Queens College Technology Standard	No: QC-ITS-Cyber-029
Secure Software Support Standard	**Updated: 09/08/2023**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

This standard establishes that Information Technology (IT) will only provide support for software versions that are currently supported by the respective companies and are regularly updated with security patches. This standard aims to enhance the security posture of Queens College by ensuring the usage of secure and up-to-date software applications.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services
- **Responsible Executive(s)**: Chief Information Officer (CIO)
- **Responsible Officer(s)**: Chief Information Security Officer (CISO)

3.0 Scope – College-Wide

This is a college-wide standard and includes requirements that must be followed if Queens College is to protect the information that is collected in the standard process of business. This standard is to be an additional layer of security on top of existing CUNY security policies and is not intended or able to supersede CUNY policies.

This standard encompasses all systems, automated and manual, for which Queens College has administrative responsibility, including systems managed or hosted by third parties on behalf of Queens College. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4.0 Information Statement

1. Secure Software Support:

    a. IT will prioritize the support, maintenance, and troubleshooting of software applications that are currently supported by their respective companies and receive regular security updates.
    b. Supported software versions must have a demonstrated commitment from the vendor to address security vulnerabilities promptly.
2. End-of-Life (EOL) Software:
    a. ITS will work with users to ensure that Queens College versions of EOL software purchased through the Purchasing Office will be upgraded to the latest supported version or an alternative supported software solution.
    b. IT will not provide direct support for personal software versions that have reached their official End-of-Life (EOL) or End-of-Support (EOS) date as declared by the software vendor.
    c. The usage of EOL software poses significant security risks due to the absence of regular updates and vulnerability patches, making them susceptible to exploitation.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the standard owner at:

Chief Information Security Officer
Damon Vogel
CISO@qc.cuny.edu

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
07/12/2023	Creation of Policy	DVogel
09/08/2023	Added # 10, Converted to Standard, Aligned to Gartner Recommendations.	

9.0 Related Documents

10.0 External Documents