Surveillance Technology Policy

Bibliotheca RFID Circulation and Security Gate System
San Francisco Public Library

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of the Bibliotheca RFID circulation and security gate system itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The San Francisco Public Library system is dedicated to free and equal access to information, knowledge, independent learning and the joys of reading for our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Bibliotheca RFID circulation and security gate system will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure the Bibliotheca RFID circulation and security gate system, including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of the Bibliotheca RFID circulation and security gate system technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

- Passive RFID tags applied to library material – For use in inventory management and circulation functions.
- Staff workstation RFID pads – For use by staff to check in and out material and trigger holds.
- Self-check machines – For use by patrons to check out material.
- Inventory wand – For use by staff to confirm the current inventory on the library's shelves.
- Sorting machine – For use in checking in material and sorting the items into carts and bins for delivery to other floors and branches.

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Surveillance Oversight Review Dates
COIT Review: February 20, 2020
Board of Supervisors Review: August 4, 2021

BUSINESS JUSTIFICATION

The Bibliotheca RFID circulation and security gate system supports the Department's mission and provides important operational value in the following ways:

It is the Library's opinion that the use of passive low frequency RFID technology as an inventory control mechanism does not constitute the implementation of Surveillance Technology. No patron information is collected, retained, processed or shared through the use of RFID in the process of circulating and securing materials. Patron's library cards will continue to use eye readable barcode labels which will only be readable by barcode scanners. The Library is including this technology in its response because RFID is specifically cited as a possible surveillance technology in the relevant ordinance.

The use of passive low frequency RFID tags on the library's collection in conjunction with Bibliotheca staff workstations and self-service equipment improves the customer service experience at the library. Self-check machines are significantly quicker and easier to use than those based on tattle-tape technology. Staff RFID workstations speed up the circulation tasks significantly, freeing up staff time to better serve the public. Both patrons and staff will be able to check in or out approximately 8 items at a time (piles up to 12 inches high), since RFID eliminates the existing need to scan and desensitize each item. The overall improved inventory control ensures patrons find the items they are looking for and reduces the time that books are unavailable to the patrons by streamlining circulation cycle from check-in to on-shelf.

RFID security gate technology will improve security, while improving service through improved communication. If the alarms sounds, staff will be able to quickly identify which item was not checked out or if it is a false alarm, eliminating the need to go through bags and check every item the patron may have against the printed check-out slip or pull up their record in the Sierra ILS database.

In addition, the Bibliotheca RFID circulation and security gate system promises to benefit residents in the following ways:

- Time savings and improved customer interaction

The Bibliotheca RFID circulation and security gate system will benefit the department in the following ways:

- Time savings during the check in and check out process of handling the library material. See attached Radio Frequency Identification (RFID) Costs/Return on Investment report. During staff tests, it was found that an average savings of 5.16 seconds will be saved for each item checked in (CKI) and 7.83 seconds will be saved for each item checked out (CKO). While some staff time will be saved as we tag each branch's collection, the complete conversion will not be finished until the end of FY20. For the report we opted to only track a full year of savings, estimating approximately $626,185.40 in organizational time savings in FY21.
- Improved Collection Inventory - Improved accuracy during circulation transactions and the ability to perform collection inventories will greatly reduce the number of missing items that are repurchased. SFPL replaces missing items on a regular basis, and the average cost of replacing such material is $25.00 per item.

Other benefits include Improved Customer Service at security gates. Security gates that use tattle-tape technology can only notify staff that an item may not be checked out. This requires staff to

ask patrons to go through their items and check item by item to see if any material is not checked out. RFID gates do not read RFID tags from other libraries, book stores or other sources, so false hits will be eliminated. If an SFPL item is not checked out, the specific title will be listed in the StaffConnect software, allowing staff to provide that title to the patron and ask them to check the item out.

To achieve its intended purpose, the Bibliotheca RFID circulation and security gate system (hereinafter referred to as "surveillance technology") works in the following ways:

Passive RFID tags applied to library material: RFID tags have adhesive on the back and are applied primarily to the inside back cover of a library book or directly on to DVDs or CDs. The tag is used to store the 14-digit barcode number that is assigned to the item for use of inventory tracking within our Sierra ILS database. There is also a security component stored on the RFID tag, which tells an RFID reader whether the item is checked out or not. The tags are passive and only transmit data when a Bibliotheca reader comes into range.

Staff workstation RFID pads: The pads can simultaneously read multiple RFID tags in piles of material that are placed on top of the pad. The number of items may vary, since the read range is 12 inches from the pad. USB RFID pads have a smaller read range of only 6 inches, so they are mainly used for single-item transactions.

Self-check machines: The touch-screen devices allow patrons to check out their own library material. They allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of items may vary, since the read range is 12 inches from the pad.

Inventory wand: These portable wands include a RFID reader and allow staff to upload a shelf list of items that should currently be on the shelf. Items on a shelf can be inventoried by moving the handheld wand along the spine of each item. The read range is 8 inches from the front of the wand.

Sorting machine: RFID scanners track the item as it moves along the conveyer belt to be sorted. The read range is limited within the equipment to ensure the sorting process is not interrupted. The equipment also communicates using SIP2 communication to the Sierra ILS system, so that the library material is checked in.

Department staff may use the technology for authorized use cases only, and is expressly prohibited from the following use cases:

The Library will not use RFID tags on patron library cards. To ensure patron privacy, the library will continue to use eye readable barcodes on library cards. The Library's revised Privacy Policy specifically references the library's use of passive low frequency RFID technology and excludes the use of RFID tags on patron cards.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

Barcode for library material	The 14 digit number is transferred as temporary plain text and not stored.	Level 2

Notification: *No personally identifiable information (PII) is collected or tracked through this technology, so the Library does not post a notice.*

Access: All parties requesting access must adhere to the following rules and processes:

Data are not stored. RFID readers transfer the item barcode number to the Bibliotheca Staffconnect software, which temporarily stores it while it transfers the number to the Sierra ILS database. Once the RFID pad is used again or the software is closed, Bibliotheca Staffconnect software deletes the number. RFID gate logs will retain data for only titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.

Access requirements vary by party:

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology.

- 36xx, 99xx, 18xx

Department shall maintain access logs for surveillance technology and all data collected, processed, and/or stored by the surveillance technology. The name of the person making the log entry should be recorded, along with the date and time.

B. Members of the public, including criminal defendants

Data collected by surveillance technology is not stored and therefore will not be made available to members of the public, including criminal defendants.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants.

Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

Data used in circulation transaction are not stored.

Data Sharing: For internal and externally shared data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security)

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

Data are not stored nor shared. Only assigned library staff will be allowed to use the technology. The Library has a Privacy Policy and Privacy Inventory that governs how circulation data will be handled by staff.

B. External Data Sharing

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

Data Retention: While the Department does not collect PII through this technology, it adheres to the following data retention period and justification for the data it does collect.

Barcodes are stored in the passive RFID tags on each library item. Data are only stored by RFID readers long enough to pass the barcode number into the Sierra ILS database. Once another tag is read the barcode will be deleted. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Inventory wands will only use barcodes of material not currently checked out.	Barcodes collected during circulation transaction are not stored to ensure privacy. RFID gates and inventory wands only track items not connected with a patron account, so purging is less frequent. Security gate logs are retained to give staff the time to check the title provided and to interact with patron. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out. Barcodes collected during circulation transaction are not stored to ensure privacy. RFID gates and inventory wands only track items not connected with a patron account, so purging is less frequent. Security gate logs are

	retained to give staff the time to check the title provided and to interact with patron. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed. PII data collected by the surveillance technology may be retained beyond the standard retention period only in the following circumstance(s):

Under no conditions would data be retained past the timeline described above.

Departments must establish appropriate safeguards for PII data stored for longer periods.

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

Data are not stored.

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

Staff need to be trained on how to launch the Bibliotheca Staff connect software, how to toggle between checking in material and checking out material, and how to ensure the cursor is in the Sierra ILS database input box to ensure the barcode number will be transferred.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Library will provide the Policy document and overview on internal intranet and on the public website.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

> Michael Liang, Chief Information Officer, San Francisco Public Library

Sanctions for violations of this Policy include the following:

> The Library would work within existing City and departmental human resources guidelines to address and determine appropriate sanctions.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

Personally Identifiable Information:	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Raw Data:	Information collected by a surveillance technology that has <u>not</u> been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Public:

Complaints or concerns can be submitted to the Department in person, by phone, in writing that can be turned in by mail or in person, or electronically via the library's chat service, or "Comments and Suggestions" page.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall forward all questions and complaints to the proper internal department entities for timely response.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

APPENDIX A: Surveillance Technology Policy Requirements

The following section shows all Surveillance Technology Policy requirements in order as defined by the San Francisco Administrative Code, Section 19B.

1. A description of the product and services addressed by the Surveillance Technology, including the identity of any provider(s) whose services are essential to the functioning or effectiveness of the Surveillance Technology equipment or services for the intended purpose.

Passive RFID tags applied to library material: RFID tags have adhesive on the back and are applied primarily to the inside back cover of a library book or directly on to DVDs or CDs. The tag is used to store the 14-digit barcode number that is assigned to the item for use of inventory tracking within our Sierra ILS database. There is also a security component stored on the RFID tag, which tells an RFID reader whether the item is checked out or not. The tags are passive and only transmit data when a Bibliotheca reader comes into range.

Staff workstation RFID pads: The pads can simultaneously read multiple RFID tags in piles of material that are placed on top of the pad. The number of items may vary, since the read range is 12 inches from the pad. USB RFID pads have a smaller read range of only 6 inches, so they are mainly used for single-item transactions.

Self-check machines: The touch-screen devices allow patrons to check out their own library material. They allow multiple items to be stacked on the reader for instant and simultaneous check-out. The number of items may vary, since the read range is 12 inches from the pad.

Inventory wand: These portable wands include a RFID reader and allow staff to upload a shelf list of items that should currently be on the shelf. Items on a shelf can be inventoried by moving the handheld wand along the spine of each item. The read range is 8 inches from the front of the wand.

Sorting machine: RFID scanners track the item as it moves along the conveyer belt to be sorted. The read range is limited within the equipment to ensure the sorting process is not interrupted. The equipment also communicates using SIP2 communication to the Sierra ILS system, so that the library material is checked in.

Passive RFID Tags:

Staff Workstation RFID Pad Specification: Reader connects to PC via USB; it is supplied with a localized plug-in supply (110V ac/60Hz or 240V ac/50Hz). The RF power output is 1.2 Watt and the workstation™ shielded conforms to CE and FCC. Our staffConnect™ circ software will need to be installed on your existing PC, running Microsoft™ Windows (XP SP3 or W7 32/64). Connection to the LMS/ILS is only required for some of the functionalities.

Self-Check Specification: Operating frequency: 13,56MHz, Max. Transmitting power: 1.2W Supported tag types: ISO 15693, ISO 18000-3-A (NXP SLI, SLIx, SLIx2) RFID Item capacity: Approximately 5 items at any one time. Software: selfCheck™ components uses our quickConnect™ self-service software, which provides the customer with the full range of borrow, return and account functions. The software is configured for connection to the library ILS/LMS through SIP2. Access to the library's network via Ethernet is required.

Inventory Wand: Scan rate: Up to 20 items per second. Operating frequency: 13.56 MHz. RF Transmitting power: Standard Mode 1.5 W / Boost Mode 4.0 W. The mobile inventory device comes with our staffConnect™ inventory software which provides the user with the full range of search, inventory and shelf order functionality. The software does not require a connection to the LMS/ILS, but it can be configured to communicate directly via SIP2/NCIP. Access is required via a Wi-Fi access point. The software can be used on tablets and mobile devices that are able to run Java version 6.

Sorting Machine: SPECIFICATIONS LYNGSOE LIBRARY MATE™ 1200 SELF-RETURN KIOSK

Dimensions Large front: 708 mm H x 506 mm W / 28" H x 20" W Tunnel2000: 800 mm L; Max. angle: 7 degrees

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet

Capacity Up to 1,100 materials/hour

Touch screen 19" color touch screen

Standard colors Front plate: Green (RAL 6025/Brilliance 70); Shelf: Storm (RAL 7015)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.)

Item restrictions Item size: Min: 100 mm L x 100 mm W x 2 mm H / 4" L x 4" W x .1" H Max: 400 mm L x 300 mm W x 100 mm H / 15.8" L x 11.8" W x 4" H Item weight: Min: 30 g / 1 oz Max: 5 kg / 11 lbs

For use with LMS/ILS using SIP standard interface protocols Sorters: Sort Mate 1000 and 2000 sorter series Software: Library Mate software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish Data Model

LYNGSOE SORT MATE™ 2000 MODULESPECIFICATIONS

Dimensions Module: 600 mm L x 420 mm W x 860/950 mm H / 23.6" L x 16.5" W x 34/37.5" H Chute: Depending on choice of chute

Weight 44 kg / 88 lbs

Power 100-240 V AC 50-60 Hz

Network connection Wired Ethernet to master module containing the PLC

Capacity Up to 2,400 materials per hour

Materials Steel chassis

Chute Standard chute for trolley

Standard colors Chassis: Black (RAL 9005) Corner and end plates: Green (RAL 6025) Standard chute covers: Green (RAL 6025)

Suitable for receiving Library materials (books, magazines, CD/DVDs etc.) Material restrictions Material size: Min: 100mm L x 100mm W x 2mm H / 4" L x 4" W x .1" H Max: 400mm L x 300mm W x 100mm H / 15.8" L x 11.8" W x 4" H Item weight: Min: 30 g/1 oz Max: 5 kg/11 lbs

For use with Hardware: Library Mate™ inductions Hardware: Lyngsoe Ergo Staff™ inductions Hardware: Lyngsoe Turn Mate™ Hardware: Lyngsoe Ergo Chutes™ Hardware: Standard chutes Software: Lyngsoe PLC software 1.0 and newer Software: Library Mate™ software communicating with the ILS/LMS Software: IMMS for control of floating collections and reservations RFID: Danish data model Bar code: Dependent on Library Mate™ and Ergo Staff™ induction configuration

Data collected or processed by the Bibliotheca RFID circulation and security gate system will not be handled or stored by an outside provider or third-party vendor on an ongoing basis. The Department will remain the sole Custodian of Record.

---

2. A description of the purpose(s) for which the Surveillance Technology equipment or services are proposed for acquisition, including the type of data that may be collected by the Surveillance Technology equipment or services.

It is the Library's opinion that the use of passive low frequency RFID technology as an inventory control mechanism does not constitute the implementation of Surveillance Technology. No patron information is collected, retained, processed or shared through the use of RFID in the process of circulating and securing materials. Patron's library cards will continue to use eye readable barcode labels which will only be readable by barcode scanners. The Library is including this technology in its response because RFID is specifically cited as a possible surveillance technology in the relevant ordinance.

The use of passive low frequency RFID tags on the library's collection in conjunction with Bibliotheca staff workstations and self-service equipment improves the customer service experience at the library. Self-check machines are significantly quicker and easier to use than those based on tattle-tape technology. Staff RFID workstations speed up the circulation tasks significantly, freeing up staff time to better serve the public. Both patrons and staff will be able to check in or out approximately 8 items at a time (piles up to 12 inches high), since RFID eliminates the existing need to scan and desensitize each item. The overall improved inventory control ensures patrons find the items they are looking for and reduces the time that books are unavailable to the patrons by streamlining circulation cycle from check-in to on-shelf.

RFID security gate technology will improve security, while improving service through improved communication. If the alarms sounds, staff will be able to quickly identify which item was not checked out or if it is a false alarm, eliminating the need to go through bags and check every item the patron may have against the printed check-out slip or pull up their record in the Sierra ILS database.

The surveillance technology collects the following data types:

| Barcode for library material | The 14 digit number is transferred as temporary plain text and not stored. | Level 2 |

3. The uses that are authorized, the rules and processes required prior to such use, and uses of the Surveillance Technology that will be expressly prohibited.
[Toolkit 1.3, 1.5, & 3.16]

Use Case #1: Passive RFID tags applied to library material – For use in inventory management and circulation functions

Use Case #2: Staff workstation RFID pads – For use by staff to check in and out material and trigger holds.

Use Case #3: Self-check machines – For use by patrons to check out material.

Use Case #4: Inventory wand – For use by staff to confirm the current inventory on the library's shelves.

Use Case #5: Sorting machine – For use in checking in material and sorting the items into carts and bins for delivery to other floors and branches.

The Library will not use RFID tags on patron library cards. To ensure patron privacy, the library will continue to use eye readable barcodes on library cards. The Library's revised _Privacy Policy_ specifically references the library's use of passive low frequency RFID technology and excludes the use of RFID tags on patron cards.

Data are not stored. RFID readers transfer the item barcode number to the Bibliotheca Staffconnect software, which temporarily stores it while it transfers the number to the Sierra ILS database. Once the tag is removed from the pad, Bibliotheca Staffconnect software deletes the number. |
| 4. A description of the formats in which information collected by the Surveillance Technology is stored, copied, and/or accessed. |

The surveillance technology collects the following data types:		
Barcode for library material	The 14 digit number is transferred as temporary plain text and not stored.	Level 2

5. The specific categories and titles of individuals who are authorized by the Department to access or use the collected information, including restrictions on how and under what circumstances data collected with Surveillance Technology can be analyzed and reviewed, and the rules and processes required prior to access or use of the information.
Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology.

- 36xx, 99xx, 18xx |

Department shall maintain access logs for surveillance technology and all data collected, processed, and/or stored by the surveillance technology. The name of the person making the log entry should be recorded, along with the date and time.

Data are not stored. RFID readers transfer the item barcode number to the Bibliotheca Staffconnect software, which temporarily stores it while it transfers the number to the Sierra ILS database. Once the RFID pad is used again or the software is closed, Bibliotheca Staffconnect software deletes the number. RFID gate logs will retain data for only titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.

6. The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

Data used in circulation transaction are not stored.

7. The limited time period, if any, that information collected by the Surveillance Technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s) enumerated in the Surveillance Technology Policy, the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period

Barcodes are stored in the passive RFID tags on each library item. Data are only stored by RFID readers long enough to pass the barcode number into the Sierra ILS database. Once another tag is read the barcode will be deleted. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Inventory wands will only use barcodes of material not currently checked out.

Barcodes collected during circulation transaction are not stored to ensure privacy. RFID gates and inventory wands only track items not connected with a patron account, so purging is less frequent. Security gate logs are retained to give staff the time to check the title provided and to interact with patron. RFID gate logs will retain data only for titles not checked out and only for period designated by the library. Currently the time period is set for 5 minutes. Inventory wands will only use barcodes of material not checked out.

8. How collected information can be accessed or used by members of the public, including criminal defendants

Data are not stored.

9. Which governmental agencies, departments, bureaus, divisions, or units that may receive data collected by the Surveillance Technology operated by the Department, including any required justification or legal standard necessary to share that data and how it will ensure that any entity receiving such data complies with the Surveillance Technology Policy.

Data are not stored nor shared. Only assigned library staff will be allowed to use the technology. The Library has a Privacy Policy and Privacy Inventory that governs how circulation data will be handled by staff.

10. The training required for any individual authorized to use the Surveillance Technology or to access information collected by the Surveillance Technology

Every staff member likely to use the technology will be trained on using this technology. Staff need to be trained on how to launch the Bibliotheca Staff connect software, how to toggle between checking in material and checking out material, and how to ensure the cursor is in the Sierra ILS database input box to ensure the barcode number will be transferred.

11. The mechanisms to ensure that the Surveillance Technology Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the sanctions for violations of the policy

Department shall oversee and enforce compliance with this Policy using the following methods:

The Library will provide the Policy document and overview on internal intranet and on the public website.

Department shall assign the following personnel to oversee Policy compliance by the Department and third-parties.

Michael Liang, Chief Information Officer, San Francisco Public Library

Sanctions for violations of this Policy include the following:

The Library would work within existing City and departmental human resources guidelines to address and determine appropriate sanctions.

12. What procedures will be put in place by which members of the public can register complaints or concerns, or submit questions about the deployment or use of a specific Surveillance Technology, and how the Department will ensure each question and complaint is responded to in a timely manner.

Complaints or concerns can be submitted to the Department in person, by phone, in writing that can be turned in by mail or in person, or electronically via the library's chat service, or "Comments and Suggestions" page.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response. To do so, Department shall forward all questions and complaints to the proper internal department entities for timely response.