University of Liverpool

Information Security Review Policy

Reference Number	CSD-014
Title	Information Security Review Policy
Version Number	1.2
Document Status	Active
Document Classification	Open
Effective Date	27 November 2012
Review Date	28 March 2018
Author	Computing Services Department (David Hill)
Approved by	Corporate Services & Facilities Committee (Nov 2012)
Implemented by	Information Security Officer
Monitoring of compliance	Faculty Information Security Managers (Local) CSD Information Security (Central)
Comments	• 28/03/2017 Annual Review (No Changes)

Information Security Review Policy

1. Introduction

Information is a vital asset to any organisation, and this is especially so in the University which is a knowledge-driven organisation. Virtually all of our activities create information assets in one form or another. The Information Security Review Policy and its associated policies are concerned with managing University expectations and risks through a continuous improvement process where evidence of security controls can be observed and are of a sufficient standard to protect the information assets.

2. Principles

The Information Security Review Policy allows the University to determine if information security controls are in place. The confidentiality, integrity and availability of University information assets can then be safeguarded.

- All information assets must be appropriately handled and managed in accordance with their classification
- University information assets should be made available to all who have a legitimate need for them
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events.
- All staff and students of the University with access to information assets have a responsibility to handle those assets appropriately and in accordance with their classification
- Information asset owners are responsible for ensuring that the University classification scheme (which is described in the Information Security Policy) is used appropriately
- Information assets must be sufficiently protected in accordance with University security policies and the Information Security Management System (ISMS).

3. Objectives

This Policy is designed to:

- Define the purpose of security reviews
- Define the different types of security review
- Engage, where appropriate, with the relevant Faculty/Professional Service manager or appointed delegates in the co-ordination of security reviews and external audits
- Provide clear and timely communication to all relevant parties
- Ensure ownership and follow up actions plans are documented and agreed
- Ensure that all University staff, who are responsible for information security reviews, are clearly identified
- Ensure that actions to mitigate security vulnerabilities are reviewed and documented accordingly

4. Action Implementation

Procedures will be put in place to ensure the effective use of audits and security reviews. These procedures include:

- Defining relevant roles and responsibilities
- Making University staff and students aware of the requirements of internal and external audits

- Ensuring that the integrity of information gathered in reviews and audits is maintained. Throughout the process information must be: accurate, complete, timely and consistent with other information and events that may determine the reasoning and outcome of an audit and its findings
- Producing, reviewing and maintaining Audit Review Reports in a timely manner

5. Purpose of Security Reviews

The University undertakes regular reviews, as part of a commitment to protecting information assets, in accordance with security policies, standards, processes, legislation, regulation and best practice methods across all activities.

There are many types of security reviews that can be defined within the scope of the University's Information Security Management System (ISMS). There are two different types of security review that are designed to detect vulnerabilities with the University's information assets and core services. These include:

- Technical
- Non-technical (Entity)

6. Critical/High Risk Applications and Sensitive Data

The University has adopted a security review programme based on a corrective, detective and preventative approach, aimed at controlling risks against the confidentiality, integrity and availability of information assets and services.

The aim of the programme is to minimise the impact of any vulnerabilities to proposed and current University systems and information assets that are considered to be critical and sensitive.

Examples of critical systems, data and/or applications include, but are not limited to those in the areas of:

- Payment data/applications/systems
- HR data/applications/systems
- Student data/applications/systems
- Medical data/applications/systems

For more information on how the University classifies its sensitive data please refer to the Information Asset Classification Policy .

7. Technical Security Management (TSM)

Technical Security Management (TSM) consists of ***systematic reviews and assessments*** which are carried out on a regular basis by technical teams in the Computing Services Department (CSD):

TSM activities include, but are not limited to:

- Data discovery
- Internal vulnerability scanning
- External vulnerability scanning
- Penetration testing

N.B. Automated tools and approved service providers e.g. JANET/QSA/PWC/KPMG may be appointed to undertake specialised technical reviews on behalf of the University.

Tools and approved service providers that are used to carry out these reviews and assessments will be selected in accordance with their capability in the areas of legislation, regulation, industry best practice and vulnerability identification.

8. Technical Security Management (TSM) Schedule

It is mandatory to undertake Technical Security Management (TSM) as part of risk assessment for any activity associated with University critical systems and/or sensitive data.

TSM is required to identify possible technical vulnerabilities **prior** to implementing a service as well as **during** its lifetime on a **periodic basis**.

The table below summarises the key phases, documents and timings of TSM activities that CSD activities must be adhere to at all times.

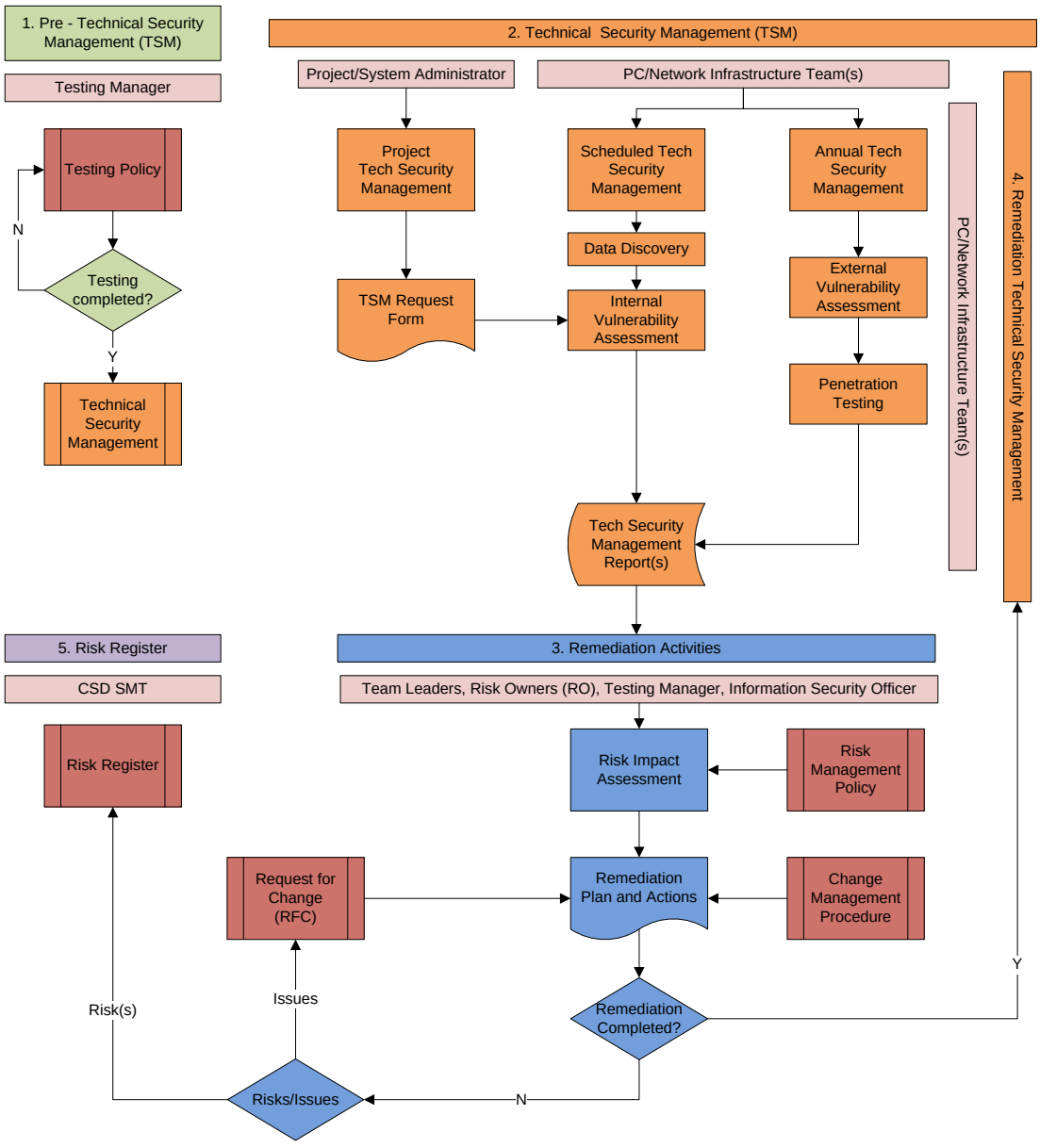
<table>
<tr><th rowspan="2">Requestor</th><th rowspan="2">Activity/Project Phase</th><th colspan="2">Technical Security Management</th><th rowspan="2">Finding(s)/Risk(s) And Remediation Activities</th><th rowspan="2">CSD Related Mandatory Reference(s)</th></tr>
<tr><th>Type</th><th>Frequency</th></tr>
<tr><td rowspan="4">Team Leader/System Administrator</td><td rowspan="3">Project TSM

Prior to “Go Live” (Proposed Services)</td><td rowspan="2">Data Discovery (PCI-DSS Specific)</td><td rowspan="2">Until all high/medium risks have been remediated and card payment details are removed and/or encrypted</td><td rowspan="2">All TSM review & assessments must be documented, recorded and communicated to the relevant CSD delegates and Risk Owners (RO)</td><td>Opportunity Assessment Document</td></tr>
<tr><td>Opportunity Lifecycle (OLC)</td></tr>
<tr><td rowspan="2">Internal Vulnerability Scanning</td><td rowspan="2">Until all High/Medium risks have been remediated</td><td rowspan="2">All TSM activities must be reviewed on a regular basis by the relevant CSD delegates and Risk Owners (RO)</td><td>Software Development Lifecycle (SDLC)</td></tr>
<tr><td>Testing Policy & Strategy</td></tr>
<tr><td></td><td>Scheduled TSM Services</td><td>Data Discovery (PCI-DSS Specific)</td><td>At least every 3 months</td><td>Any outstanding TSM activities must be acknowledged, accepted and/or transferred to the</td><td></td></tr>
</table>

PC/Network Team	During "Go Live"	Internal Vulnerability Scanning	At least every 3 months	relevant risk owners (RO) and CSD SMT	Change Management Procedure
	Annual Compliance and Monitoring	External Vulnerability scanning	At least once a year	Remediation activities must be recorded and evidenced prior to and upon completion	
		Penetration Testing			

Table 1: Technical Security Management (TSM) Schedule.

9. Technical Security Management (TSM) Process



10. Roles and Responsibilities

Testing Policy (Pre Technical Security Management)

It is the responsibility of the CSD Team Leader/System Administrator and/or those responsible for the configuration, administration and management of the critical system/data to ensure:

- All relevant testing procedures have been carried out prior to requesting Technical Security Management (TSM) input.

For more information please refer to the Testing Policy.

Technical Security Management (TSM) - CSD Project/Pre Go Live

It is the responsibility of the CSD Team Leader/System Administrator and/or those responsible for the configuration, administration and management of critical systems to request TSM input prior to:

- Significant changes/configurations to current critical systems
- Significant new services connecting to critical systems or to the core University network

The CSD Team Leader/System Administrator and/or those responsible for the configuration and management of the critical systems must submit a formal request via the CSD Service Desk.

Upon receiving the TSM request, the PC/Network team will review, schedule and undertake the requested TSM activities accordingly

When the TSM review has been completed, a copy of the TSM assessment report containing the findings will be sent to the relevant CSD Team Leader/System Administrator and those responsible for the configuration and management of a critical system

Technical Security Management (TSM) – CSD Scheduled and Annual TSM activities

The PC Systems and Network teams in CSD will ensure that scheduled and annual TSM activities are undertaken on a regular basis as part of University information security and compliance and monitoring activities.

When the scheduled and annual TSM has been undertaken, a copy of the assessment report(s) containing any findings will be communicated and made available to:

- CSD Senior Management Team (CSD SMT)
- CSD Team Leaders
- CSD Testing Manager
- CSD Information Security Officer

Remediation Activities

The appropriate CSD Team Leader/System Administrator and/or those responsible for configuration of the critical system must undertake a risk assessment to review the potential impact of remediation activities on other critical University systems, data and infrastructures.

- Any vulnerability findings must be addressed and remediated accordingly
- Any vulnerability findings that cannot be mitigated must be referred to the CSD Team Leader and CSD Senior Management Team in the first instance

- Any outstanding vulnerability findings must be recorded on the CSD risk register and, depending upon the impact, the University strategic risk register
- Any ***unforeseen issues or impacts*** may require a Request for Change (RFC). Unforeseen issues include, but are not limited to, the requirement of additional/specialist resource, software and/or hardware.

Follow-up Reviews

Once any vulnerabilities have been mitigated to an acceptable level, a follow-up TSM assessment must be undertaken to verify that the remediation activities have been completed successfully.

Any vulnerability that cannot be mitigated must be referred to the CSD Senior Management Team (CSD SMT) and relevant risk owners. It must be recorded in the CSD operational risk register and, depending upon the impact, the University strategic risk register.

11. Non-CSD Technical Security Management (TSM) Requests

CSD may undertake additional TSM activities outside of the scheduled and annual undertakings. Additional TSM activities are considered for cases involving the following factors:

- Legislative obligations
- Regulative obligations
- Contractual obligations
- Incident response activities
- Compliance and monitoring activities

Examples of Non-CSD TSM requests include:

- Non-MWS technical environments
- Technical environments managed by Faculties or Schools

Non-MWS, Faculty or School Requests

Requests must be made via the CSD Service Desk All relevant details should be supplied as part of the request: failure to provide all of the necessary information may result in a delay in the handling of the request.

Important! Resource, capacity and scheduled TSM activities will be taken into consideration prior to undertaking additional requests for individual TSM assessments.

Remediation Activities

When the TSM has been completed, a copy of the report containing the vulnerability findings will be sent to the requestor in the first instance.

It is the responsibility of the requestor to then ensure that any potential vulnerability findings which have been identified in the report are communicated to all relevant members of staff.

12. Reports and Findings - classification

All TSM and security reviews and their vulnerability findings must be treated as strictly confidential and must be restricted to the CSD department and specific University staff only.

13. Non-Technical Reviews - Gap Analysis/Audit

Non-technical reviews are known as "entity" level controls and are carried out by the Information Security Officer to ensure adherence to security policies, standards, processes, legislation, regulation and best practice across the University.

Type and Scope of Security Audits

There are two types of non-technical security audit that are undertaken across the University, described in the table below:

UoL Internal Review	Approved External Reviews
Security, Risk and Compliance	**Internal /External Audit**
This is a high level risk overview using an interview based security review which requires the input of Faculty/Professional Services managers and/or appointed delegates. The Gap Analysis/Risk assessment is required as part of the day to day compliance and monitoring and the University's Information Security Management System (ISMS) and its adherence to relevant security controls.	Internal and External audits require engagement from various stakeholders including Information Security, Faculty/Professional Services managers and/or appointed delegates along with approved and contracted external bodies. These methods of audit require approved and contracted auditors to undertake governance and assurance reviews of the University, its full Information Security Management System (ISMS) and operational security controls.

Table 2: Types of security audit that are undertaken via Information Security and CSD activities.

Scope of Audits

Scheduled security reviews and internal/external audits will be defined and agreed based on:

- Previous audit reports e.g. outstanding risks, follow-up actions and evidence of closed down actions
- Annual compliance and monitoring checks
- Security posture across the University
- Additions/changes to legislation, regulation, security policies and/or University services

Security, Risk and Compliance in Day to Day Operations

Security risk and compliance reviews are undertaken in accordance with day to day security operations of the University. The reviews include but are not limited to:

- Response to security incidents
- Third party and external party risk assessments (SPSR)
- Project assurance reviews
- Security contract and control reviews
- Security technical and activity requirements

14. Scheduled Information Security Reviews

Scheduled reviews are mandatory. The Information Security Officer, along with the relevant **Faculty/Professional Service Managers or delegates,** must ensure the relevant security reviews and internal/external audits are successfully undertaken.

15. Reports and Findings

The following tables summarise the types of TSM activities and information security reviews, resources required, interpretation of risk when undertaking a security review or internal/external audit, and the findings reports produced.

Summary Table:

Type of Review	Minimum Delegates and Resources Required	Findings Report
Gap Analysis/Risk Review	• Information Security Officer • CSD Technical Team(s) • Faculty/School/Institute Delegates **ONLY**	UoL Info Sec Internal Report
Internal Audit	• Information Security Officer • Faculty/School/Institute Delegates • Approved and contracted Internal Auditors	Independent Report
External Audit	• Information Security Officer • Faculty/School/Institute Delegates • Approved and contracted Internal Auditors • Approved and contracted External Auditors	Independent Report

Table 3: Types of reviews, delegates required and types of reports produced.

Findings Table:

Review Finding(s)	Definition of Finding(s)	(Red/Amber/Green) Risk Status
Full Conformance (FC) with industry best practice, standards, regulation and legislation	• Good security practice and controls maintained and evidenced throughout. • Comprehensive awareness and use of University Information Security Policy • Compliant and best practice implemented throughout Operation • Limited/low risk of security incident occurring, information assets are protected in accordance with legislation/regulation/contractual obligations/good practice	**Low**
Opportunity to Improve (OTI) **And/or follow up with minor remediation works that are required to ensure full**	• Good security practice in place for most activities and controls maintained and evidenced throughout. • Some awareness and use of University Information Security Policy	**Medium**

compliance with best practice industry standards	• Partial compliance throughout University operation • Mitigating controls of risks may need to be reviewed long term to ensure security incidents are limited/low risk and information assets are protected from being exposed, damaged or lost in accordance with legislation/regulation/contractual obligations/good practice	
Non-Conformance (NC) with industry best practice, standards, regulation and legislation	• Inadequate evidence /no evidence of security practice or controls maintained and evidenced throughout • Lack of awareness and use of University Information Security Policy throughout operation. • Non-compliance of legislation/regulation/security controls throughout operation. • Security Incident occurring and information assets **"at risk"** and currently being exposed, damaged or lost in accordance to legislation/regulation/contractual obligations/good practice	**Critical/High**

Table 4: Information security review findings and definitions. N.B. Specific automated security technical reports may define a risk methodology based on the different controls e.g. PCI-DSS

16. CSD Service Desk

The CSD Service Desk should be contacted in the first instance for all problems and queries relating to IT services and software. The Service Desk can be contacted using several methods including:

- The self-service portal at: servicedesk.liverpool.ac.uk
- Email: servicedesk@liverpool.ac.uk
- Telephone: 44567 (internal)
- Telephone: +44 (0) 151 794 4567 (external)

17. Security Incident Response

In the event of suspected loss or damage to University assets please refer to the Information Security Incident Response Policy.

18. Legal Obligations and University Policies

This policy is aimed at all members of the University who have a responsibility for the use, management and ownership of University assets. This policy is part of the University Information Security Management System (ISMS) and should be read in conjunction with the Information Security Policy and its sub policies and relevant UK legislation. Further relevant policies and legislation are listed in Appendix A.

19. Compliance and Monitoring

All staff and students are directly responsible and liable for the information they handle. Members of staff are bound to abide by the University IT regulations by the terms of their employment. Students are bound to abide by the University IT Regulations when registering as a student at the University.

Authorised staff members of the University may monitor the use and management of information assets to ensure effective use and to detect unauthorised use of information assets.

Appendix A – University ISMS Reference

- Regulations for the Use of IT Facilities at the University of Liverpool
- JANET Acceptable Use policy
- Information Security Policy
- Workspace and IT Equipment Security Policy
- Information Security Incident Response Policy
- Information Asset Classification Policy
- Information Security Review Policy
- IT Procurement and Third Party Security Policy
- IT Asset Disposal Policy
- Security Investigation Policy
- Procurement Policy
- Data Protection Policy
- Freedom of Information Policy
- Copyright Policy
- Card Payment Policy
- Records Management Policy
- Records Retention Policy
- Risk Management Policy
- Student/HR Disciplinary Procedures

Relevant legislation includes:

- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Data Retention Investigatory Powers Act 2014
- Counter Terrorism and Security Act 2015 (Prevent)
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002

Relevant Regulation includes:

- PCI-DSS (Payment Card Industry Data Security Standards)