Queens College **Technology Standard**	**No: QC-ITS-Cyber-013**
Enterprise Service Management Standard	**Updated: 08/21/2023**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

This standard establishes Information Technology Services (ITS) as the primary area responsible for running and managing enterprise services, including Active Directory, Domain Name Servers (DNS), Dynamic Host Configuration Protocol (DHCP), and other critical infrastructure components within Queens College. This standard aims to ensure consistency, security, and efficient operations across the university's IT environment.

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. Responsibilities:
    a. IT Department:

        i. The ITS department shall have the primary responsibility for the configuration, management, and maintenance of enterprise services.
        ii. ITS personnel will possess the necessary expertise, training, and knowledge required for effective management of these services.
        iii. ITS shall ensure the integration, security, scalability, and interoperability of enterprise services with other ITS infrastructure components.
    b. Collaboration:
        i. ITS shall collaborate with relevant stakeholders, departments, and users to understand their needs and ensure the proper functioning of enterprise services. ii. Collaboration with departmental administrators and other stakeholders shall be sought to define user access levels, permissions, and other service-specific requirements.

2. Service Configuration and Optimization:
    a. ITS shall establish and enforce standard configurations, best practices, and security protocols for enterprise services.
    b. ITS will monitor and optimize the performance of enterprise services to ensure optimal service delivery and user experience. c. Regular reviews and updates shall be conducted to incorporate emerging technologies and industry best practices.
3. Security and Compliance:
    a. ITS shall implement robust security measures to protect enterprise services from cyber threats, unauthorized access, and data breaches.
    b. Security controls, including access controls, authentication mechanisms, and encryption, shall be implemented to ensure the confidentiality, integrity, and availability of enterprise services.
    c. Compliance with relevant regulations, industry standards, and data protection laws shall be ensured in the management of enterprise services.
4. Review and Audit:
    a. Regular audits and reviews shall be conducted to assess the performance, security, and compliance of enterprise services.
    b. Audit findings and recommendations shall be addressed promptly to maintain the integrity and effectiveness of these services.

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
08/21/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents