Open Access Technology Facility Policy

Date: March 24th, 2021

Issued By: University Chief Information Officer

Policy Owner: Computing and Information Services

Purpose and Background:

Open Access Technology Facility is a general term for a facility or lab that provides shared technology and related resources supporting the campus community, typically, but not necessarily, on a “drop in” basis. This policy defines supplementary information security requirements specific to CUNY Open Access Technology Facilities intended to promote a safe, secure and welcoming environment.

Scope:

This policy applies to all University Open Access Technology Facilities.1

Statement:

I. Each user of the technology facility is required to use a unique login credential or equivalent unique access code to access services, where implementation of such is technically achievable.

   a. Such sign-ons and sign-offs must be securely logged with a timestamp, username (or other unique identifier) unique system name and IP address that, in response to an incident, would help facilitate the attribution of activity to a particular account holder.2

   b. Users are permitted to request to view this sign-in/off log (i.e., when they have logged in or out) in a read-only manner, if feasible, but a user’s log must not be accessible to, nor alterable by, other users.

   c. The logs must be retained for three years in a manner in which the logged information can be retrieved to support an investigation within three business days.

---

1 Whether on-premises or operated on behalf of CUNY.

2 Investigations must be conducted in accordance with the CUNY Acceptable Use of Computer Resources policy.
Open Access Technology Facility Policy

Where the above is not technically achievable, other means to log usage, such as a supervised sign-in/out procedure, should be used where practical.

II. Periodically present a logon banner or equivalent conveyance\(^3\) to each user in which the user agrees that use must comply with the University Acceptable Use of Computer Resources policy and other relevant University policies, and highlighting that:

a. All use must be legal and in accordance with the Acceptable Use of Computer Resources policy.
b. Activity may be monitored in accordance with the Acceptable Use of Computer Resources policy.
c. The display or play of visual or audible material that is disruptive to other facility users, or that could violate the Policy on Sexual Misconduct, is not permitted. Where such is in support of a faculty-endorsed, academic purpose, appropriate care must be taken to avoid offending or disrupting other facility users.

III. Users should be automatically signed-off from their session after a period of inactivity, where implementation of such is technically achievable. The maximum period of inactivity before sign-off should be 30 minutes.

IV. Facility computers, loaner equipment (laptops, tablets, etc.) and other devices that access University networks or the Internet must conform to all CUNY IT Security policy requirements, including the following that may reinforce or supplement such requirements:

a. Real-time, anti-malware protection must be active with scheduled full scans of accessible memory and files performed at least weekly.\(^4\)
b. Anti-malware software and related signatures and configurations must be kept up-to-date.
c. Malware-infected computers or devices must be promptly removed from the network until verified as malware-free.
d. Facility Admins/Facility Managers are responsible for creating procedures that ensure the requirements are implemented on an ongoing basis.

V. Use of non-persistent desktops (e.g., virtual desktops) or automated system restore (e.g., “Deep Freeze”) upon sign-out or at regular intra-daily intervals is encouraged to ensure that facility users are presented with a clean, known-good environment. Non-persistent desktops help to avoid breaches of security or privacy that could occur from remnant temporary files, etc., persisting between user sessions, and to reduce cross-session, malware-related risks.

---

\(^3\) Conspicuous signage may be substituted if a logon banner or equivalent is not technically achievable.

\(^4\) Use of non-persistent desktops, as in V, may obviate the need for scheduled full scans.
VI. Facility device software and operating systems, including system images used for non-persistent desktops, etc., must be updated as needed or required (at least monthly or promptly\(^5\) when there is a critical vulnerability, whichever is sooner) to include vendor-released security and anti-malware software updates.

Related Information

CUNY IT Policies - [http://www.cuny.edu/about/administration/offices/CIS/policies.html](http://www.cuny.edu/about/administration/offices/CIS/policies.html)

CUNY IT Security Policies and Procedures – [https://security.cuny.edu](https://security.cuny.edu)

\(^5\) After appropriate but expeditious testing.