Queens College Technology Standard	No: QC-ITS-Cyber-006
Auditing and Accounting Standard	**Updated: 08/21/2023**
	Issued By: Queens College, Office of Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2.0 Authority

- **Responsible Office(s):** Information Technology Services & General Counsel
- **Responsible Executive(s)**: Chief Information Officer (CIO)
- **Responsible Officer(s)**: Chief Information Security Officer (CISO)

3.0 Scope

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.

These policies apply to information systems that are determined to contain sensitive or otherwise information judged to need protection by the CISO.

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 Policy Statement

1. Audit Events

a. Determine that the information system can audit all events determined as needed.

b. Coordinate the security audit function with other organizational entities requiring audit.

c. Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

d. Determine that the following events are to be audited within the information system, such as:

- Account logon events
- Logon events
- Account management
- Directory service access
- Object access
- Policy change
- Privilege use
- Process tracking
- System events

2. Reviews And Updates

   a. The organization shall review and update the audited events every semester.

3. Content Of Audit Records

   a. The information system shall generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

4. Audit Storage Capacity

   a. The information owner shall ensure audit record storage capacity is allocated in accordance with minimum 1 year storage.

5. Transfer To Alternate Storage

   a. The information system shall off-load audit records annually onto a different system or media than the system being audited.

6. Response To Audit Processing Failures

   The information system shall:

   a. Alert CISO in the event of an audit failure.

   b. Take the following additional actions: overwrite oldest audit records.

7. Audit Storage Capacity

   a. If possible, the information system shall provide a warning to CISO & D-CIO within 24 hours when allocated audit record storage volume 80%-90% of repository maximum audit record storage capacity.

8. Real-Time Alerts

   a. If possible, the information system shall provide an alert in a pre-determined time based on system to CISO when the audit failure events occur.

9. Configurable Traffic Volume Thresholds

   a. If possible, the information system shall enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity and rejects or delays network traffic above those thresholds.

10. Audit Review, Analysis, And Reporting

    The information system owner shall:

    a. Review and analyze information system audit records as needed for indications of issues every semester.

    b. Report findings to CISO's Office.

11. Process Integration

    a. If possible, the information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

12. Audit Repositories

    a. If possible, the information system owner shall ensure analysis and correlation of audit records across different repositories to gain situational awareness.

13. Audit Reduction and Report Generation

a. The information system shall provide an audit reduction and report generation capability that:

    i. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.

    ii. Does not alter the original content or time ordering of audit records.

14. Automatic Processing

    a. If possible, the information system shall provide the capability to process audit records for events of interest based on severity.

15. Time Stamps

    The information system shall:

a. Use internal system clocks to generate time stamps for audit records.

16. Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

17. Synchronization With Authoritative Time Source

    The information system shall:

a. Compare the internal information system clocks regularly with NTP servers.

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than 5 minutes.

18. Protection Of Audit Information

    a. The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

19. Audit Record Retention

    a. The information system owners shall retain audit records for 1 year minimum to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

20. Long-Term Retrieval Capability

    a. The information system owners shall employ all needed measures to ensure that long-term audit records generated by the information system can be retrieved.

21. Audit Generation

    The information system shall:

    a. Provide audit record generation capability for the auditable events as defined.

    b. Allow CISO's office and/or designates to select which auditable events are to be audited by specific components of the information system.

    c. Generate audit records for the events with the content as defined.

22. Time-Correlated Audit Trail

    a. The information system shall comply with audit records from all areas into a system-wide (logical or physical) audit trail that is time-correlated.

23. Standardized Formats

    a. The information system shall produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

24. Changes By Authorized Individuals

    a. The information system shall provide the capability for CISO's Office or designates to change the auditing to be performed on all systems as needed.

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:

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
11/09/22	Initial changes to apply to Queens College	DVogel
06/12/2023	More Changes to apply to Queens College	DVogel
08/21/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Auditing and Accountability (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100

10.0 External Documents