UNIVERSITY COLLEGE CORK

IT Policy Framework

11/27/2012

This document provides a clear overview for the UCC Community on how each IT policy interacts, the differences between policies, standards and guidelines, the template for these documents, the roles of various stakeholders, the approval process for these documents and final the Hierarchy of compliance.

Document Location

http://www.ucc.ie/en/it-policies/policies

Revision History

Date of this revision: 09/10/2012	Date of next review: 10/10/2012

Version Number/Revision Number	Revision Date	Summary of Changes
0.1	18/09/2012	Added section on Scope of Policy documents after discussion with John Fitzgerald
0.2	9/10/2012	Reviewed with OCLA for regulatory compliance check
0.3	10/10/2012	Submitted to IS & AR committee for discussion/feedback
0.4	25/11/2012	Updated based on OCLA feedback and IS&ER feedback and resubmitted to IS&ER for final approval

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date
Gerard Culley	Director of Information Technology	
John Fitzgerald	Director of Information Services	
John Morrison	Chair of IS & AR committee	
Michael Farrell	Corporate Secretary	4/12/2012

This policy shall be reviewed and updated on an annual basis.

Table of Contents

1. Purpose

The purpose of this document is to provide direction, coordination and management of relevant Information Technology (IT) documentation within University College Cork – National University of Ireland, Cork (the "University"). IT Policy is considered to include IT Policies, IT Standards, IT Procedures and related guidelines.

The University endeavours, at all times, to ensure consistent, high quality implementations and management of its IT resources, processes and practices. A comprehensive framework of well-defined policies, procedures and standards are required to facilitate and ensure this. The need for formal IT Policy has been highlighted in risk management processes and internal control frameworks for the University. This IT Policy Framework is a key element in meeting and supporting these requirements.

In developing this framework of IT policies, procedures and standards for the University, due regard and consideration has been given to the ISO 27000 series of standards which have been specifically reserved by ISO (International Standards Organisation) for information security matters. It is not intended that the University seeks to be compliant with all aspects of the relevant ISO information security standards as this would not be appropriate in all instances. However, it is intended that the University would aspire to implement policies, standards and procedures which are consistent with key aspects of the standards.[1]

2. Definitions

This section defines relevant terms, in an IT Policy framework context, that may be unfamiliar to the readers of this document.

Policy

Is a high-level overall IT plan embracing the general goals and rules on how to manage information technology and data in the University, a policy sets direction. As opposed to policies, IT standards and procedures are tools to implement and enforce the IT policies.

Procedures

Are detailed step-by-step tasks that should be performed to achieve a certain measure. Procedures spell out how the policy and the supporting standards will actually be implemented in an operating environment.

Procedures can fall into a number of categories including:

- Administrative
- Logical/Technical
- Physical (in the case of security and access control)

[1] Other relevant standards include ITIL (IT Infrastructure Library)

Standards

Specify how hardware and software products are to be used. They provide a means to ensure that specific technologies and business applications are used in a uniform way across the University to meet a defined goal. Standards are sometimes referred to as protocols in the documentation. Adherence to defined standards is considered mandatory by the University.

Standards can fall into the three categories of

- Administrative
- Logical/Technical
- Physical

Guidelines

Aim to streamline particular processes according to a set routine or sound practice. By definition, following a guideline is never mandatory. Guidelines may be issued by the University to ensure the actions of its staff, student and external parties are more predictable and of higher quality.

Policy, standards, procedures and guidelines are intended to apply to the following defined the University related groups:

Staff

All full-time and part-time employees of the University, including current and retired staff.

Students

All full-time and part-time students of the University, including current students and alumni.

External parties

All the University's subsidiary companies, contractors, researchers, visitors and/or any other parties who are granted access to the IT resources of the University.

3. Roles And Responsibilities

The following roles and responsibilities apply in relation to this Framework[2]:

Governing Body:

To review and approve the framework on an annual basis or as recommended by the audit committee of the Governing Body.

VP for Information Services

- To ensure the framework is reviewed and approved by the Governing Body as appropriate.
- To consult as appropriate with other members of the University Management Teams.
- To ensure the appropriate policies, standards and procedures are in place to support the framework.

[2] Specific roles and responsibilities are set out in each policy, procedure and standard as roles and responsibilities can vary across various documents.

IT Director:

- Provide training resources and awareness facilitation.
- To contribute to the development of policies which support the framework.
- To define and implement standards and procedures which enforce agreed policies.
- To initiate regular reviews and ensure documentation is updated as appropriate.
- To provide secure mechanisms for central storage of IT Documentation.
- To facilitate Version Control of IT Documentation.
- To facilitate publishing documents as appropriate.

Staff/Students/External Parties:

- To adhere to policy, procedures and standards noted in this framework.

If you have any queries on the contents of this framework, please contact the IT Director in the first instance.

4. Scope

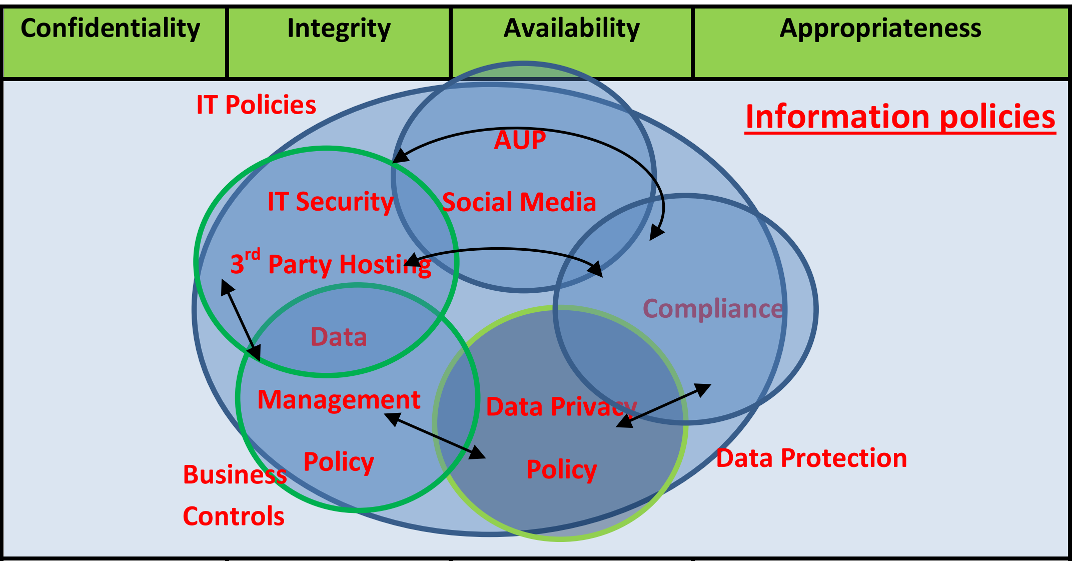
This IT Policy Framework covers documentation of policy, procedures and standards relating to:

- The University's information assets
- The University's IT Resources

This framework applies but is not limited to the following, the University related groups as defined in section 3.0:

- The University's Staff
- The University's Students
- The University's External Parties

Appendix I provide an index of the University IT Policy in accordance with the following approach.

Principles	Confidentiality	Integrity	Availability	Appropriateness
Policy Layers				
Standards Layer	*Password Standards*	*Website Standards*	*Anti-Virus Standards*	End User Guidelines (including portable devices Guidelines)
Procedural Layer	*User Admin* *Physical Access*	*Change Management*	*Data Backups* *D R Plans*	
Physical and Logical Layers				

The policies above have significant overlap; therefore each policy should focus on the domain it is legislating for and refer to other appropriate policies as the need arises. Duplication across policies should be avoided. For example the Acceptable Usage Policy should refer readers to the data privacy policy when referencing issues of data protection or data privacy; it should reference the IT Security policy when referencing issues of technical security.

5. Version Control Information

The University requires that all IT documents within the scope of this framework are version controlled by the IT Director and, as such, each separate document includes a control sheet which must be completed as shown below:

Revision History

Date of this revision:	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes

Approval

This document requires the following approvals:

Name	Title	Date

In addition, the footer of the document must clearly indicate the current version number/ revision number. Where the document is in draft or going through a review cycle it should be numbered as version number/ revision number – for example 1.02 is the second revision of version 1.0 prior to finalisation of version 2.0. When a final version is agreed, it should be version 1.0, 2.0 and so on.

All IT policy documentation should be held in one secure central location to which access is restricted to "READ ONLY". Once finalized, changes to documents are not allowed. To amend a document a new version needs to be created and reviewed. The IT policy documentation custodian

(IT Director) will be the only person with full access to upload new documents/new versions and will only do so following the appropriate review cycle (Refer to Section 6). This access restriction is critical to ensure appropriate documentation change control.

6. Review/Approval Process and Timeframe

All IT documentation must be reviewed and approved at the appropriate level.

- For IT Policies, Procedure and Standards, the appropriate level is the University's Management Team and/or the Governing Body as appropriate. However all policies should firstly go through appropriate consultation process with staff via the Information Strategy & Education Resources Committee and the relevant Industrial Relations (IR) forum as appropriate.

- For Guidelines the appropriate level is deemed to be the Information Services Management Team (ISMT) and/or relevant data owners.

Approval Process		
Type	**Document**	**Reviewers/Approvers**
Policies	IT Policy documents	1. Created by IT Services, with expert support 2. ISMT Approval 3. Approved/amended by OCLA 4. IS&ERC & Academic Council 5. UMTS/Governing Body
Guidelines	Procedures, Standards and Guidelines Logical/Technical Administrative Physical	1. Created by technical experts 2. Approved by Director 3. Approved by ISMT

All IT Policies should be reviewed and approved as outlined in Section 6 above. Following review and approval, the IT Policy should be again communicated to all staff as a reminder of its content. It is only through on-going campaign of communications and awareness that all staff can remain up-to-date on Institute Policy.

IT standards and procedures should be reviewed as required by technology changes and/or changes in policy and / or processes.

6.1 Review Timeframe

Review cycles should be completed as quickly as possible but should take no longer than 12 weeks end to end. If feedback is not provided within the specified timeframe (8 weeks), the relevant document is deemed to be agreed and automatically routed to the next stage in the approval process.

6.2 Approval Timeframe

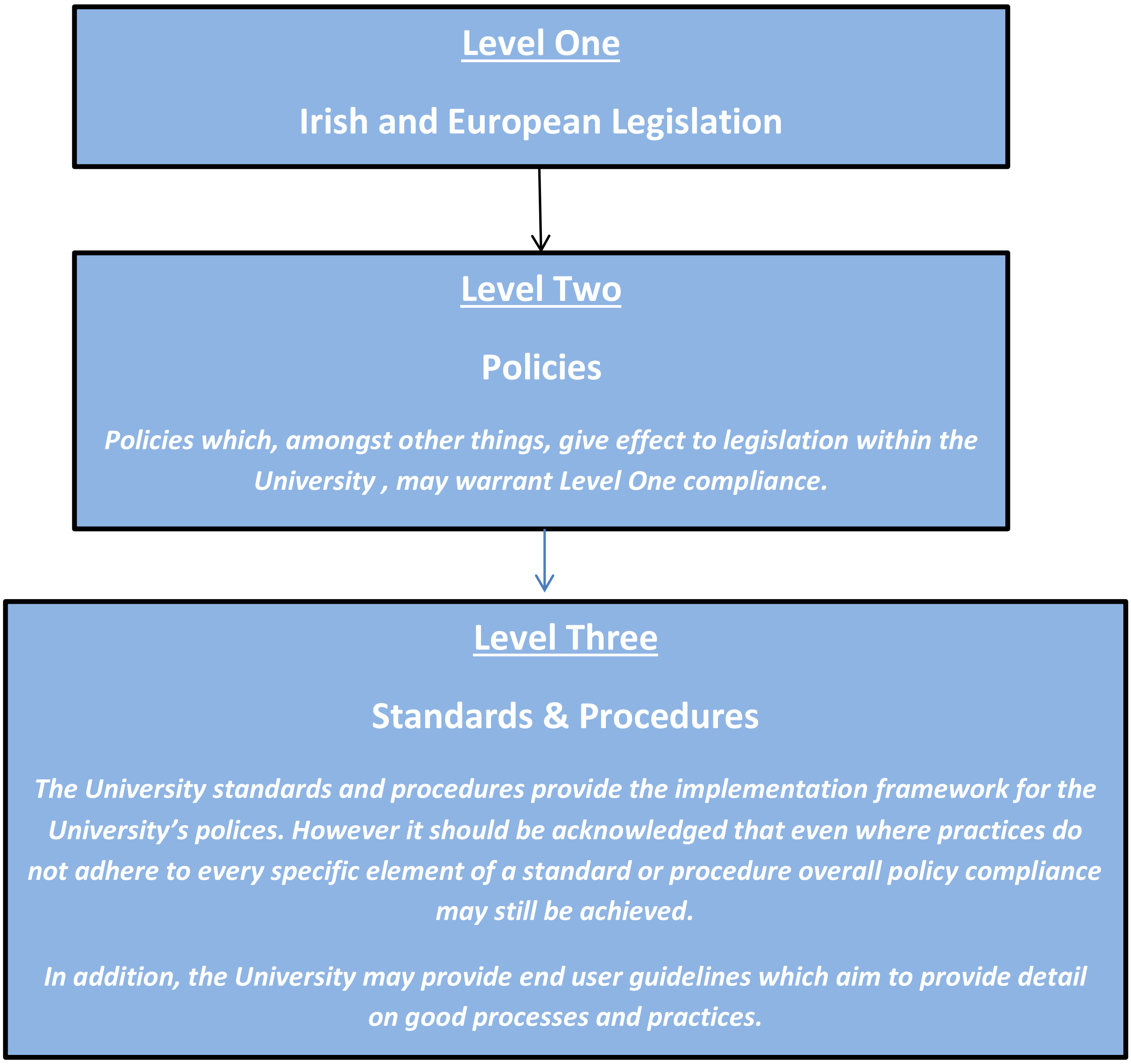
Newly developed, amended and /or reviewed IT documents to be distributed to relevant approvers requesting a response within 4-6 weeks of distribution. Approval of policies will be dependent on Governing Body meeting schedules and agendas.

7. Appendix I - It Documentation Index

Type of Documentation	Name	Status	Location
Policy	Information Security	GB approved	*www.ucc.ie/en/it-policies*
	Acceptable Usage	IS & ER pending	*www.ucc.ie/en/acceptable-usage-policy*
	Social Media Management	IS & ER pending	*www.ucc.ie/en/it-policies/policies*
	Data Management	GB approved	*www.ucc.ie/en/it-policies/policies*
	Data Protection Policy	GB approved	*www.ucc.ie/en/it-policies/policies*
	Third Party Hosting	IS & ER pending	*www.ucc.ie/en/it-policies/policies*
Standards	Password Standard	*To be completed*	*To be completed*
	Anti Virus Scanning and Protection Standard	*To be completed*	*To be completed*
	Data Backup Standards	*To be completed*	*To be completed*
Procedures	User Administration Procedure	*To be completed*	*To be completed*
	Data Backup and Monitoring Procedure	*To be completed*	*To be completed*
	Change Control Procedure	*To be completed*	*To be completed*
	Physical Access Procedure	*To be completed*	*To be completed*
	Disaster Recovery Plan	*To be completed*	*To be completed*
	Data Classification	Being Drafted	
	Protocol for Systems Abuse	Being Drafted	

Guidelines	Mobile phone and smart phone User Guidelines	*Completed*	www.ucc.ie/en/it-policies/guidelines

Section 8 - Hierarchy Of Compliance



Level One

Irish and European Legislation

Level Two

Policies

Policies which, amongst other things, give effect to legislation within the University , may warrant Level One compliance.

Level Three

Standards & Procedures

The University standards and procedures provide the implementation framework for the University's polices. However it should be acknowledged that even where practices do not adhere to every specific element of a standard or procedure overall policy compliance may still be achieved.

In addition, the University may provide end user guidelines which aim to provide detail on good processes and practices.