Boston Public Library
Collections Security Policy
Approved by the Board of Trustees of the Boston Public Library
May 24, 2022

INTRODUCTION/PURPOSE OF POLICY

The Boston Public Library holds extensive research and special collections reflecting a wide diversity of subjects, cultures, countries, and languages. Although most resources are print-based (books, periodicals, newspapers, and documents), significant collections in other formats include manuscripts, photographs, archives, prints, fine art, audiovisual materials, maps, architectural drawings, sheet music, sculpture, digital content, and other objects.

All BPL research and special collections are held in the public trust. As a public library, we commit to providing free, open and equitable access, and we work to encourage use and discovery. We recognize that there is an inherent tension between access and long-term security and preservation.

This Collection Security Policy outlines a framework for the security of research and special collections that focuses on creating and maintaining an environment in which these materials are protected, carefully handled, and returned intact to the collection for use by future patrons. The framework relies on a library-wide culture of responsibility for collections security. All staff members share responsibility in reporting incidents and observations related to collection security. Everyone—regardless of position, rank, title, or status—is responsible for compliance with the policies and procedures that are designed to protect the collection, visitors, and staff.

In support of the Library's mission, this policy and the procedures that stem from it prioritize public use of collections, and all collections security procedures will be governed by the Library's ongoing work related to diversity, equity, and inclusion. In planning and drafting this policy, we have relied on standards such as the Association of College & Research Libraries' code of ethics and the ACRL/RBMS Guidelines Regarding Security and Theft in Special Collections to ensure we are following ethical and equitable best practices and standards.

RESPONSIBILITY FOR COLLECTIONS SECURITY

The Library's leadership is responsible for all aspects of collections security. The strategic and procedural oversight of collections security is led by the Collections Security Team (CST). Members of the CST are designated by the Library President and include relevant managers that oversee collections, security, and technology functions.

The CST is responsible for writing and implementing procedures and reviewing and auditing enforcement, effectiveness, and compliance. Members of the CST manage responses to incidents related to collections security and will keep leadership apprised on a regular basis.

The CST also reviews the Library's emergency response plans and provides direction on procedures that pertain to collections security.

For this policy to be effective, there needs to be a widespread understanding across all Library departments of the importance of collections security. To this end, the Library is responsible for making employees aware of and providing training on collections security policies and procedures. Staff are responsible for the implementation and execution of policies and procedures developed by the Library and the CST.

INSTITUTIONAL COMMITMENT

The Library commits to allocating resources, routine auditing and maintenance of existing technologies, and exploring and implementing new solutions to deliver the level of collections security outlined in this policy.

The library is responsible for the upkeep of all security infrastructure. Security infrastructure throughout the system is serviced routinely as a procedure to verify adequate function. The Collections Security Team is responsible for reviewing this policy every two years and updating as needed.

SECURITY OF DIGITAL COLLECTIONS

In addition to physical holdings, collections security applies to digital collections materials in the Library's care. It also pertains to metadata about library collections stored in digital form. The security of digital files and records relies on designated levels of access—including the ability to upload, download, and edit files or metadata—as well as clearly defined roles and appropriate privileges for staff or patrons.

The CST will work in an advisory capacity with stakeholders, relevant library departments, and the Information Technology team to provide guidance on security-related procedures, including maintaining backups and preservation copies of digital assets; periodic auditing of files and records; establishing criteria for evaluating vendor security practices; and the protection of the library's networks, servers, applications, and other infrastructure components related to the management of digital assets from unauthorized access.

ACCESS TO COLLECTIONS AND SPACES

Collections are found in both public and staff-only spaces. Access may be limited based on the way the space is used: for example, offices and collections storage areas are accessible only to staff. Access may also be limited by day and time: for example, patrons can access public spaces during normal operating hours or during events.

The Library relies on defined levels of access to spaces for security. The CST works with stakeholders to determine access levels to each space. Physical and/or electronic access to

spaces is assigned accordingly. The Library performs audits and updates permissions with staffing changes.

The CST consults stakeholders to establish guidelines for patron use of special collections. The Library's goal is free, open, and equitable access. Alternate modes of access may be offered based on preservation or security concerns.

Patrons will be notified of any relevant security guidelines, identification requirements, on-site surveillance practices, and data retention policies.

SPECIAL COLLECTIONS DATA RETENTION AND PRIVACY

The Library's collections security program relies on the systematic retention and maintenance of personal information. With respect to special collections, personal information may include usage data and surveillance footage. Usage data includes information that identifies materials requested by specific patrons and information about when and how such materials were used. Personal information necessary to identify specific patrons, including names, addresses, and photographs may also be retained. Requirements for the retention of security-related data are established by the CST in consultation with the IT Department and with any other relevant departments. The Library may keep records on personal information and usage data related to special collections in perpetuity. The Library is committed to patron privacy and will not share data with a third party unless required by law and/or in response to a security incident.

RESPONSES TO SECURITY EVENTS

It is the responsibility of all BPL staff members, contractors, and affiliates to follow established procedures to report incidents, observations, or concerns related to collection security in a timely manner. The Collections Security Team (CST) will review and document each incident or report with the immediate goal of securing the particular item or collection in question.

When incidents occur or when reports are received, the Library will immediately notify stakeholders, investigate incidents, and document findings. The Library will utilize all available resources as appropriate, including legal action, and work with partners, stakeholders, and authorities in their efforts to secure or recover the collections under review. The CST will provide recommendations, guidance, and support to library leadership when incidents occur.