Security Update and Patching Policy	
Operational Owner:	Sam Wong, Head of IT Security
Executive Owner:	Mary Hensher, Chief Information Officer
Effective date:	01/02/2019
Review date:	01/02/2020
Related documents:	

Approval History

Version	Reviewed by	Reason for review	Approved by	Date
v0.1	N/A	First draft	ISAGG Chair's Action	12-3-19

1. Introduction

1.1 Purpose

1.1.1 This policy stipulates and governs the way the University applies security updates and patches on managed IT systems. The policy focuses on the security standards maintained throughout the operational lifetime of the technology of concern. University data is a critical asset and must be protected from the consequences of breaches of confidentiality, failures of data integrity and interruptions to its availability.

1.2 Scope

1.2.1 Technology: This policy applies to all University IT systems managed by the University's IT Services Department, including (but not limited to) physical and virtual servers, infrastructural services, appliances, applications, end user computing devices, network infrastructure, and automated configuration deployment systems.

1.2.2 Unmanaged devices are not in scope e.g. Bring-Your-Own-Devices (BYOD).

1.3 Definitions

Term	Definition
ITS	IT Services Department
Relevant IT team	The IT team best suited for supporting the application of security updates and patches on a particular piece of technology
TCR	Technical Change Request
PCI DSS	Payment Card Industry Data Security Standards
CE	Cyber Essentials
DSP	Data Security and Protection Toolkit (NHS data)
Compensating Controls	Technical security controls, ratified by the ITS IT Security team.
BYOD	Bring Your Own Device. For example, personal computing devices

2. Policy Principles

2.1 Responsibilities

2.1.1 It is the responsibility of all University of Surrey staff and all applicable external support services, who have the role of managing IT equipment and technology to adhere to this policy and follow all applicable standards and guidelines.

2.1.2 The ITS IT Security team are a consultative function and must be used to facilitate a secure resolution for any activities that are unable to meet this policy.

2.2 Security Updates and Patching Requirements

2.2.1 Where possible, automatic deployment systems for security updates and patches on devices in scope must be used. The schedules for applying security updates and patching should be set appropriately to ensure a secure IT system is maintained and service availability is maximised.

2.2.2 Where automatic deployment systems can't be used, the relevant IT team must monitor security advisories from the applicable vendor and/or support company.

2.2.3 The IT Security team must be informed in a timely manner when any of the technology in scope is not supported by the vendor and/or lacks security updates and patches.

2.2.4 Should security updates or patches have a negative effect on the core functionality of an IT system, the IT Security team must be consulted to confirm an appropriate compensating control.

2.3 Logging and Monitoring

2.3.1 All administrative activity must be logged and retained for at least 90 days. This is in the interest of incident response, accountability, and non-repudiation.

2.3.2 All technology in scope must be monitored for performance and appropriate alerts must be configured to notify the relevant support teams when the technology when an event is triggered.

2.4 Documentation

2.4.1 All documentation, including policies and its integration with other systems in scope, must be accurate, up-to-date, and reviewed on an annual basis or after a significant change.

3. Governance Requirements

3.1 Implementation / Communication Plan

3.1.1 This Policy will be published on the University's IT Services SharePoint Online site alongside other internal IT policies. All public University Policy Documents (either direct or clearly linked to other pages) will be included on the University's public website.

3.2 Exceptions to this Policy

3.2.1 The principles of information security are underpinned by legislation and the consequences of a serious breach of information security are severe. Therefore, exceptions to the principles outlined in this policy are not expected to be allowed. In highly exceptional cases, and with a very high level of justification, any request to relax the normal information security requirements must be authorised in writing by the Chair of the Information Security and Governance Group (ISAGG).

3.3 Review and Change Requests

3.3.1 This policy must be reviewed annually, or when there's significant change in University requirements, or related legislation, contractual obligations, and University regulation.

3.4 Related Legislation, Contractual Obligations, and University Regulation

3.4.1 PCI DSS controls must be maintained where applicable.
3.4.2 DSP Toolkit controls must be maintained where applicable.
3.4.3 PREVENT Duty controls must be maintained where applicable.
3.4.4 Related University Policies must be understood and adhered to, to provide a secure, regulated, and reliable IT infrastructure.

3.5 Stakeholder Statements

3.5.1 Equality: The University is strongly committed to equality of opportunity and the promotion of diversity for the benefit of all members of the University community. The University's approach is to promote equality across the full range of its activities, in employment, teaching and learning and as a partner working with and within local, national and international communities. Equality Analysis is a process which examines how the impact of the policy has been considered on the diverse characteristics and needs of everyone it affects. This policy has been reviewed and no negative impact on equality has been identified.

3.5.2 Health & Safety: Health and Safety implications have been considered during the drafting of this policy and are incorporated (where necessary) into the policy

3.5.3 Other: N/A