Patch Management Policy

Policy Owner	**James Drain**
Policy Version	**1.0**
Approved By	**Corporation**
Approval Date	**23 March 2020**
Review Date	
Related Policies	
Distribution	

SIGNIFICANT CHANGES FOLLOWING REVIEW

Policy Review on [Insert Date]

Page Number or Heading Name	Details of significant change	Changes made by

1. INTRODUCTION

South Essex College of Further and Higher Education (The College) has a responsibility to uphold the confidentiality, integrity and availability of the data stored on its computer systems. Installing patches helps to mitigate against vulnerabilities and bugs in the College's computer systems.

Following this policy will reduce the overall exposure of the College computer systems to bugs and vulnerabilities which would otherwise leave them open to compromise and exploitation.

2. PURPOSE

This policy outlines the requirements to keep the College computer systems "up-to-date" and the timelines to abide by to keep the overall exposure to threats to a minimum.

3. DEFINITIONS

- Workstation – Desktop, laptops, and tablets such as Microsoft Surface
- Mobile Device – Devices running mobile operating systems such as iOS and Android. Typical devices included are mobile phones and tablets such as iPads.
- Network appliance – Switches, routers, firewalls, wireless access points, and DNS.
- Software – Operating systems, commercial off-the-shelf applications, plugins, interpreters, scripts, libraries, network software and firmware.

4. SCOPE

- Workstations, mobile devices, networking appliances, hardware devices owned by South Essex College of Further and Higher education and supported by Computing Services or third-party supplier.
- Systems that contain South Essex College data owned or managed by Computing Services or third-party supplier

5. POLICY

5.1 All computer systems in scope must be manufacturer supported, licenced and running the latest security patches to protect these systems from known vulnerabilities

5.2 When an application or system as defined in section 3 is no longer licenced or supported by the manufacturer it must no longer be used and removed or uninstalled.

5.3 Patches should be tested where reasonably possible before being deployed. Testing should encompass a diverse test base to represent the wider IT estate.

5.4 All patches must be deployed within the timeline defined in the following schedule unless prevented by an operational business impact:

Update Severity	**Timeline (from release date)**
Critical/High or CVSS of 7.0 and above	14 days
Medium or CVSS of 4.0-6.9	21 days
Low or CVSS 0.1-3.9	28 days
None/bug fix only	Deployed as soon as reasonable possible or the next available maintenance window.

If a vendor releases a cumulative update with multiple patches, the cumulative update will be

deployed based on the highest severity patch.

Ref: https://www.first.org/cvss/

5.5 Where a patch is found to cause instabilities or impacts on business operations a risk assessment should be conducted by the Computing Services Security Analyst to approve or deny the patch from being deployed until such a time a solution or replacement patch is available.

5.6 When a patch cannot be deployed due to reasons stated in point 5.5 or one is not available additional mitigations where possible must be implemented to reduce the exposure of the vulnerability.

5.7 Patches that do not address any security vulnerabilities and contain only bug fixes will be evaluated based on the operational impact to the College. Where a patch addresses a known issue being experienced it should be tested and deployed as soon as reasonably possible.

6. ROLES AND RESPONSIBILITIES

Computing Services

- Manage the patching needs of all devices as defined in Section 3 and liaise with application owners, as necessary.
- Routinely assessing compliance with the patching policy

Computing Services Security Analyst

- Monitor emerging security vulnerabilities and review patching compliance.
- Evaluate vulnerabilities and patching when there may be a significant impact on business operations.

End Users

- The end user is responsible for ensuring patches are installed on their devices. End users should make time to install and reboot for the complete installation of the patch. Any noticed issue as a result of installing a patch should be reported to the IT helpline.

Third Parties

- Will ensure security patches are applied and maintained on systems under their control and management as stipulated in Section 5. Where this is not possible this must be escalated to the Computing Services Security Analyst.

7. MONITORING

Those with the responsibility for patching IT systems should maintain reports of the patching compliance of their systems to review current patching levels and overall risk of vulnerability exposure. These reports shall be made available to the Computing Services Security Analyst upon request for audit and review.