Information Security Controls Policy

Version 2

Version:	**2**
Dated:	**17 September 2019**
Document Owner:	**Head of IT Security and Compliance**

Document History and Reviews

Version	Date	Revision Author	Summary of Changes
0.1	May 2018	Ali Mitchell	New policy
0.2	May 2018	Ali Mitchell	Added in sections on responsibilities and advice and support
0.3	May 2018	R Platt	Amendments in line with other IG policies
1	May 2018	Ali Mitchell	Approved Version
1.1	April 2019	Ali Mitchell	Links added to paragraph 5 and removed Data Protection policy. Included reference to the Information and Governance and Security Policy and Data Breach Policy.
1.2	July 2019	Ali Mitchell	Removed last sentence in paragraph 1.1. Added in reference to IT Security and Compliance team to paragraph 4.1. Changed paragraph 6 from advice and support to policy requirements. Paragraph 7 renamed from Principles and Objectives to Policy Principles
2	Sept 2019	Ali Mitchell	Various changes made, links added and general formatting.

Review Distribution

Name	Title
Rhiannon Platt	Information Governance Manager and Data Protection Officer
Ian Tilsed	Assistant IT Director (Strategy and Architecture)
Mike Maling	Operations and Security Manager

Approval

Version	Approval	Date
1	Members of the IGSSG	May 2018
2	Members of the IGSSG	Sept 2019

1. Introduction

1.1 This policy is based upon the ’10 steps to cyber security’, originally published in 2012 and promoted by the National Cyber Security Centre (NCSC) as an effective method to protect organisations from cyber-attacks. The ’10 steps’ provide a framework that can be used to establish policies and controls within the University to mitigate information and cyber security risks.

2. Purpose

2.1 This policy sets out high-level objectives that demonstrate the University’s approach to a number of key areas in information security. It also provides a baseline framework upon which a range of technical controls can be built and maintained.

3. Scope

3.1 This policy applies to all Information Technology (IT) systems owned or managed by the University. The term ‘information system’ will be used to denote any such system typically involving hardware and software components. This policy and the controls contained within apply to all members of the University.

4. Implementation

4.1 The principles and objectives outlined in this policy will be implemented through an evolving framework of security controls based on current industry best practice and guidance, as published by the NCSC. To support this methodology, the University’s IT Security and Compliance team will review new information system designs and make recommendations for additional technical security controls to be used in order reduce security risks.

5. Responsibilities

5.1 The University will take the appropriate measures to ensure security and privacy by design and to protect all University information assets. The following roles explain the responsibilities for staff engaged in procuring new information systems.

5.1.1 **Project Managers**
It is the Project Manager’s (PM) responsibility to ensure these ‘10 steps to cyber security’ are included in the planning of any new system and that a Data Protection Impact Assessment (DPIA) has been completed before the information system has been designed and gone live. The PM will engage with the IT Security and Compliance team during the early planning stages of setting the project plan to ensure suitable resources are available. PMs must also ensure the project has included budget for security penetration testing.

5.1.2 **Business / Information System Owner’s**
It is the Information System Owner’s responsibility to ensure these ‘10 steps to cyber security’ are being implemented from the offset when any new systems are being designed. They are responsible for ensuring compliance with the 10 steps and this policy is maintained throughout the system lifecycle. They are also responsible for ensuring a DPIA has been completed and reviewed by the Information Governance and IT Security and Compliance teams and also the relevant Information Asset Owner.

5.1.3 **Information Asset Owner (IAO)**
The IAO is responsible for ensuring their data is held in systems that have a DPIA and are included in the University Information Asset Register. IAOs are also responsible for ensuring there is an appropriate level of compliance and security on systems that hold their information assets and must report any concerns to the Information Governance office at

dataprotection@exeter.ac.uk. Any occurrence of data breaches must be reported to the Student Information Desk (SID) as soon as the breach has been discovered.

5.1.4 **Senior Information Officers (SIO)**
Director of College Operations and Directors of Professional Services have the responsibility of overseeing compliance and developing good data protection practice within their designated areas. They should ensure any new processing of personal data has appropriate security controls in place and is compliant with this policy.

5.1.5 **Exeter IT Business Partners**
The Exeter IT Business Partners are responsible for supporting designated areas with the requirements for new IT systems and liaising with relevant subject matter experts to ensure the University has secure and compliant systems. Refer HERE for more information.

5.1.6 **IT Security and Compliance** Team
The IT Security and Compliance team is responsible for informing and advising on technical and cyber security controls and providing advice regarding the technical aspects of a DPIA and how to ensure systems conform to the 10 steps. Depending on the value of the data being processed in the new information system additional security controls can be imposed which are often referred to as either non-functional requirements or technical security controls. They are also responsible for reviewing DPIAs and conducting third party assurance assessments for existing legacy information systems.

6. Policy Requirements

6.1 University staff (including associates) are required to engage with one of Exeter IT **Business Partners** (ITBPs) before purchasing either a new information system, software or storage platform. The ITBPs are there to be the linkage to the Exeter IT team and to support and help determine the requirements for the new system. The ITBPs will ask staff to complete an 'Idea Creation' form which will help Exeter IT to start visualising your requirements and the compliance and security controls that will need to be designed to keep information and data safe and secure.

6.2 In line with capturing a new idea, staff are also required to complete a Data Protection Impact Assessment which will aid in the identification of potential security and compliance risks. For further information see the DPIA Policy or contact the Information Governance Office dataprotection@exeter.ac.uk

7. Policy Principles

7.1 In order to ensure a new information system has been designed with security and privacy measures from the offset, the following '10 steps' must be applied. These requirements outline the high-level security controls and standards that are required when new University information systems are being designed.

The 10 Steps

Secure configuration

Establishing and actively maintaining the secure configuration of systems is a key security control. Vulnerabilities must be rectified; this should usually be done by regular patching. Systems that are not effectively managed will be vulnerable to attacks that may have been preventable.

Network security

Networks need to be protected against both internal and external threats. This is usually done by ensuring compliance with University policies and having appropriate architectural and technical

controls in place. Failing to protect University networks appropriately will leave the estate vulnerable to a variety of attacks.

Managing user privileges

The University should understand what level of access employees need to information, services and resources in order to do their job otherwise it won't be possible for those responsible to manage user rights effectively.

All users should be provided with a reasonable (but minimal) level of system privileges and rights needed for their role. The granting of highly elevated system privileges should be carefully controlled and managed.

Failure to manage rights effectively leads to a number of risks including privilege misuse, increased attack capability, and the ability to negate existing security controls.

User education and awareness

All University members have a critical role to play in helping to protect the organisation, but this should not affect their ability to perform their role. All staff are required to complete the Information Governance mandatory training.

Bespoke training, guidance and documented procedures should be in place for all systems that are system specific. Additional training and/or guidance must be in place for those with elevated system privileges.

Failure to effectively support users with the right tools and awareness may leave the University vulnerable to risks such as legal and regulatory sanction, non-reporting of security incidents, and external attack.

Incident response and management

Security incidents will inevitably happen and will vary in their level of impact. All incidents need to be managed effectively, particularly those serious enough to warrant invoking business continuity or disaster recovery plans.

The University will develop its incident management capability to detect, manage and analyse security incidents in line with supporting policies.

For more information see the *Data Breach Policy*

Malware prevention

Malware (malicious software) can cause material harm to systems, including disruption of critical business systems and unauthorised export of sensitive information or data loss. The range of technologies used to introduce malware span the entire infrastructure, and the risk of attack is wide and varied. The risk may be reduced by following the *Anti malware policy* and implementing appropriate anti-malware controls within each system as part of an overall 'defence in depth' approach.

Monitoring

Monitoring provides the means to assess how systems are being used and whether they are being attacked. Without the ability to monitor our systems we may not be able to detect or react to attacks, or to account for activity.

Removable media

Removable media introduces the capability to transfer and store huge volumes of sensitive information as well as the ability to import malicious content. Failure to apply any controls to removable media could expose the University to the risks of information loss, introduction of malware, and reputational damage.

Staff should take additional care with any removable media which carries greater risk than information held on the University network and ensure they comply with the Portable and Removable Media Devices Policy. Any loss or compromise of removable media that holds University information should be reported in line with the Data Breach Policy.

Mobile and remote working

Mobile working and remote access extends the transit and storage of information (or operation of systems) beyond the University infrastructure, typically over the internet. Mobile devices will also be typically used in spaces that are subject to risks such as oversight of screen, or theft/loss of devices. As such the University must establish sound mobile working practises to mitigate against these risks. Staff must ensure compliance with the Remote Access Policy.

Personally enabled devices

The University recognises the need for flexible working practises amongst a diverse workforce. However, ineffective management of unmanaged devices may lead to unauthorised access to sensitive business or personal information, or compromise of internal infrastructure.

Staff must ensure compliance with the Bring Your Own Device Policy and remember that the loss of a personal device may also result in the loss of University information and therefore may require reporting in line with the Data Breach Policy.

8. Policy Deviations

8.1 Any information system that has not been designed with security and privacy in mind will be treated as an information risk and if a DPIA has also not been completed then there is a strong possibility that the system will not be able to go live.

9. Related Policies and Documents

- Laptops Encryption Policy
- Data Breach Policy
- User Management Policy
- Encrypted USB and Hard drives recommendations
- Portable and Removable Media Devices
- Mobile and Remote Working Policy
- Bring Your Own Device
- Password Security
- Information Governance and Security Policy
- Anti-Malware Policy
- Viruses and Malware Protection Guidance
- Data Protection Impact Assessment Policy
- iPad and iPhone Security

10. Related Policies and Documents

10.1 Further advice is available from the IT Security and Compliance team, please email itsecurityandcompliance@exeter.ac.uk