Version: 1.3
Published: November 2015

Information Security Specific Policy set

These policies govern the use of specific services, solutions and systems at the Open University

Open University – Information Security Team

Information Classification: **Internal use only**

Table of Contents

Ref: P-ICP-01/19
Creation date: 23.08.2013
Review date: 22.10.2016
Version: 1.2

Information Classification Policy

Purpose

The purpose of this document is to define the classification of Open University information so that appropriate controls can be applied.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 The data owner of any information set created is responsible for assigning the appropriate data classification in accordance with this policy.

1.2 Data ownership may be transferred upon agreement with the newly identified data owner.

1.3 Open University information in any form must be managed in accordance with Information Security Policies and the Information and Records Management Policy.

1.4 Data owners are accountable for ensuring that appropriate technical controls are implemented by the Data custodian (IT designer and administrators of IT systems) to safeguard information in accordance with its classification.

1.5 Where a conflict in controls arises the most restrictive control must be applied.

Classification

Classification	**Description**	**Open University Specific Example**
Highly Restricted	Information that requires controls above those implemented by the University to manage Highly Confidential information. Typically these controls are required for data types rarely handled by the University. For example data where its loss could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. Data of this nature would require specific controls that must be supplied by the data owner, and must be adhered to by users of the information.	No normal line of business data falls into this category. Examples would include sensitive defence or medical research information.
Highly Confidential	Information that, if made public or inappropriately shared around the organisation, could seriously impede the organisation's operations and is considered critical to its on-going operations or the University's legal obligations under data protection regulations. Information may include accounting	Student personal details Staff Personnel records Some types of research data Sensitive business

	information, sensitive business plans, sensitive customer information of banks, solicitors and accountants etc., medical records and similar highly sensitive data. Such information should not be copied or sent to third parties without specific authority. Security at this level should be at the highest level for the University's normal operational requirements.	papers. Banking details, payment card details (PCI) Organisational Risk registers containing confidential information Financial records Other items covered under Data Protection Legislation. Alumni & Donor information
Proprietary	Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organisation operates. Such information is normally for proprietary use to authorised personnel only. Security at this level is high.	Unit plans Operational plans Software and configuration specifications (unless given by agreement to open source communities) Analysis of anonymised student data.
Internal Use Only	Information not approved for general circulation outside the organisation where its loss would inconvenience the organisation or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level is controlled but normal.	Most committee minutes Unit hierarchies Depersonalised student data. Copyright protected Educational Resources
Public Documents	Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level is minimal.	Marketing information Open Educational Resources Open access research data and publications. University statistic and course information intended for public consumption

Acknowledged Data Owners

Data ownership in the University is recorded by the University Secretary's Office and is described in the document "Information Guidelines, Roles and Responsibilities." Which can be found on the Information Management Services intranet site.

Ref: P-ISEP-02/19
Creation date: 23.08.2013
Review date: 22.10.2016
Version: 1.2

Information Security Exceptions Policy

Purpose

The purpose of this policy is to define how exceptions to the Information Security policies will be managed.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 Exception to Information Security policies will be considered where there is a justified requirement and the additional risk and/ or cost to mitigate that risk can be balanced with the business benefit.

1.2 For an exception to be considered an Information security policy exception request form must be completed.

1.3 All exception requests will be considered and processed by IT Information Security.

1.4 Approved exception to policy requests will be logged and regularly reviewed.

Ref:	P-ISIP-03/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Information Security Incidents Policy

Purpose

This document defines the Incident Response Policy to minimise the impact to the Open University information and Information Systems.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 All users of Open University information systems are responsible for reporting any identified information security Incidents to IT Helpdesk.

1.2 To prevent weaknesses in Open University information systems from becoming incidents, all users are required to report any observed or suspected security weaknesses in systems or services.

1.3 Network and system components must be configured to alert system administrators of security incidents as defined in the Network Configuration Standard.

1.4 An Information Security Incident Response Plan must be maintained by the Information Security Team and circulated to all relevant parties.

1.5 The Open University will maintain the capability to detect and respond to the unauthorised access, disclosure, modification or loss of information on Open University information systems.

1.6 Incidents relating to information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Password Policy

Purpose

This document defines the password policy relating to Open University information and information systems.

Scope

All users of Open University information and information systems, with the exception of mobile devices and publicly accessible, externally presented systems. For securing mobile devices, please refer to the Mobile Device Policy.

Policy

1.1 All passwords must be communicated separately from a user's Open University Computer Username (OUCU).

1.2 First time passwords must be randomly generated and changed on first use.

1.3 Where systems capable, passwords must be a minimum of 8 characters and match 3 of the following conditions: Uppercase, lowercase, numeric, and non-alphanumeric characters.

1.4 Passwords must be set to expire automatically after a maximum of 90 days, prompting the user to create a new password.

1.5 Machine to machine accounts otherwise known as Service Accounts are exempt from expiry and consequently must be a minimum password length of 15 characters and match 3 of the following conditions: Uppercase, lowercase, numeric and non-alphanumeric characters.

1.6 User accounts must be set to automatically lockout for a minimum of 30 minutes after 8 failed logon attempts. IT Helpdesk is permitted to re-enable accounts upon request.

1.7 Users should be restricted from reusing the previous 12 passwords.

1.8 Passwords should be prevented from being changed more than once in a 24 hour period.

1.9 Computers and Mobile devices must not be left unattended whilst unlocked and must be set to automatically lock after 15 minutes or less.

1.10 Passwords must not be shared, written down, recorded or printed.

1.11 The same password must not be used for multiple accounts across Open University systems.

1.12 A password must be changed immediately if it has been discovered that the password has been compromised. If this is not possible, IT Service Delivery must be notified.

1.13 Passwords for information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Ref:	P-ACP-05/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Access Control Policy

Purpose

This document defines the Access Control Policy relating to Open University information and information systems.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 Access to Open University information and information systems must be granted through the provision of a unique Username.

1.2 Users must not intentionally disclose their Username to anyone outside of the Open University.

1.3 Provisioned Usernames grant access to Open University information and information systems and are required for a user’s job role and responsibilities. Users must only access information for which they have appropriate authorisation.

1.4 IT Service Delivery will periodically review access permissions.

1.5 Public facing systems which facilitate access to Highly Confidential information will be subject to an Information security risk assessment to assess if two-factor authentication is required.

1.6 Administrator or ‘root’ access to Open University information systems will be limited to staff whose job roles require it.

1.7 Administrator or ‘root’ accounts must only be used to facilitate tasks where elevated privileges are required.

1.8 For compliance, auditing and reporting purposes the use of generic IDs that are shared and not assigned to a specific named individual are restricted and should only be provisioned after an exception request is raised and approved.

1.9 The Open University will actively monitor IT information systems for the detection and prevention of unauthorised access.

1.10 It is the responsibility of every user to report any unauthorised access to the IT Helpdesk.

1.11 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Ref:	P-MDP-06/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Mobile Device Policy

Purpose

The purpose of this policy is to define the secure use of Mobile Devices within the Open University to protect the university's information and information systems.

Scope

This policy applies to devices including but not limited to Smart Phones and Tablets, referred to herein as 'Mobile Devices', either personally owned or supplied by the Open University, which connect to the internal network or are used to access or store Open University information classified as internal or above.

Policy

1.1 All mobile devices must be secured using a passphrase, PIN number or a pattern lock which is not easily guessable.

1.2 Mobile devices must be set to erase all data after a maximum of 10 unsuccessful login attempts.

1.3 Mobile devices must not be left unattended whilst unlocked and must be set to automatically lock after 15 minutes or less.

1.4 Any security updates for the device must be applied when available.

1.5 "Jailbroken" or "rooted" devices or those mobile devices which have otherwise circumvented the installed operating system security requirements (making them vulnerable to compromise) are not permitted to connect to Open University IT services.

1.6 Information on the mobile device, including memory cards must be protected via encryption.

1.7 Only Open University authorised mobile devices used in conjunction with IT approved mobile device solutions and configurations as described in the IT mobile device standard may be used to send or store information classified as proprietary and above.

1.8 If a mobile device has been lost or stolen it must be promptly reported to the IT Helpdesk, and where necessary, IT Service Delivery will take steps to protect Open University data from unauthorised access by remotely wiping the device.

1.9 Mobile devices are not permitted to connect to the Payment Card Industry Data Security Standard (PCI DSS) segregated network.

Ref:	P-SCCP-07/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Cloud Computing Security Policy

Purpose

This document defines the policy relating to the security of cloud services including but not limited to; Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) Facilities Management (FM) solutions or Business Process Outsourcers (BPO) for the Open University.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 The use of cloud computing services to process store or transmit Open University information classified as Proprietary or above must be approved by IT.

1.2 Information processed, stored or transmitted using cloud computing services must be securely controlled in accordance with the classification controls defined within the table below.

1.3 Cloud computing services that have been approved by IT must be assigned a sponsor who is responsible for managing the relationship between the service provider and the Open University.

1.4 Prior to initiating a service, cloud computing service providers must provide assurance to the IT Information Security team that they can adequately protect and manage Open University information in compliance with Open University policies and standards.

1.5 Cloud computing service providers that are used to process, store or transmit card holder data as defined by Payment Card Industry Data Security Standard (PCI DSS) must be PCI DSS compliant. See https://www.pcisecuritystandards.org for further information.

1.6 When considering cloud computing service providers to host personally identifiable information in a country outside the European Economic Area, you must consult with the Open University Data Protection Officer.

Technical Controls

Controls	Highly Restricted (Exceptional level of sensitivity)	Highly Confidential (Very high level of sensitivity)	Proprietary (High level of sensitivity)	Internal Use (moderate level of sensitivity)	Public (low level of sensitivity)
Cloud Authentication	Mandated by the information owner	Multi factor required	Multi factor required	Single factor required	None required
Cloud Data Transmission & Storage	Mandated by the information owner	Encryption required	Encryption required	Encryption not required	Encryption not required

Ref: P-RAP-08/19
Creation date: 23.08.2013
Review date: 22.10.2016
Version: 1.2

Remote Access Policy

Purpose

This document defines the policy for remotely accessing devices connected to Open University information systems from external networks.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 Any computing device connected at an Open University site to the internal network must not be remotely accessible unless authorised by the Open University IT department.

1.2 Remote access to Open University devices will only be granted through solutions provisioned and supported by the Open University IT department.

1.3 Any IT equipment is permitted to remotely connect to Open University information systems provided it satisfies security criteria of the remote access solutions.

1.4 All computers remotely connecting to The Open University's networks must use a vendor supported operating system with up to date security patches and antivirus software.

1.5 All requests for remote access must be raised with IT Helpdesk for approval.

1.6 Open University user accounts with administrator or "root" level privileges must not be used for remote access unless specifically required for support purposes.

1.7 Tokens and/or PINs that facilitate two-factor authentication must not be stored with related IT equipment.

1.8 Remote access will be restricted to only those IT information systems or resources that users have been granted permission. No attempt should be made to circumvent any restrictions.

1.9 The Open University will actively monitor all remote access sessions for the detection and prevention of unauthorised access.

1.10 Resources that are in scope of the Payment Card Data Security Standard (PCI-DSS) require stringent security controls. Consequently remote access to PCI-DSS in scope resources is not permitted.

Ref:	P-NSP-09/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Network Security Policy

Purpose

This document defines the Network Security Policy relating to Open University information and information systems.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 All Open University network equipment must be owned and configured by IT to comply with networking configuration standards.

1.2 The connection of personal networking equipment including, but not limited to: routers, hubs, switches and wireless access points is not permitted.

1.3 Laptop and Mobile devices must not be configured and used as publically accessible internet 'Hot Spots' while concurrently connected to the Open University network.

1.4 Devices connected via a network cable to the Open University network must not be concurrently connected to any wireless network.

1.5 The Open University reserves the right to deny network access to any IT equipment that may compromise the confidentiality, integrity or availability of the Open University network.

1.6 A secure network perimeter must be maintained to protect Open University network resources from any untrusted / public networks.

1.7 Public / Internet facing Open University services must be securely separated from the internal network, only permitting the network resources required to facilitate the service.

1.8 Configuration changes to production network infrastructure must be subject to the Change Management process.

1.9 The Open University will monitor network traffic for the detection and prevention of network security incidents.

1.10 Internet services for guests to the Open University should be provisioned to be distinct and securely separate from the internal network.

1.11 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Ref:	P-DEP-10/19
Creation date:	23.08.2013
Review date	22.10.2016
Version:	1.2

Data Encryption Policy

Purpose

This document defines the Data Encryption Policy relating to Open University information and information systems.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 The Open University will provide appropriate encryption capabilities for use on Open University equipment.

1.2 Where passwords are used to secure encrypted data, users must adhere to the Password Policy.

1.3 Where a password or encryption key needs to be shared, to enable another party to access encrypted information, the password or key must be communicated separately and securely.

1.4 Any data written to portable devices and storage from Open University IT equipment must be encrypted.

1.5 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

1.6 The table below defines the minimum security controls required relative to the classification of information and should be adhered to at all times.

Technical Controls

controls	Highly Restricted (Exceptional level of sensitivity)	Highly Confidential (Very high level of sensitivity)	Proprietary (High level of sensitivity)	Internal Use (moderate level of sensitivity)	Public (low level of sensitivity)
Data Transmission	**On OU Network**: Mandated by the information owner **Public Network**: Mandated by the information owner	**On OU Network**: Encryption not required **Public Network**: Encryption required	**On OU Network**: Encryption not required **Public Network**: Encryption required	**On OU Network**: Encryption not required **Public Network**: Encryption not required	**On OU Network**: Encryption not required **Public Network**: Encryption not required
Data Storage	**On OU network**: Mandated by the information owner **3rd Party storage**: Mandated by the information owner **Portable devices & storage**: Mandated by the information owner	**On OU network**: Encryption not required **3rd Party storage**: Encryption required **Portable devices & storage**: Permitted with encryption for approved devices (See Mobile Device standard for further information) only with restrictions	**On OU network**: Encryption not required **3rd Party storage**: Encryption required **Portable devices & storage**: Permitted with encryption for approved devices (See Mobile Device standard for further information)	**On OU network**: Encryption not required **3rd Party storage**: Encryption not required **Portable devices & storage***: Permitted without encryption	**On OU network**: Encryption not required **3rd Party storage**: Encryption not required **Portable devices & storage***: Permitted without encryption

*Note that section 1.4 implements a stronger safeguard for some data types than stated in the table above to reduce the risk of incorrectly storing sensitive information

Ref:	P-MDP-11/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Media Disposal Policy

Purpose

This document defines the media disposal requirements relating to data stored on Open University information systems media including but not limited to electronic media (e.g. hard drives, USB memory sticks, memory cards, magnetic tape), optical media (e.g. Blu-Ray/DVD/CD) and hard copy .

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 Any optical media or hard copy classified as Proprietary or above must be destroyed using a shredder. Please refer to the Information Classification Policy for further details.

1.2 Where IT electronic media has been identified for disposal, the IT Service Delivery team must be contacted.

1.3 IT electronic media identified for disposal must be tracked in accordance with the Asset Management Lifecycle.

1.4 Where IT electronic media has been identified for reuse within the Open University then the re-imaging of data storage devices must be undertaken.

1.5 Where computer and portable media has been identified for reuse outside the Open University or for disposal, then a secure wipe to UK Government Communications Electronics Security Group (CESG) approved standards, must be completed by a CESG approved third party.

Ref:	P-PCP-12/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Payment Card Policy

Purpose

This document defines the Payment Card Policy relating to Open University information and information systems.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 The storage of cardholder data as defined by the Payment Card Industry Data Security Standard (PCI DSS) is strictly prohibited.

1.2 Information systems which process and/or transmit payment card information must adhere to all applicable requirements mandated in the PCI DSS.

1.3 It is the responsibility of all project managers and sponsors to ensure that projects are compliant with the PCI DSS Standard where applicable.

1.4 Wherever possible systems should restrict interfacing directly with the cardholder data environment (CDE) to limit the necessary scope of PCI DSS compliance.

1.5 Card payments may only be accepted using methods approved by the Open University Finance Division.

1.6 Each person who has access to payment card data is responsible for protecting the information.

1.7 Any suspected or actual information security breach resulting in the compromise of payment card data must be reported immediately to IT Helpdesk.

1.8 The payment card Primary Account Number (PAN), which is typically 16 digits in length, must never be sent and / or received via email or instant messaging and should be automatically detected and blocked wherever possible.

1.9 A list of all authorised devices and personnel with access to the PCI DSS in scope resources must be maintained by IT and Treasury Services Finance.

Ref:	P-VMP-13/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Vulnerability Management Policy

Purpose

This document defines the Vulnerability Management Policy for the identification and remediation of information security vulnerabilities relating to Open University information and information systems.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1. Vulnerability Assessment

1.1 Core systems and supporting infrastructure must be assessed for vulnerabilities prior to acceptance into service and on a periodic basis in accordance with the Vulnerability Management Standard.

1.2 All new externally facing websites must be approved by IT and are subject to vulnerability assurance testing prior to acceptance into service.

1.3 Existing externally facing websites that have undergone significant development changes must also be subject to vulnerability assurance testing.

1.4 Externally facing websites must be subject to annual vulnerability assurance testing.

1.5 Any software solution including, but not limited to, device firmware, operating systems, and applications must be supported by the vendor; evidenced by the timely release of security patches and upgrades.

1.6 Open University developed software applications must be approved by IT and are subject to a vulnerability assurance assessment before release into production.

1.7 Vulnerability assessments for the externally facing Payment Card Industry Data Security Standard (PCI DSS) network infrastructure must be conducted at least quarterly by an Approved Scanning Vendor (ASV).

1.8 Internally and externally facing PCI DSS in- scope devices and network infrastructure will be subject to penetration tests annually or after any significant changes.

2. Remediation

2.1 Software patches and configuration items must be applied to remediate vulnerabilities in accordance with the Vulnerability Management Standard

2.2 System and application owners are responsible for remediating identified vulnerabilities within their operational remit.

2.3 Wherever possible the ranking of identified vulnerabilities should be aligned to Common Vulnerability Scoring System (CVSS).

2.4 A vulnerability remediation schedule must be established to assist in the timely treatment of identified vulnerabilities commensurate with the criticality of the asset and the associated risk.

2.5 All remediation activity is to take place via a centrally held vulnerability register that tracks all related actions and provides an auditable record.

Ref:	P-SSDP-14/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Secure Software Development Policy

Purpose

This document defines the secure software development policy relating to Open University information and information systems.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 Where software developed for the Open University has the potential to cause business impact as defined by the Open University Risk Management Framework then development must comply with the "Secure Design and Coding Standard".

1.2 Where software development is outsourced to a third party, an Open University project sponsor must be assigned and is responsible for ensuring that this policy and the requirements from the Third Party IT Services Security Engagement Policy are implemented.

1.3 Software developers must be familiar with all relevant up to date security best practices for the programming languages and technologies used.

1.4 Bespoke University production software applications must have security defects treated in accordance with the Vulnerability Management Policy.

1.5 Software developed to process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Ref:	P-TPSSEP-15/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Third Party IT Services Security Engagement Policy

Purpose

This document defines the policy for engaging with and managing third party service providers who connect, process, store and/or transmit Open University information.

Scope

Third parties and all users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1. Engagement

1.1 All third parties working on behalf of the Open University must be assigned a project sponsor.

1.2 When engaging with a third party for the first time, a Non-disclosure agreement (NDA) must be signed before any Open University information classified as Proprietary or above is disclosed.

1.3 All third parties engaged to provide IT services to the Open University must have a commercial contract in place.

1.4 All third parties who process personal data on behalf of the University must have a data processor clause written into the commercial contract. Please refer to the Data Protection Office for further information

1.5 The commercial contract must include requirements for the third party to comply with all Open University Information Security policies and allow the Open University to immediately terminate any third party network connections in the event of a security breach.

1.6 The project sponsor is responsible for ensuring that; the appropriate agreements and contracts are in place; the third party access rights to information and information systems are provisioned in accordance with the data owner's approval; third party requirements from the Secure Software Development Policy, are implemented.

1.7 Third parties will be periodically audited by Information Security to ensure compliance to Open University security policy.

1.8 Third parties must notify the Open University of any security incidents impacting Open University information or information systems within 24 hours of the incident occurring.

2. Third Party Connections

2.1 All third party connection requests must have Project Sponsor, Data Owner, Service Delivery, Infrastructure, and IT Security level sign-off before being granted.

2.2 Where third party access is granted, connectivity will be provisioned through approved Open University solutions, restricted to the IT resources required.

2.3 Third party connections must be terminated when no longer required.

2.4 The Open University will monitor third party connections for the detection and prevention of unauthorised access.

2.5 A central register of all third party connections will be maintained by IT Service Delivery, reviewed and updated quarterly as necessary.

2.6 Third party access to information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Ref:	P-ISRMP-16/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Information Security Risk Management Policy

Purpose

The purpose of this policy is to define the information security risk management framework that must be adopted to reduce the Open University's exposure to risk which, if unmanaged could result in the loss of reputation, fines or penalties from regulatory bodies.

Scope

All users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 An information security risk management methodology must be implemented which ensures information security risk assessments produce comparable and reproducible results.

1.2 Where information security risks have been identified, a central risk register must be maintained and be subject to at least annual review by the Information Security Steering Group (ISSG).

1.3 A risk assessment schedule must be maintained by Information Security for existing IT services and systems.

1.4 New IT services and systems must be submitted to Information Security for assessment to identify if a risk assessment is required at the initiation of a project.

1.5 Risks that are identified in the risk management process must be aligned to the University's published risk tolerance threshold.

1.6 For identified risks which exceed the university's risk tolerance, a risk treatment plan must be produced that defines the appropriate responsibilities, priorities and remediation action for the management of information security risks.

1.7 Risks identified for treatment must be recorded in a central information security risk treatment log and must be subject to regular review.

Ref:	P-ASLP-17/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Audit and Security Logging Policy

Purpose

This document defines the Audit and Security Logging Policy relating to Open University information systems.

Scope

This policy applies to IT administrators of Open University core systems.

Policy

1.1 Logging of authentication and system events will be configured as described in the Logging Configuration Standard.

1.2 Access to logs and reports stored by the log concentrator must be restricted to personnel whose job role requires it.

1.3 Roles and permissions to the log concentrator must be reviewed at least annually by the technical systems owner.

1.4 The log concentrator must be secured to prevent unauthorised access.

1.5 Logs stored in the log concentrator must not be edited by any user.

1.6 Other than defined by the Data Retention Policy logs should not be deleted or moved without explicit permission from the relevant IT Head of Unit and the Information Security Team.

1.7 Log concentrator administrators must ensure that servers are configured securely and comply with Payment Card Industry Data Security Standards PCI DSS requirements where applicable.

Ref:	P-DSP-18/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

Database Security Policy

Purpose

This document defines database security policy relating to Open University information and information systems.

Scope

All users of OU information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 When using a database to store information that is classified as Highly Confidential, as defined by the Information Classification Policy, a managed enterprise class database solution must be used.

1.2 Enterprise class database solutions must be provisioned within a secure hosted infrastructure in accordance with the database configuration standard and applicable policies.

1.3 Databases must be securely maintained in accordance with the database configuration standard and the Vulnerability Management Standard.

1.4 Service Delivery is responsible for identifying and maintaining a central register of databases which store information classified as Highly Confidential.

1.5 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).

Ref:	P-SRAP-19/19
Creation date:	23.08.2013
Review date:	22.10.2016
Version:	1.2

IT Systems Rooms Access Policy

Purpose

This document defines the governance of physical access to IT systems rooms at the Open University.

Scope

This policy applies to all users of Open University information and information systems with the exception of the use of publicly accessible externally presented systems.

Policy

1.1 Core IT systems must be located in IT systems rooms, secured to provide elevated, monitored protection against unauthorised access.

1.2 Access to IT systems rooms will be restricted to staff whose job roles require it.

1.3 Third parties who require access to IT systems rooms must be accompanied by authorised personnel at all times.

1.4 The granting, changing or revoking of physical access rights to IT systems rooms must be approved and regularly reviewed by IT Service Delivery.

1.5 An access log must be maintained to record all personnel access to IT systems rooms.

1.6 Information systems which process, store and/or transmit payment card information must adhere to all applicable requirements mandated in the Payment Card Industry Data Security Standard (PCI DSS).