Information Security Framework

THE UNIVERSITY OF WARWICK

Working Practices for Protecting Electronic Information

1. Purpose

The following pages provide more information about the minimum working practices which seek to ensure that the University's electronic information is kept safe. We will all follow these working practices to play our part in the shared responsibility for protecting electronic information and to comply with the requirements of University Regulation 31 governing the use of University computing facilities.

The minimum mandatory working practices below are presented in ***boxed text*** to distinguish them from recommended practices and cover the following areas:

- Passwords
- Basic Computer and Internet Safety
- Use of Personal Computers/Devices for University information
- Electronic Information Asset Protection
- Third Party Access and Outsourcing
- Information Security and Systems Development

2. Passwords

The use of passwords helps to control the risk of unauthorised access to University information. However, the use of public computers or internet services presents a threat as usernames and passwords could be stored or shared inappropriately, and sometimes without your knowledge. Whilst nothing can absolutely guarantee the security of passwords, the following working practices will help minimise this risk by increasing password security.

Everyone will use passwords/PINs as a first-line security control on ALL devices (e.g. PCs, laptops, smartphones) processing University information and will not share these details with anyone.

University IT Services will never ask for your password and neither should anyone else. If someone asks you for your password, you can politely say no.

Everyone will create passwords adhering to the minimum password standard for University information and systems:

- ***Easy to remember (i.e. doesn't need to be written down) but difficult for others to guess***
- ***Longer than 8 characters – the longer the better!***
- ***Contain one character from the following: numbers, letters in uppercase, letters in lower case, symbols such as £$%^&****
- ***Changed immediately if you suspect someone knows it*** *(some corporate information systems (PSe, SITS) will require a frequent change as part of usual practice)*

Don't use your University username and password as login details for other accounts. *This is to limit access to systems and exposure if your University account is compromised. Same applies to any other passwords you have!*

Use the IT Services 'Change Password' tool to reset your password - warwick.ac.uk/passwords
This includes a check against the University minimum standard above.

Passwords for files or devices must not be sent with the file or device. You will communicate the password via another mechanism e.g. by email, text or phone. Passwords for protected email attachments must never be sent in the same email as the attachment.

IT Application Administrators will be responsible for the appropriate application and management of password controls (based on the classification of the information)

In cases where Reserved[1] information is being used, it may be appropriate to use a password which is longer, more complex or changed more frequently (or all three aspects) than the University minimum standards. This is for the individual or team to determine based on the potential level of impact caused by its disclosure or the likelihood that it could be targeted.

3. Basic Computer and Internet Safety

We will take the following steps to protect our computers from threats as well as protecting ourselves and our information when using the Internet:

Computer Safety

Always lock your computer screen when you leave your desk (On Windows <Ctrl><Alt><Del> then <Enter> (or <Windowskey><L>))

Be careful entering login details in public places – you don't know who may see

Always log off computers in public areas, such as meeting rooms or training rooms, after you have used them

Don't click on links or respond to emails from unknown people asking for your personal or login details

Make sure your computer has acceptable anti-virus and firewall software installed and install regular updates to maintain a high level of protection. *IT Services provide further information warwick.ac.uk/software/antivirus and will manage this for ITS managed computers. Responsibility for ensuring appropriate protection for locally managed IT equipment (including laptops) lies with the Head of Department.*

Install software updates quickly. *You will be prompted to do this on ITS managed computers and it is advisable that you set your personal computer up to install updates automatically or at least prompt you that updates are ready to install.*

[1] Refer to the University Information Classification and Handling Procedure for more information: www.warwick.ac.uk/services/gov/informationsecurity

Internet Safety

Don't access your University email or other important information from a shared computer or over wireless networks you don't know. It is easy for your details or information to be copied, shared or left behind without your knowledge

Before you submit any of your personal info online, make sure the website you are using is legitimate and won't use the information for anything harmful

Don't allow your internet browser to remember your University login details

Only install the software you really need and buy direct from reputable companies; never install browser software provided via a website pop-up or email

Make sure you are aware of the JANET Acceptable Use Policy. *JANET is the University's internet provider and has specific conditions of use. IT Services provides further details on the use of University networks*
warwick.ac.uk/its/servicessupport/networkservices

The following symptoms can indicate when there is a problem with your computer:

- slower than usual performance (generally or when using particular applications);
- unwanted pop-ups, additional requests to login or unusual error messages where messages did not appear before

If you suspect that your work computer has been tampered with, you must contact IT Services helpdesk@warwick.ac.uk or ext 73737

4. Use of Personal Computers/Devices for University information

We recognise that staff and students will at times use their personal computer and devices to access and process University information. See section 6 of University Regulation 31 governing the use of University computing facilities

Individuals will manage the risks associated with the use of a personal or shared computer or device for University information

You are responsible for the protection and secure disposal of Restricted or Reserved Information[2]

In addition to meeting the minimum requirements for computer safety and internet browsing above:

- ***Use secure means to access University information (e.g. Virtual Private Network, myfiles, Files.Warwick, Sharepoint or other, similar University provided facilities)***
- ***Do not store local copies of Protected, Restricted or Reserved University information - see below for storage procedures***
- ***Delete your browsing history from shared personal computers to remove any cached session details***

[2] Refer to the University Information Classification and Handling Procedure: www.warwick.ac.uk/gov/informationsecurity

5. Electronic Information Asset Protection

Everyone will take an active role in identifying risks to University information assets[3] within their areas and protecting them as far as can be reasonably expected.

You must not store University information on local computer drives (desktops, C or D drives) as these are not backed up and loss/failure of the computer will mean that the information may not be recoverable or available as required to undertake your activities.

You must only store Protected, Restricted or Reserved information[4] in secure, access controlled and backed up locations (your H: drive, departmental shared drives, encrypted USB or other University provided facility appropriate for the task) to ensure it is available when required and protected from loss, theft or alteration. If these are not suitable for specific reasons or you need help, please seek advice from the IT Security Service *(helpdesk@warwick.ac.uk)*

Everyone will handle Restricted and Reserved information in line with the University Information Classification and Handling Procedure, to reduce the likelihood of security incidents and the resulting impact on confidentiality, integrity and availability of University information assets.

Everyone will seek advice from the Institutional Resilience Team if unsure (informationsecurity@warwick.ac.uk)

As set out in the Information Security Framework, all information assets must be owned by an Information Custodian – a senior individual with management responsibility for controlling the production, development, maintenance, use of, access to, retention, security and destruction of a specific information asset or group of assets.

Information Custodians should ensure that the electronic systems containing Restricted or Reserved data for which they have management responsibility are subject to periodic penetration testing and vulnerability scanning[5] to identify new risks and to check the effectiveness of existing controls. This will be handled by IT Services for centrally provided services, such as departmental shared drives and H: drives. Advice on testing can be given by IT Security Team in IT Services for electronic systems (helpdesk@warwick.ac.uk).

Heads of Departments will maintain a list of systems (e.g. shared network drives, local admin databases) under their control that contain Restricted or Reserved information and are responsible for ensuring access is restricted to only those with appropriate authorisation.
Heads may delegate the operational responsibility to a named representative but remain accountable for ensuring these obligations are met.

The above responsibilities of Information Custodians and Heads of Departments include ultimate oversight of who has access to information assets and/or to information within their management responsibility.

[3] Defined within the Information Security Framework as a useful or valuable store of information or information processing system of any type or format.

[4] Refer to the University Information Classification and Handling Procedure: www.warwick.ac.uk/gov/informationsecurity

[5] Both are periodic tests of systems to highlight weaknesses and potential security risks. A vulnerability scan looks for known vulnerabilities in a system (e.g. SQL injection attacks, session hijacking, cross-site scripting) and reports potential exposures. A penetration test is designed to exploit weaknesses in the system architecture or computing environment.

Good practice would be to formally review the processes for granting access and the currency of those individuals with access annually and whenever there is a change in the classification of the information. This is to ensure that those with access still have a valid need to access the data. There should be an evidenced authorisation mechanism to set up new users and remove leavers consisting of approval of an access request and authorisation by a named individual with responsibility for the system concerned.

Heads of Departments, Information Custodians and IT Services will ensure information assets (electronic; fixed or removable) within their care or control are protected from damage, unauthorised access or disruption.

University and departmental Business Continuity Plans should include contingency or alternative arrangements for vital information assets supporting critical activities. Significant departmental risks, either specific to information assets or arising from vulnerabilities in systems, should be included within departmental risk registers and appropriate measures should be put in place to manage the risks.

- You may find this guidance and template useful when carrying out a risk assessment

Where identified information security risks pose a significant concern to the University (operationally or strategically) and/or cannot be managed effectively at departmental level, Information Owners, IT Services and Heads of Departments will escalate these to the Institutional Resilience Team *(informationsecurity@warwick.ac.uk).*

6. Outsourcing and Third Party Access to University Information Assets

Outsourcing

The University provides 'approved' IT facilities and services. These are defined as provided directly by University staff and facilities or those provided by a third party on behalf of the University and subject to a formal legal contract and/or service level agreement.

We acknowledge that staff and students are able to access unapproved IT facilities, mostly available via the Internet, provided by third parties with which the University does not have any formal agreement. Examples of this are the use of Google Docs, DropBox and Hotmail/Gmail. The University has issued specific guidance on the use and selection of Cloud services.

Users signing up to the terms and conditions of informal IT facilities do so at their own risk. There are potential risks associated with using informal IT facilities including a lack of knowledge and control over:

- Who may have access to user data
- How user data is used
- Where user data is stored
- How securely user data is stored
- How viable the facility will be in the long term
- Whether user data will be recovered in the event of a disaster
- How much support will be provided in the event of a problem

Non-approved IT services and facilities will not be used for Protected, Restricted or Reserved University information[6] or for processing similar information on behalf of a third party.

[6] Refer to the University Information Classification and Handling Procedure: www.warwick.ac.uk/gov/informationsecurity

Prior to seeking approval for a non-University approved IT facility or service for processing of Protected, Restricted or Reserved University information, a formal risk assessment will be undertaken by the Department to ensure that the processing will take place securely, that the relationship will not give rise to any further risks for the University (e.g. reputational, financial or legal risks) and that the impact of any disruption or problem caused by or affecting the third party is clearly understood. *Please contact the Institutional Resilience Team via informationsecurity@warwick.ac.uk for help.*

- *You may also be interested in reading How do I choose a supplier or service provider?*

Third Party Access

The appropriate Information Custodian will be accountable for ensuring that risks are identified and managed where University information is to be accessed or handled by third parties. This is to protect the interests of the University and continue the safeguarding of University information in line with our legal obligations.

A named University staff member (or named members) will be accountable for managing the access provided to a third party and their activities on the network. The named University individual(s) will ensure that obligations around acceptable use and event record keeping are understood by the third party prior to access being granted.

IT Services can advise on the standard event logging requirement to comply with our obligations under the JANET Acceptable Use Policy. [7]

Third party access (physical or logical) will be strictly controlled and must only allow access to information or systems necessary to carry out the agreed activities. This is to reduce the risk of disclosure or theft of University information, theft or damage to equipment (intentional or accidental) or misuse of information or facilities.

Temporary Guest access to University network will be approved and facilitated by IT Services (helpdesk@warwick.ac.uk)

7. Information Security and Systems Development

Development and test systems and data must be kept separate from live systems and data; live data must not be used for testing or development.

As part of the requirements gathering and testing process for new or changes to existing systems, project executives[8] will liaise with the Information Custodian, IT Security and the Institutional Resilience Team via informationsecurity@warwick.ac.uk. This is to allow for potential threats and concerns to be identified to assure that the information held or to be held in the system can be properly secured.

For example (but not limited to), applications must be able to demonstrate appropriate prevention of SQL injection attacks, session hijacking, cross-site scripting and information leakage.

[7] https://community.ja.net/library/acceptable-use-policy

[8] Developers, Project Managers, IT Service Analysts, Business Analysts or local IT/project leads

Document History

13	May	2013	J. Findlay	Created document with comments from Dr Duncan Hine (WMG, Cyber Security specialist), Verification Group members and Head of Service Development (ITS), Senior Assistant Registrar (Governance, Risk and Continuity) and Head of Institutional Governance Services (v1)
20	May	2013	J.Findlay	Comments incorporated and approved for release by the Director of Campus Services and IT (v1.1)
2	Sept	2013	J.Findlay	Minor amendments to update password length protocol and to feed in revised info classifications (restricted and reserved) (v1.2)
08	Jun	2017	S Cooke	Updated department names and hyperlinks as part of annual review. Approved for release by Head of Institutional Resilience (v1.3)

The official version of this document will be maintained online. Before referring to any printed copies please ensure they are up to date.

Next Review

Summer 2018