and design principles than can/should be deployed in UWL or vet specific solutions during the project, following and IT architecture methodology. Approval by IT Services or ultimately the Vice-Chancellor's Executive must be obtained for exceptions.

7.5.2 Information security in any project

Information security shall be addressed in project management explicitly as a requirement, regardless of the type of the project, and will be incorporated into the methodology.

7.5.3 Default configuration un-trusted

The default and vendor recommended configuration of any acquired system should not be trusted but subject to review and security lock down by an employee or independent reviewer with sufficient expertise. The reviewer will be responsible and accountable for commissioning a system sufficiently secure for its purpose.

7.5.4 Separation of Environments

There must be separate development, test, and production environments for all business critical applications, with appropriate segregation of duties. These environments must be kept separate by system-enforced security measures appropriate to protect the sensitivity of the software. In addition to protecting live data, attention should be given to protecting test data, migration data and approved source/object code.

7.5.5 Protection from malware

The default approach is that all UWL systems should have detection, prevention and recovery controls to protect against malware combined with appropriate user awareness. Exceptions need to be formally approved on a case by case basis by senior management from IT and the business affected

7.5.6 Minimum security features in systems

Systems should be developed/acquired and configured with the security features necessary to enable enforcement of the following:
a) Users can only access data and functionality for which they are authorised ("least privileges" approach)
b) Accountability for usage is maintained via appropriate audit trails.
c) Availability and integrity of the systems, including disaster recovery (DR) arrangements are addressed.
These security requirements need to be made explicit, should follow UWL project management and architecture methodology and should be included in services agreements, whether these services are provided in-house or outsourced.

7.5.7 Secure development and Vulnerability Management in the IT infrastructure

All systems must be developed/configured following practices that specifically identify and minimise vulnerabilities, and subsequently, processes will be in place to promptly address newly discovered vulnerabilities according to their criticality.

7.5.8 Installation of software, patching

Software installation should be restricted to users approved by IT Services. Only licensed software, approved by IT Services is allowed to be installed on systems. Installation of software updates should be managed by IT Services and follow the standard (or emergency) change management process.

7.5.9 Testing of security

The IT security of IT systems should be tested as part of the regular business as usual.
Systems should be probed for vulnerabilities before the go-live or significant change, and at least annually afterwards (special regulatory requirements may apply).

7.5.10 Multi-layered security in systems and networks

Every asset in the network should be configured securely individually as well as protected by a network architecture that secures the perimeter and incorporate segregation of environments. The design should aim at minimising weak links or "single points of failure" by establishing resilient, redundant, complementary controls, separation of duties, etc. Specific measures need to consider the risks and criticality/value of the asset protected, balancing usability and regulatory requirements.

7.6 TECHNICAL AND OPERATIONAL SECURITY

7.6.1 Control requirements for remote, mobile access and “bring your own device”

Additional security measures should be put in place to grant, revoke/restrict, authenticate and monitor such usage, compared with on-site “wired” access from a fully owned UWL device. At a minimum, the technology used to access UWL systems need to be approved by IT and the line manager of the user, prior to using/granting such access. Management approval must be documented and explicit (i.e. not available by default).

7.6.2 Encryption of data

Only IT Services approved tools and methods will be used to encrypt data UWL have ownership or custodianship. Data owners are responsible for selecting the encryption method and ensuring the recoverability of the data and safeguarding of the encryption keys, in consultation with IT. Minimum requirements for encryption are defined in a separate technical policy, in alignment to the UWL data classification model.

7.6.3 Protecting the business processes stability

IT Services and the Business Management that owns the system have a joint responsibility for defining operational procedures and training users to ensure the secure operations of the processing facilities.

Changes and tests on live (i.e. Production) systems including servers and end-user devices should be conducted in a controlled manner. Direct changes in production, un-announced tests/hacking, or intentionally creating a failure are not authorised by default.

7.6.4 Monitoring and duty of care

IT Services has a mandate to monitor the performance, integrity and overall confidentiality of the systems and have the technical knowledge and authority to apply measures to protect the overall infrastructure against threats, following normal or emergency procedures.

UWL reserves the right to monitor individual’s usage, to the extent granted by the law, in order to protect its legitimate business interests. Monitoring may include accessing stored or transmitted data as well as observation of user activity.

UWL has also a "duty of care" obligation to reasonably monitor usage of company resources to detect abuse in breach of the law, and to report to the appropriate authorities.

7.6.5 Logging and Auditing policy

By default system logs should be enabled to capture user logon, exceptions, faults and information security events/alerts. Regulatory and audit/compliance requirements involving logging, audit trails, reporting and any other functionality/processes to enable verification of operational systems are a mandatory requirement to be assessed explicitly in any systems project.

7.6.6 Change management and security

All changes to production data and programs must be done following a documented change management process, and security should be in place to enforce that process via automated controls where possible.

7.6.7 Physical and environmental security

Equipment shall be installed with appropriate protection from environmental factors and unauthorised access, in line with the sensitivity of the data and business process it supports. All equipment by default should be provisioned, installed and managed by IT Services, with vendor warranty and maintenance in place. Exceptions, including vendor managed installation and pre-approved decentralised purchases, need to be reviewed by IT Services and approved on a case-by-case basis.

7.6.8 Data backup and restore procedures

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup plan approved by the data/system owner. As a default/minimum criteria, backups plans should allow restore at any point of past 30 days, plus last 12 months of monthly snapshots and 7 years of annual copies, stored in a different location than the system being backed up. Backups should be stored encrypted, under physical security and inventory control. Restore tests of the media/files should be done at least once a year.

7.7 ACCESS MANAGEMENT

7.7.1 Need to know principle

Access to UWL systems and data should be granted on a "need to know basis", that is, the minimum access needed to perform a duty. This is to protect the systems and data in them from accidental or intentional loss.

7.7.2 Due diligence before granting access

Access to systems and information, including setting up permanent network connectivity solutions, will be granted to employees and third parties/service providers only after a due diligence risk assessment has been performed and after the employment or service contracts, including confidentiality and accountability clauses has been agreed in writing. Processes should be in place to ensure ongoing monitoring of compliance.

7.7.3 Business management responsibility for access control

Each Business Unit must have a consistent process to approve modify and remove, as well as regularly review the access granted to users on systems and information he/she is accountable for, and monitor the usage of the system, with assistance and tools provided by IT.

7.7.4 Minimum standard for authentication

All enabled accounts in computer systems must have passwords or a comparable authentication method to establish user accountability. If using passwords, these need to have system enforced complexity, expiration, reuse and lockout controls. System enforced session timeout is required. Passwords and other secret information needed for authentication should not be transmitted over the networks or stored in the clear (i.e. needs to be encrypted).

7.7.5 Individual accountability

Systems and procedures should ensure activity in the systems or with IT assets can be linked to an individual. When the individual is not an employee, the manager accountable for allowing and monitoring such access should be clearly identified. If the account is used by another system, there still need to be an appointed individual responsible for the setup and system credentials and generally the safeguarding of that account.

7.7.6 User accountability for security

All employees and third parties using UWL's systems are accountable for understanding and following UWL's security policies, in particular on how to protect their accounts and passwords from misuse. All employees are expected to report any concern or potential suspect activity they may encounter. Employees should contact their line manager, IT or Human Resources for clarification or assistance.

7.7.7 Privileged access to systems

All privileged/administrator activity (e.g., ID and password creation, direct access to data, maintenance, and support) must be traceable to the individuals whether directly accountable for these activities, or indirectly accountable, in the case of automated processes.

7.8 INCIDENT MANAGEMENT

7.8.1 Incident response

UWL will maintain an information security incident response plan that will rely on ongoing operational monitoring and incident response procedures, including escalation procedures to senior management and integration with the UWL institutional continuity management plan.

7.8.2 Contact with authorities

Appropriate contacts with relevant authorities and external entities (e.g. the Press) shall be maintained. In case of an incident, only nominated contacts are authorised to liaise with authorities and external entities, following the protocols defined in the UWL incident response plan and/or instructed by the Vice-Chancellor's Executive.

7.8.3 Responsibilities of staff and students

If a member of the University (staff or student) is aware of an information security incident then they must report it to the IT Service Desk. If necessary, members of the University can also use the institutional whistle blowing process (see Public Interest Disclosure policy).

7.9 CONTINUITY MANAGEMENT

7.9.1 Secure operations in contingency

People, assets and information services need to be protected in a disaster situation; to save lives and to ensure the continuity of the going concern. For that UWL establishes and maintain a business continuity plan.

Information Security shall be embedded in the continuity plan to ensure operations, even during an adverse situation, maintains acceptable levels of security and meets regulatory requirements.

7.9.2 Business Management responsibility for security

Managers are responsible for specifying the requirements for protecting the availability of systems/data, and ensuring the necessary funding to implement these is in place, and are ultimately accountable for its implementation. It should

be based on the analysis of risks, criticality of assets and consider regulatory requirements. IT Services responsibility is to deliver and maintain the contingency arrangements as agreed.

7.9.3 Disaster recovery and business continuity

Resilience and disaster recovery capabilities are an integral part of all IT services and need to be defined in the design phase of any project.

7.9.4 Testing of Disaster Recovery arrangements

Disaster recovery capabilities are especially vulnerable to failure and will not be deemed acceptable unless they pass regular documented tests.

7.10 COMPLIANCE, VALIDATION AND CERTIFICATION INITIATIVES

7.10.1 Compliance with the law

UWL and each employee is accountable for operating within the law, and it is their responsibility to be aware of legal and contractual requirements and implement the controls within their remits to comply.

7.10.2 Information security in contracts with third party

Service Providers with access to UWL systems and data must contractually commit to implement security measures to meet the business objectives (e.g. protecting intellectual property, availability) as well as regulatory or contractual obligations for which UWL has ultimate accountability.

7.10.3 Supplier service delivery management

The manager that owns the service is responsible for regularly monitoring, review and audit supplier service delivery. Information Security considerations, including protecting UWL intellectual property and maintenance of regulatory compliance requirements should be explicit in this review.

7.10.4 Management controls

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements. Evidence of the performance of such controls should also be kept.

7.10.5 Internal and independent security reviews

The information security programme and its implementation shall be reviewed independently at planned intervals or when significant changes occur. It is expected that evidence of the controls performed by employees/systems as well as any controls management performs over them (also called “second tier” or “control over the control”) are kept. Management should be prepared for -and fully cooperate during- internal reviews performed by Internal/External Audit and the Information Security Manager.

7.10.6 Compliance with the Payment Card Industry Data Security Standards

UWL specifically acknowledges the contractual requirement to handle payment card details of UWL customers securely and with care, and meet the appropriate data security standards maintained by the PCI Council.

8. GUIDANCE ON LEGAL, REGULATORY AND CONTRACTUAL OBLIGATIONS

Relevant legislation to consider (please note this is not a complete list and laws are constantly enhanced with modifications or underlying administrative procedures):

- Agreement on Trade-related Apects of Intellectual Property 1994
- Anti-terrorism Crime and Security Act 2001
- Broadcasting Act 1990
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Software) Amendment Act 1985
- Copyright Directive 2001/29/EC
- CE Convention on Cybercrime 2001
- Criminal Justice Act 1988
- Data Protection Act 1998
- Defamation Act 1996
- Digital Economy Act 2010
- Electronic Commerce (EC Directive) Regulations 2002 (2000/31/EC)
- Electronic Communications Act 2000

- Interception of Communications Act 1985
- Obscene Publications Act 1964
- Police and Criminal Evidence Act (PACE)
- Protection of Children Act 1978
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 and 2004 Amendment
- Protection from Harassment Act 1997
- Regulation of Investigatory Powers Act 2000
- Telecommunications Act 1984
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- The Freedom of Information Act 2000
- The Telecommunications (Data Protection and Privacy) Regulations 1999
- Terrorism Act 2000
- The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

9. ADMINISTRATION, MAINTENANCE, COMMUNICATIONS

- As defined in the policy, this set of documents is maintained by the Information Security Manager and is to be reviewed annually.
- The Information Security Manager, in coordination with Human Resources and Legal counsel will announce the exercise, which will involve representation of Academic, Non-Academic and Student bodies.
- The review and update will be approved by the ISG group.
- Every new employee will have this policy included in the induction pack.
- After each review, the news of the policy update will be communicated to all employees (TBD: All employees will need to formally accept the revised policy).
- The current approved version of this policy will be published in the UWL Internet site.
- Previous versions with its validity period will be kept by the Information Security Manager.

10. ENFORCEMENT

This Policy forms part of the UWL set of policies every employee needs to understand and follow as indicated in the standard employment contract.

Failure to follow the policy may lead to disciplinary action, led by Human Resource.

This policy is enforceable, from the effective date stated at the beginning of the document. Transition periods, where applicable, would be stated at each point/article, and also summarised at the beginning of the document. This policy does not apply retrospectively.

11. SUPPORTING POLICIES, PROCEDURES AND GUIDELINES

Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated procedures and guidelines are published together and are available for viewing on the UWL's website in the Policies section.

All staff, students and any third parties authorised to access UWL's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

An information security charter will accompany this policy to provide the readers with a view of their roles and responsibilities across the range of activities that information security comprises.

The relevant supporting policies/Standards are:

1. ISMS definition, internal validation, audit response (TBD)
2. Data classification (TBD)
3. Data Protection Policy (Owner: Data Protection Officer)
4. IT Record management, logging and retention (WIP)
5. Encryption standard (WIP)
6. Security by design (TBD)
7. Operational Security (TBD)
8. Identity and Access management (WIP)
9. Third party access (TBD)
10. Remote access and working and mobile access (POL_ITS_007)
11. Incident management (TBD)
12. Continuity management (TBD)
13. Third party assurance (TBD)

Related policies

- Acceptable usage policy (Owner: HR main lead, IT in support role)
- Social media policy (Owner: Marketing)
- Data Privacy Policy (Owner: Legal counsel)
- Information Governance Policy (Owner: Secretary)
- Business Continuity Planning (BCP) (Owner: VCE)
- Student Handbook (Owner: Student Services)
- Record Retention Policy (Owner: Legal counsel)

12. GLOSSARY

Access Control - ensures that resources are only granted to those users who are entitled to them.

Appropriate - suitable for the level of risk identified and justifiable by risk assessment.

Asset – anything that has a value to the University

Audit - information gathering and analysis of assets, processes and controls to ensure policy compliance.

Authentication - is the process of verifying a claim of identity. Three different types of information can be used for authentication: something you know (a PIN, a password, mother's maiden name), something you have (magnetic swipe card) or something you are (biometrics).

Availability – information and supporting IT systems should be available to authorised users when needed.

Confidentiality - information is disclosed only to those who are authorised to view it.

Control – a means of mitigating risks by providing safeguards. This includes policies, procedures, guidelines, other administrative controls, technical controls or management controls.

Data - Information held in electronic or hard copy form.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.

Information Asset Owner – is a person or entity that has been given formal responsibility for the security of an information asset.

Information Security – preservation of confidentiality, integrity and availability for information and supporting IT systems.

Information Systems – any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.

ISO/IEC 27001:2013 - information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information Technology – Security Techniques – Information Security Management Systems – Requirements.

ISO/IEC 27002:2013 - information security standard (list of controls) published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information Technology – Security Techniques – Code of practice for Information Security - Controls.

Integrity - maintaining and assuring the accuracy and consistency of information over its entire life-cycle. It should not be possible for information to be modified in an unauthorized or undetected manner.

Policy – overall intention and direction as formally expressed by management.

Risk - the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats and vulnerabilities

Risk Assessment – overall process of identifying and evaluating risk.

Third party – person or body that is recognised as being independent of the University.

Threat – something that has the potential to exploit a weakness to result in some form of damage. Threats can be environmental, deliberate, accidental, logical or technical.

Vulnerability – weakness of an asset or group of assets that may be exploited by a threat.

13. VERSION HISTORY

Date	Version	Description	Who
	V.00	Initial draft.	JC
	V.00	Initial comments and edits.	AE
30/3/2014	V.01	Incorporated suggestions from AE mark-up.	JC
31/4/2014	V.02	Simplified mapping to ISO, also addressed most of the orphan ISO points. Spitted roles and responsibilities into the charter piece and Organizational security section of the policy.	JC
7/5/2014	V.03	Various tweaks, mark-up with track changes.	JC
1/6/2014	V.04	Removed most of the comments and all ISO mappings, moved them to a companion document called “Guidance”. Minimal tweaks in the actual content from previous version.	JC
24/06/2014	V.05	Mark-up from AE review.	AE/JC
28/7/2014	V.06	Amended risk treatment policy as per University Secretary review. Added a third party chapter in the “responsibilities” section as per suggestion from KPMG (internal audit).	JC
31/7/2014	V.07	Tweaked the wording for the data retention statement as per suggestion from KPMG. Changed the Data Classification TBD comment to refer to the need to decide what approach to data classification we want to adopt, if at all. The table is an example.	JC
16/12/2014	V1.0	New foreword to the Information Security Policy by the VC. Improved document control. Updated legislation. Added Glossary.	AE/FP