

Software Updates and Patching Policy

Reference: CES DOC 5.1

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 16/03/2021

Organisation Issue Date:

1. Scope

Software is considered within scope if it is installed on a computer or other device that is connected to or able to be connected to the Internet.

All in-scope software in Organisation Name supported by ongoing updates and patches is subject to this policy.

All in-scope software that is not supported
"by ongoing updates and patches"

is to be removed in accordance with this policy.

2. Responsibilities

2.1 The Owner of the software is responsible for identifying the update and patch procedure used by the software developer. They are also responsible for providing a summary of this procedure to the Head of IT (CIO) for review.

2.2 The Head of IT (CIO) is responsible for ensuring that all update and patch procedures are reviewed for security.

2.3 The Head of IT (CIO) is responsible for maintaining the programme of updates and patches and ensuring that all updates are logged for review.

3. Software updates

3.1 Software used is the latest supported and licensed version.

3.1.1

"The following software is exempt for the identified reason: Software, approved version and justification. "

3.2 The following changes are considered routine or insignificant and are therefore the primary subject of this policy:

<<3.2.1-3.2.4 removed for sample purposes>>

3.3 The Owner of the software identifies the developer's update/patching schedule (weekly, monthly, etc.) and informs the Head of IT (CIO) by "email/form."

3.4 Software will be audited every "six months"

to ensure that the cumulative impact of patches and updates has not compromised security or functionality.

<<3.5 removed for sample purposes>>

4. Patching

4.1 The Head of IT (CIO) ensures that the regular patches are approved to update automatically, applying system permissions as necessary.

4.1.1 Patches are approved once they have been through the appropriate testing process and deemed sufficient.

4.2 All automated updates should be logged so that discrepancies that may indicate cyber security threats or vulnerabilities are recorded.

4.3 The Owner of the software monitors the contents of each patch or update and reports the results to the Head of IT (CIO).

<<4.4-4.6 removed for sample purposes>>

Document owner and approval

The Head of IT (CIO) is the owner of this document and is responsible for ensuring that it is reviewed in line with the requirements of the management system.

The current version of this document is available to "Specify which members of staff this document is intended for"

and is published

"Describe the location(s) - electronic and physical - where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).