

Swansea University

Prifysgol Abertawe

Information Security Policy

###### 2015-2016

# Swansea University Information Security Policy Statement

Our Information security policy objective is to protect Swansea University’s computer systems and information from possible external and internal security breaches that might have an adverse impact on our operations and our professional standing.

## Principles

* All staff and students at Swansea University have an obligation to protect our information assets, systems and infrastructure. They will, at all times, act in a responsible, professional and security-aware way, maintaining an awareness of and conformance to this Policy.
* All members of Swansea University are responsible for identifying security breaches or shortfalls in our existing security practices and/or improvements that could be made.
* All members of staff and students must adhere to the Universities computing regulations and the Janet acceptable use policy <http://www.swan.ac.uk/lis/AboutLis/Comp_Regs/>
* All members who have supervisory responsibility are required to actively coach and encourage best practice amongst their supervised staff or students.
* The Registrar is responsible and accountable for ensuring that our security objective is achieved. The Director of ISS is authorised by the Registrar to pursue appropriate programmes, activities and actions that contribute to achieving our security objective and that are consistent with this Information Security Policy.
* Swansea University will ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any form of disruption or security incident to it as an organisation or to any of its locations or services.

## Applicability and Enforcement

Failure to comply with the Information Security Policy could harm Swansea University ability to achieve its mission, security objectives and damage the professional reputation of the establishment. The Registrar will be responsible for all decisions regarding the enforcement of this policy, utilising the disciplinary procedures as appropriate.

Swansea University will encourage the adoption and use of this Information Security Policy by third parties involved in joint ventures with us.

**Contacts**

 **IT Support on 5060 for all queries or incidents**

#  Security Guidelines

These guidelines set out the responsibilities of the “owners” and “system administrators” of Computer Systems: e.g. networked devices, PCs, Workstations, Multi-users systems, Mobiles, Tablets, PDAs and Servers. It has guidance on usage and configuration that departments should adhere to in order that a certain level of security can be maintained.

To achieve a reasonable secure level of operation staff should adhere to the following:-

*Guidelines for all Staff*

1. **Authorisation**. Wherever feasible, all devices must require login authorisation. All computing/communication devices must have a mechanism for authenticating its user onto the computer and hence network or wireless network.
2. **Passwords.** Passwords should never be exchanged with other users, and should never be written on easily viewable paper. Never respond to requests to verify your username and password via email or telephone. Users are advised to use passwords not found in the dictionary, passwords should be greater than 10 characters and contain at least two numeric and one punctuation character. Password cracking tools will detect words found in the dictionary even if “I”s and “O”s have been changed to “1”s and “0”s etc.
3. **Logout.** Users should logout from services each evening, power down their Computer Systems and secure their room if possible. Workstations should be locked if unattended
4. **Antivirus, Spyware and Downloads.** All University computer systems should have the latest virus detection and malware protection software installed and activated. The University has a site license for anti-virus software which is automatically installed and updated on all centrally supported desktops and E-mail services. Departments or individuals may obtain this software from the IT Support helpdesk in ISS. Files and software downloaded from the internet, including mobile code and files attached to email, must be treated with utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.
5. **Service Packs**. Staff must ensure that Firmware, Operating System and Application security service packs and updates are automatically run on their Computer Systems etc. to protect against system and software vulnerabilities. Central services, ISS managed desktops have this enabled.
6. **Data Stewardship**. Users should be fully aware of any policies pertaining to data they have access to or have created. These policies will come from Government, University, funding bodies and other third parties and will be based upon the risk assessment of the criticality of the information asset being used. These policies should then be used to drive any decision about who is permitted access to the data and where to store that data. Access to information must be relevant and not excessive as defined by the Data Protection Act and Freedom of Information Act
7. **Remote Access to Confidential or Sensitive Information.** Users accessing University information systems remotely to support business and University activities must be authorized to do so by their HOD/School. Staff may use the University VPN (Virtual Private Network) service. This makes your Computer System appear as though it’s connected to the university network, even though the connection is off campus, encrypts your data and provides authentication for certain JANET services. Details at <http://vpn.swansea.ac.uk/>
8. **Data Backup.** University data stored on University computer systems should be regularly backed up to a network fileserver and/or removable media.
9. **Encryption, Personal Devices, and Removable Media**. Removable media, such as USB keys, should be kept secure wherever possible and suitable encryption software used for sensitive or confidential data. If University data is held on personal laptops, home computers, tablets or mobiles devices it should be secured through password protection and encryption and a recent backup or synchronised copy stored on a University system in case of loss of device or password.
10. **Cloud Services.** Users wishing to use cloud services to store data owned by the University or its partners, should be especially vigilant of the Cloud Service providers’ terms of conditions. Specifically terms and conditions which allow the Service Provider to access, process or analyse data stored on their systems. Users should also be vigilant of in which country the data is stored as laws pertaining to access vary. The University has signed up to the JANET Office 365 Amendments Pack which provides a higher level of confidence that data held on the University’s “Office 365” “OneDrive for Business” service complies with UK and EU legislation – <http://office365.swan.ac.uk>
11. **Ownership and Responsibility.** For any networked or wireless IT device owned by the University or located on University premises there should be identified responsible person or persons. This will in the first instance be assumed to be the Head of Department. However in many cases this will be delegated to the local IT support person or member of staff/research officer. Staff should take all reasonable measures to secure the IT device against unauthorised access by a local/remote user or another local or remote IT device.
12. **Software Licences**. Staff should ensure that all installed applications and software that are not “site licenced” have a valid licence for that device and that the licence information is held on the School/department asset inventory.
13. **Home Wireless**. Users should ensure that home wireless networks are made secure with suitable encryption of data being transmitted from the Computer System to the wireless router and not “open” to nearby outside users who could eavesdrop.
14. **Public Wireless Hotspots**. Users should be aware that public wireless hotspots are not normally secure from eavesdropping and users should use recommended encryption software available from the service provider or the university VPN service. <http://vpn.swansea.ac.uk/>
15. **Social Networks.** Users should be aware that personal information contained in “profiles” on social networks such as photographs, date of birth, addresses etc. maybe of interest to people outside of your own “social network” and used for unlawful end. Be aware of your profile settings and availability to others.

***Guidelines for School System Administrators***

1. **Accounts.** Username accounts should not be generic unless used in a supervised area/class. Password management procedures should be put in place. Free unauthorized access to the network in public places is not allowed. Generic/shared accounts are allowed for set periods of time for supervised courses/visitors provided that access to those Computer Systems is not freely available at other times.
2. **Old Accounts**. Users who have left the University/Dept. must have their accounts removed or disabled from University services after an appropriate period, normally 3 months.
3. **Honorary and Emeritus staff.** Honorary members of staff should have a staff number through personnel and will then be able to continue using services. Emeritus staff may obtain accounts where suitable. All these policies apply to Honorary and Emeritus Staff.
4. **Backup and Business Continuity.** Computer systems and information should be regularly backed up to disk and/or tape. Extra backup copies should be stored offsite. Offsite storage should be secure as media could still be readable. System administrators of critical systems should adopt a comprehensive backup policy, ISS can advise on a suitable backup routine and location for backup media. The University’s Disaster Recovery Policy covers circumstances and actions for the more serious potential loss of information.
5. **Retention of Documents.** The archiving/retention of documents, research data, email etc. must take into account legal, funding body, regulatory and business requirements. The period of retention for a record series will be determined by the retention criteria which are:
	* Administrative need. For example subject files and correspondence files, have a clear lifecycle beginning with their creation, current use, semi-currency when they are referred to less and finally to non-currency when they have been superseded by new information and can be confidentially destroyed.
	* Statutory requirement. Many record series exist within a statutory framework where specific legislation determines a minimum period in which the information must be kept, for example the Companies Act 1985, the Finance Act 1985 and the Taxes Management Act 1970 set minimum retention periods for a range of financial records. There will also be instances where the University will retain records to defend itself against potential civil actions and certain retention periods will then be determined by reference to the Limitation Act 1980, the Latent Damage Act 1986 and other relevant legislation.
	* Retention Schedule. An agreed retention period, and the criteria on which the retention period is based, will need to be agreed with the "data owner" and communicated to technical, academic and administrative staff as appropriate. The retention period starts from the last entry in the record, for example from file closure.
	* Disposal. At the end of the retention period the records should be assessed to ensure whether changes in legislation, particular disputes,claims and enquiries require extended retention. If the retention period remains valid the records will be appraised for their historic value in accordance with the University’s archive collection policy. All records not retained as archives will need to be confidentially destroyed.
6. **New Systems and Services.** Schools should consult ISS before considering purchasing server hardware as central services can offer virtualized servers hosted in a secure environment that Departmental/School staff can be trained on to administer.
7. **System Administrator.** School/dept. staff who have system administrator responsibility should have suitable training and consult with ISS staff prior to configuration to enable correct integration with existing services. ISS can also advise on general support issues such as username control, virus protection, backup routines and maintenance. Heads of School and administrators must ensure that more than one employee has administrator privileges and experience to operate and maintain critical services. Documented procedures should exist where reliance is placed upon one member of staff. In some circumstances, ISS may be able to help with short-term advice and support.
8. **Server Consoles and System Passwords**. Server consoles must be kept in secure locations, System admin passwords should only be known by trusted personnel.
9. **Unlawful Material**. Data owners and system administrators must ensure that data held on workstations and servers is lawful and has no links to unlawful material. The University reserves the right to bar access to information servers containing material considered illegal or likely to bring the University into disrepute. Personal information or material held on information/web servers must be relevant to or associated with the information owner’s authorisation to use University IT facilities.
10. **Computer Hardware Refresh and Disposal.** Computer Systems that are no longer suitable for use should have all data/software removed and disks destroyed and disposed of following Waste Electrical and Electronic Equipment guidelines. Data can easily be retrieved from old disk drives. Old Computer Systems can be recycled, donated to charity or sold to staff providing security/data removal guidelines and software licencing laws are followed. The current replacement lifecycle of Computer Systems is approximately 4 years for business and student applications.
11. **Regulation of Investigatory Powers and Data Protection Acts**. System administrators must be aware of the Regulation of Investigatory Powers Act 2000 when monitoring information flow through computers/networks and of the Data Protection Act 1998 if personal data is being processed. The University Data Protection officer should be notified and consulted as required.

<http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1>

<http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1>

1. **Licenced Software.** Owners and system administrators must ensure that all software is licensed for use. ISS IT Support will advise on campus wide licenses. A named individual in departments should keep an annual inventory of all networked and standalone software in use on their systems, a copy of the licence and proof of purchase.
2. **Security Patches**. Operating systems must have the recommended security patches installed. ISS will advise and recommend host firewall or intrusion detection software which may be installed. Systems which are not administered properly can create a security loophole for would-be hackers: these systems may be disconnected from the network.
3. **Data Security Breach.** If a data security breach is suspected or is known to have occurred staff should immediately contact IT support or, depending upon the severity or confidentiality, the ISS Director, or Deputy Director of ISS who will initiate the appropriate action.

# Network Connection Policy

**Network Connection Policy**

The ISS Network Team is responsible for the management of the campus network and all external connections and applications that use the Internet. ISS, in liaison with departmental staff, administer and maintain the integrity of this network to enable the smooth operation of the many and varied applications. To prevent any one person/device compromising the integrity of the network it is mandatory that all departments adhere to the following procedures.

## Network Connection Rules – call IT Support - telephone 5060 for assistance.

1. New network wiring must be approved by the ISS network team and use Estates recommended installers.
2. Departments must not add or remove sections of the network without permission from ISS.
3. Wireless networks must not be installed without ISS approval. The University has a comprehensive wireless network and authentication system covering 100% of university buildings and Halls of residence.
4. Computers or network devices must register their MAC address (a unique identifier associated with that device) with ISS or the department delegated authority to obtain Internet name and address, sometimes referred to as the IP address.
5. Computers must be registered within IPDBASE (in house database of all computers at Swansea administered by ISS) and preferably use DHCP (Dynamic Host Configuration Protocol) to obtain Internet parameters from the network.
6. Prior consultation is needed with the ISS Network Team where a new server or service requires large amounts of bandwidth from the local network, the PSBA or JANET.
7. Prior consultation must take place with ISS if the network is to be used for other services such as control systems, security etc.
8. Prior consultation must take place with ISS Systems team if a department wishes to set-up a new Microsoft/Novell/other computer network domain.
9. Mini networks should not be created by University staff and students without prior consultation with ISS networking staff.
10. ISS reserves the right to disconnect computers that compromise the integrity of the network.
11. Legal peer to peer and limited gaming use is allowed but bandwidth usage will be monitored and reviewed as appropriate.

## Actions following a suspected network attack

Several times a day, the University’s computer systems are scanned by possible intruders for potential security weaknesses. If a security loophole exists there is a high risk that it will be exploited and the end system or network compromised. There is also the possibility that an attack could originate from Swansea and that the University must take immediate action to isolate and identify the attacker.

Swansea University will, to the best of its ability, take strenuous measures to prevent any IT device either owned by the University or located on premises of the University being used to attack any other IT device anywhere in the world. If an IT security breach is traced to the University, then the University should be able to trace the IT security breach to an individual device and an individual user or group of users of that IT device.

The ISS network team will monitor network activity and respond immediately to any security breaches and liaise with departmental IT support and the national CERT (Computer Emergency Response Teams) to identify the source and rectify the problem. ISS will periodically scan the SU network resources and inform departments if vulnerabilities are found. In doing this, ISS staff will adhere to Data Protection and Regulatory Investigative Powers guidelines.

If a department suspects that a security breach has occurred they should immediately contact IT support or, depending upon the severity or confidentiality, the ISS Director, Deputy Director of ISS or head of Networking who will initiate the appropriate action.

The ISS Network/CERT team may take all reasonable steps to limit the damage of the attack these may include:

* Swansea University network maybe disconnected from external networks.
* Network partitioning. Sections of the network maybe disconnected from the campus backbone while the problem is isolated.
* Computer systems found to be the source of an attack, or acting as an intermediary, will be disconnected until the problem is rectified.
* Prevention of applications using the network/Internet, such as e-mail, while the problem persists.
* Unauthorised activity by local users may be logged. Persistent misuse of University computing facilities will lead to access to these facilities being withdrawn.

# Security Firewall Policy

## Introduction

Swansea University has a single 1 Gigabit connection to the Internet via the PSBA Public Sector Broadband Aggregation network (a network which links all public sector services in Wales to JANET and the Internet). Security access to and from the University is controlled through this single connection point.

Security Firewalls are used to control access between networks. These can range from powerful computers, which check the validity of every fragment of information, to more generic allow/deny connection rules maintained as access lists within network equipment. Network security cannot be guaranteed by installing dedicated security firewalls alone. Access control is only one part of a much wider overall Information Security Policy. An Identity policy (accounts, passwords) and user awareness training are fundamental to overall security.

## Firewall Policy

1. Perimeter firewalls.

External firewalls are located at the border between SU and the Internet. Packet inspection is used to detect denial of service attacks and port attacks.

The perimeter firewall by default denies access to all services and ports apart from those specifically allowed. Requests to open up specific ports need to be agreed with the network team.

Bandwidth usage is monitored and controlled to reserve capacity for priority applications.

1. Virtual LANs - VLANs

Each department is allocated to a virtual network which is location independent, i.e. a computer can be connected anywhere on campus but still part of a departmental network, firewall rules can open or block traffic between VLANs as required.

1. Host and desktop system firewall

Security firewalls installed on either host, desktop or laptop systems to check and log all incoming connections and disconnect as appropriate.

# Security of Electronic Mail Services

Users of e-mail must adhere to the Universities computing regulations and acceptable use guidelines and in particular they must not send:

* Bulk and unsolicited e-mail (advertising, sometimes called spamming) to recipients off campus and not related to University business
* Defamatory, or libellous E-mail
* Spoofed e-mail (sending e-mail with a forged sender address) and chain e-mail
* Text or images to which a third party holds intellectual property rights, without the express permission of the right holder
* Material that contains personal data and contravenes the Data Protection act.
* Offensive e-mail such as material which is sexist, racist, homophobic, xenophobic, pornographic or paedophilic

These actions could have serious implications for the sender and result in SU being blacklisted by ISPs around the world. SU subscribes to Real Time Blacklists, this is an active list of banned e-mail servers around the world. SU also operates its own blacklist of E-mail servers, which is updated on request from members of staff who are being targeted.

Incidental and personal use of the E-mail facility is permitted providing it does not disrupt or distract the individual from the conduct of University business or affect other users of the system.

Privacy of e-mail will be respected and interception will follow the guidelines of the RIP Act. In most cases intervention by e-mail administrators to fix a problem will only necessitate seeing the address headers of e-mail messages.

SU operates many internal E-mail lists and staff may subscribe to many external e-mail lists. Users are expected to adhere to a certain level of e-mail etiquette when using these lists. The SU staff e-mail list has a particular set of guidelines.

#