

## Preparing to implement a BS 7799 based security policy using the UCISA Toolkit

Iain Stinson

The University of Liverpool

# Agenda

- Covers our initial planning
  - we are still at the very beginning...
- Focuses on using “what we’ve got already”
- Highlights issues around IS/IT Governance

# Why you may not wish to develop an Information Security Policy

- Exposes holes in organisations
- Highlights failures to follow good practice
- Embarrassment?
- Exposes lack of resources to do things properly!
- Exposes lack of professionalism within the organisation??

# Why develop an Information Security Policy?

- To manage any of the issues exposed on the previous slide should there be the most remote possibility that they exist within your institution
- Toolkit provides good advice on why we all need to do this (in the early sections).

# Outline plan

- Build a business case for developing the Information Security Policy. Use the ideas in the early part of the Toolkit.
- Establish institutional framework for the Information Security Policy. →
- Set up a “project board” to oversee the development of the policy.
- Education for the project board: “What is an Information Security Policy”
- Prepare and audit for the project board setting out the state of the institution with respect to the Information Security Policy →
- Using the audit report, have the board determine the scope of the institution’s Information Security Policy. You can omit parts for a first iteration (or forever) – if you chose to have you policy certified then you would need to address all the applicable parts of the standard. →

# Outline plan (2)

- Establish a team or teams to develop the policy (following the sections in the Toolkit) building on your existing policies for the sections the board has determined are “in scope”.
- Have the Project board:
  - review the output from the team(s)
  - Review / rework the draft policy elements for consistency.
  - Review proposed policy and determine its impact on existing IS/IT and other institutional policies and regulations.
- Short period of consultation where the proposed policies can be discussed across the institution (possibly through School / Faculty committees)
- Adoption of the Information Security Policy and consequential changes to regulations by institutions Council and Senate.

# Post adoption

- On going communications of policy to all
- Implementation of the policy across the institution
- Monitor implementation – report back to “owning committee”
- Periodic review of Information Security policy by owning committee and computing services.

# Resources

- The *Toolkit!*
- Have you got sufficient staff resources to carry this out?
- Can you make effective use of consultants (external or from other parts of the institution (internal audit)) to do some of the work?
- Will consultants get to the real state of play?
- Include sufficient staff resource in the business case.
- Will you need legal advice (particularly wrt to any changes in regulations, or contracts)?

# Who owns the Information Security Policy?

- Need to secure ownership at the appropriate senior level?  
Vice-Chancellor, Pro-VC, Director of IS/IT, Chair of institution's main IS/IT committee, Registrar
- Membership of the Information Security oversight committee
- Balance between oversight committee (policy) and working party (implementation of controls).
- Issues of IS/IT governance are likely to be raised in implementing the policy.

# At The University of Liverpool

- Information Security policy will be owned by our Information Services Committee chaired by a ProVC who will be the champion for the policy
- Information Services Committee will have oversight – and this is to be added to the committees remit. Policy will be ratified by Council and Senate
- Working party / parties likely to be run by Computing Services.

# Governance issues

- How are IS/IT decisions made, by whom? Is this set out in an open fashion?
- Who is responsible for the use (misuse) of IS/IT?
- What services does central IS/IT provide and what are provided by departments? Is this balance appropriate? What are the relationships between central and “local” provision?
- Service Definitions for major IS/IT Services. Performance targets and monitoring.

# Audit of existing policies

- Review the issues that are addressed by the policy (as set out in the *ToolKit*) and the institution's existing IS/IT policies; Map the existing policies against the policies in the *Toolkit* section by section
  - How complete are the various sections of the Information Security policy using your existing policies?
  - Are there any sections of the information policy that might be difficult to address because they do not fit with the institution's policies (not just IS/IT policies) or that is not timely to address them (for various reasons, including "political" reasons)?

# What “policies” do we have already?

- Get together copies of the current IT related policies your institution has already.
  - Regulations on usage of IT for users
  - Documents setting our good practice and /or interpreting the Regulations for users
  - Documentation about your Business Continuity / Disaster Recovery Plan
  - Guidance notes for academic groups that run their own systems
  - “Committee decisions” not yet embedded into policies
  - Formal or Informal documents about working practices
  - Contracts of employment used within the institution

# What “policies” do we have already?

- Review their content
- Are they up to date?
- Are they still relevant?
- Are they followed or ignored?
- Are they still practical?
- Do they (completely or in part) address the policy requirements set out in the *Toolkit*

# University of Liverpool Policies

- Regulations <http://www.liv.ac.uk/csd/regulations/index.htm>
- Summary of Regulations  
<http://www.liv.ac.uk/csd/regulations/summaryitregs.htm>
- Codes of Practice  
<http://www.liv.ac.uk/csd/regulations/codes/index.htm>
- Responsibilities of Heads of Department  
<http://www.liv.ac.uk/csd/regulations/hodresponsibilities.htm>
- Computing Services Business Continuity Plan documentation
  
- Records Management  
<http://www.liv.ac.uk/library/recman/Records%20Management%20Policy.htm>
- JANET AUP  
<http://www.ja.net/services/publications/policy/aup.html>
  
- *Approved and adopted by Senate and Council*

# Regulations for the Use of IT Facilities at the University

- **Scope**
- **These Regulations apply to the use of all computer, electronic information and communication facilities at or operated wholly or partly by the University of Liverpool ("the University") including:**
  - a. All local computing facilities, multi-user systems, server systems, work stations, personal computers, micro computers and networks or other electronic information and communication systems whether provided by the University or otherwise and which are intended wholly or partly for use by employees of, researchers or students of the University or wholly or partly for use for other University or University related or academic purposes;**
  - b. All remote facilities that are accessed through the computer, electronic information and communication facilities at or operated wholly or partly by the University.**

# Regulations

- Formal!
- For all IT Systems not just central regulations.
- Recognises that each System is managed under a recognised authority;
- Sets out rules for registering and managing user accounts and users
- Lists acceptable usage; addresses commercial usage;
- Addresses Usage monitoring (including monitoring “electronic communications”);
- Confidentiality of information;
- Incorporates conformance to “CHEST” software / electronic information licence
- Breaches – penalties and process

## Summary of the Regulations for the Use of IT Facilities at the University

This document includes the Regulations and Codes of Practice for the use of IT Facilities at the University. These apply to all members of staff, visitors, honorary members and all students of the University.

The Summary is provided so that users of IT facilities more easily understand their obligations

# Information Systems Security - Responsibilities for Heads of Departments

- These describe the responsibilities of Heads of Departments in relation to computers in his/her area of responsibility.
- If all the computers in a department are connected to a PC client service provided by the Computing Services Department (CSD) then no action is necessary.
- If a department connects any computer to the University network other than via a pc client service provided by CSD, then the Head of Department must appoint a system administrator and follow the instructions detailed in this policy document

# Departmental Systems - HOD responsibilities

- Formal administration for all systems
- Each departmental system must have a manager / administrator
- Users must be registered to use the system (lists of users must be available to computing service if requested)
- System administration responsibilities including data management, security patches, recording usage for monitoring
- PCs that are clients of the computing service covered by computing service not department

# Codes of Practice

- There are a number of Codes of Practice for the use of IT Facilities at the University
  - Email
  - Electronic Publishing
  - Web pages
  - Use of the data network
  - Wireless networking
  - Storage of University Information Assets

# Records management

The University of Liverpool recognises that efficient management of its records is essential, both for effective administration and to enable it to comply with legal and regulatory requirements. Records held by the University have always had legal significance, as proof of the terms of a contract for example, or evidence for employment law purposes. In recent years, however, records themselves have become the focus of legislation, notably in the Data Protection Act 1998 and the Freedom of Information Act 2000 (FOIA). From January 2005 the University will be obliged by law to respond to enquiries within the scope of FOIA.

This policy establishes requirements designed to help staff meet legal obligations relating to records management and to manage records so that their value as a corporate resource for the University is fully exploited.

# Janet AUP

## For the network

- Background and Definitions
- Acceptable Use
- Unacceptable Use
- Passing on and Resale of JANET Service
- Compliance

# How (well) do existing policies match the recommendations in the Information Security Policy

## Issues – Problem areas

### ● **Business Continuity Plan**

- Coverage.
- Highlights need to categorise systems and services more completely (link with SLAs). (Recurrs throughout the *Toolkit*)
- Updating. Keeping pace with developments and changes.

### ● **Compliance**

- Intellectual property rights. Not to be confused with IPR of university developed concepts and products.
- Terms and conditions for employment of individuals and IS/IT

## How (well) do existing policies match....

- **Outsourcing and third parties.** We have nothing at present about this area.
- **Personnel.** Really requires contract changes. Expect the institution to no want to get into this at the present time.
- **Operations.** Informal documents about change control and testing and release of systems exist.

More....

# What we've got...

- Our existing policies and security related documents provide some useful and already agreed material that can be incorporated into the Information Security Policy
- Many areas need considerable enhancement and the Toolkit provides some material from which to develop our policies

# Reprise: Outline plan

- Build a business case for developing the Information Security Policy. Use the ideas in the early part of the Toolkit.
- Establish institutional framework for the Information Security Policy.
- Set up a “project board” to oversee the development of the policy.
- Education for the project board: “What is an Information Security Policy”
- Prepare and audit for the project board setting out the state of the institution with respect to the Information Security Policy
- **Using the audit report, have the board determine the scope of the institution’s Information Security Policy. You can omit parts for a first iteration (or forever) – if you chose to have you policy certified then you would need to address all the applicable parts of the standard.**

# Reprise: Outline plan (2)

- Establish a team or teams to develop the policy (following the sections in the Toolkit) building on your existing policies for the sections the board has determined are “in scope”.
- Have the Project board:
  - review the output from the team(s)
  - Review / rework the draft policy elements for consistency.
  - Review proposed policy and determine its impact on existing IS/IT and other institutional policies and regulations.
- Short period of consultation where the proposed policies can be discussed across the institution (possibly through School / Faculty committees)
- Adoption of the Information Security Policy and consequential changes to regulations by institutions Council and Senate.

# When will it be done?

- Work in-progress
- Target completion: Easter 2006  
Ready for consideration by Senate in its  
May/June meeting