Queens College Technology Standard	No: QC-ITS-Cyber-037
Vulnerability Scanning Standard	**Updated: 09/08/2023**
	Issued By: Office of the Chief Information Security Officer (CISO) **Owner: Queens College, Information Technology Services**

1.0 Purpose and Benefits

Entities utilize automated tools to scan systems, computing and network devices, web applications and application code. The results of these scans help inform management and system administrators of known and potential vulnerabilities.

Vulnerability management is a process by which the vulnerabilities identified through scanning are tracked, evaluated, prioritized and managed until the vulnerabilities are remediated or otherwise appropriately resolved. Managing the vulnerabilities identified during scans ensures that appropriate actions are taken to reduce the potential that these vulnerabilities are exploited and thereby reduce risk of compromise to the confidentiality, integrity and availability of information assets.

2.0 Authority

- **Responsible Office(s):** 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 policy 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.

4.0 Information Statement

As per the Information Security Policy, all systems must be scanned for vulnerabilities. In addition, each system must be inventoried and have an individual or group assigned responsibility for maintenance and administration.

4.1 Types of Scans

The type of vulnerability scans appropriate for a given target depends on the target type (i.e., hardware, software, source code) and the target's location (i.e., internal or external to the network). The table below lists the types of vulnerability scans required by this standard.

Type	Description
External Infrastructure Scan	Scans of the perimeter of networks or any externally available hosted infrastructure to identify potential vulnerabilities in Internet accessible IT infrastructure.
Internal Infrastructure Scan	Scans of IT infrastructure on protected networks or any hosted infrastructure to identify potential vulnerabilities.
"Lite" Web Application Scan	Cursory unauthenticated scans of externally facing production web applications to identify security vulnerabilities.
In-depth Web Application Scan	When implemented, authenticated in-depth scans of web applications to identify security vulnerabilities.
Application Source Code Analysis	Scans of application source code run during development to identify problems in the code that could cause potential vulnerabilities.

4.2 Scanning

Queens College Information Technology Services is responsible for confirming that vulnerability scans are conducted. Entities must use a scanning tool approved by the CISO's Office. Any approved scanning tool must be able to provide remediation suggestions and be able to associate a severity value to each vulnerability discovered based on the relative impact of the vulnerability to the affected system.

As per the Information Classification Standard, scan reports are classified with moderate confidentiality and moderate integrity and should be protected as such.

Entities are required to provide all external IP addresses and Uniform Resource Locators (URLs) for all externally facing web applications to the CISO's Office.

Network and system administrators must provide sufficient access to allow the vulnerability scan engine to scan all services provided by the system. No devices connected to the network shall be specifically configured to block vulnerability scans from authorized scanning engines.

Scans must be performed within the system development life cycle (see SSDLC Standard) while in pre-deployment environments, when deployed into the target implementation environment, and periodically thereafter as specified below:

a. Pre-deployment scans occur prior to the move of the system or web application to the target implementation environment:

    1. All systems must undergo an authenticated internal infrastructure scan, where technically feasible or required, before being deployed to the target implementation environment. Any infrastructure vulnerability discovered must be remediated or determined to be a false positive or insignificant risk, by the CISO's Office, prior to the system being deployed for intended use.

    2. When source code is available, applications must undergo source code scanning before the updated code moves into the target implementation environment if there has been a change to application code.

    3. Scans must be authenticated when the application requires authentication before being deployed into the target implementation environment or into an environment that is externally accessible. When authentication is required to access the application, scans must be run with authenticated access at each access level (e.g., user, admin) supported by the application, except where limitations in the tool prevent authenticated scanning. Any web application vulnerability discovered must be remediated or determined to be a false positive or insignificant risk by the ISO/designated security representative, prior to the system being placed into the target implementation environment.

    4. Any system or application deployed to its target implementation environment with un-remediated vulnerabilities must have a formal remediation plan and the documented approval of the executive responsible for risk management or their designee.

b. Implementation scans occur the first time a system or web application is moved to its target implementation environment:

    1. Systems must be scanned immediately upon being placed into the target implementation environment with an authenticated internal infrastructure scan, where technically feasible or required. If the system is accessible from the internet or an external network, then the system must be scanned with an external infrastructure scan.

    2. Web applications must be scanned within the first month of being placed into the target implementation environment. An authenticated in-depth web application scan is required if feasible, but at minimum a "lite" web application

scan is required. Sensitivity and criticality of the application must be considered when determining the schedule for the initial implementation scan.

c. Recurring Scans: After the initial scan in the target implementation environment, the frequency of scans are to occur according to the system or application's risk rating (see Table 2).

   1. When performing internal infrastructure scans on systems built using a shared image, such as workstations, scans may be run on a sampling of systems but the sample set must vary from scan to scan.

   2. Web applications in production are required to undergo recurring scans. At minimum, web applications in production are required to undergo recurring "lite" application scans.

   3. All vulnerabilities found during scans must be addressed as per the remediation section below.

4.3 Determine Risk Rating and Frequency of Scans

The risk that vulnerabilities pose to systems and applications is based on the likelihood of a vulnerability being exploited and the impact if the confidentiality, integrity or availability of the information assets were compromised. The likelihood of a vulnerability being exploited is increased in direct relation to the system's or application's accessibility from other systems.

The impact to the information assets is based on the asset's information classification (see Information Classification Standard). Impact (i.e., high, moderate or low) if the confidentiality, integrity or availability is compromised must be considered and the highest individual impact rating for confidentiality, integrity or availability utilized within the table below.

Table 2: RISK RATING

Impact (Confidentiality, Integrity, Availability)	**Exposure**		
	Systems with no network connectivity to production data	**Systems with network connectivity to production data (not internet facing)**	**System that is publicly available from the internet**
High	**Medium**	**High**	**High**
Medium	**Low**	**Medium**	**High**

Low	**Low**	**Low**	**Medium**

Minimum frequency of scans is dependent on the risk rating. Systems without a risk rating must be scanned as if they had a risk rating of “High” until they are rated.

TABLE 3: FREQUENCY OF SCANS	
Risk Rating	**Frequency**
Infrastructure scans	
High	Monthly
Medium	Quarterly
Low	Semi-annually
Web Application Scans	
High	Quarterly or after significant change
Medium	Semi-annually
Low	Annually

4.4 Remediation

Vulnerabilities discovered during scans must be remediated based on risk rating (see Table 2) and vulnerability severity identified by the scanning tool as per the table below.

TABLE 4: REMEDIATION TIMEFRAMES			
Risk Rating (from Table 2)	**Vulnerability Severity**		
	Low or Below	Above Low to Below High	High or Above

High	At the discretion of the ISO/designated security representative	Action Plan in 2 Weeks, Resolved in 6 Months	Action Plan in 1 Week, Resolved in 1 Month
Medium	At the discretion of the ISO/designated security representative	Action Plan in 3 Weeks, Resolved in 1 year	Action Plan in 2 Weeks, Resolved in 6 Months
Low	At the discretion of the ISO/designated security representative	At the discretion of the ISO/designated security representative	Action Plan in 3 Weeks, Resolved 1 year

The ISO/designated security representative may review vulnerabilities to adjust the severity rating if necessary. Testing must be done to verify that remediation has been completed.

Individuals managing vulnerability scans are required to notify the ISO/designated security representative within 1 business day of scan completion for new vulnerabilities and at least monthly of un-remediated vulnerabilities on systems or applications that are running in production.

ISOs/designated security representatives must notify management of any un-remediated vulnerabilities not addressed in the timeframes prescribed in this standard, so that risk is accepted by the appropriate party.

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 policy 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 policy 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	Initial Alignment to Queens College	DVogel
09/08/2023	Conversion to Standard, Add # 10, Align to Gartner Recommendations	DVogel

9.0 Related Documents

Patch Management Standard

10.0 External Documents