WESTCHESTER LIBRARY SYSTEM (WLS) **POLICY #18**

Subject: Data Security Program, Safeguards and Policy

Application: Employees, trustees, customers, consultants, contractors, vendors and visitors

Purpose:
In order to maintain a secure operating environment that safeguards private data of both patrons of Westchester Library System (WLS) member libraries and WLS employees, the following policy will address:

- Scope of WLS' information security role regarding the NYS SHIELD Act
- Roles within WLS that function to maintain information security
- Definition, inventory and limits on data stored in WLS systems

Scope of Policy:
The NYS SHIELD Act which took effect in March 2020 changes how businesses respond to both potential and confirmed data breaches on electronic systems.

WLS, having less than 50 total employees, is defined as a "small business" by the NYS SHIELD Act. As a small business WLS must adopt a security program with "reasonable administrative, technical and physical safeguards that are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

The scope of data covered under this policy is limited to "private data" as defined in NYS General Business Law 899-bb2(b) and 899-aa (1) (a) and (b).

Roles:
The senior information technology (IT) employee at WLS will serve as the Data Security Coordinator. The Data Security Coordinator, or their appointee, will be responsible for implementing data safeguards for member library data held on WLS systems. The Data Security Coordinator will report directly to the Executive Director in all matters relating to the data security program regardless of direct reports defined in their job description.

The Data Security Coordinator will further develop and maintain an inventory of all private information as defined in the scope section of this policy. The inventory will include the data point, storage location and users impacted in the event of a breach or potential breach. The portion of the inventory impacting public users (library patrons) is to be posted on the WLS website Privacy Page. The inventory and public posting are to be updated no less frequently than annually.

The WLS employee charged with managing Human Resources data is responsible for implementing the safeguards as it relates to data about WLS employees.

Access Control:
The NYS Office of the State Comptroller (OSC) guidelines will serve as the primary source for

best practices. Any WLS system that stores data safeguarded under this policy must comply with the OSC guidelines for IT Governance regarding access control including, but not limited to:

- "A review of all system accounts [will] be periodically conducted and any account that cannot be associated with an authorized user or application [will] be disabled."
- "Each user should have his or her own user account (username and password)"
- Passwords will be maintained with length, complexity and history requirements set by the WLS IT Department in alignment with the OSC guidelines.

The entire OSC guide on IT Governance can be found here:
https://www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Data Stored on WLS Systems by Member Libraries:
WLS maintains two systems that have the potential to store data safeguarded under this policy:

- Shared Library Management System (LMS)
- File servers

Shared Library Management System (LMS)
The LMS is used to manage patron accounts for the lending of physical materials and patron user account authentication for access to electronic resources. The following chart defines patron data points specifically authorized for and barred from use on the LMS:

Authorized Data	Unauthorized Data
• Name • Address • Telephone number • Email address • Date of birth • Library card number • Account PIN or password • Reserve and transaction data	• Social Security ID number • Driver's license or non-driver ID number • Credit/debit card number • Bank account number • Biometric information including photos

WLS recognizes the username or e-mail address in combination with PIN or password used to access a patron's online account constitutes private information protected by the NYS SHIELD Act. Should this information be breached or suspected of being breached, WLS will change the user password for each account. The new password will be communicated to each patron via email along with notification of the breach or potential breach.

File Servers
WLS provides member library access to file servers. These file servers store the data in users' "My Documents" folders as well as file shares for each library. Under this policy the use of these file server services by any member library for the purpose of storing any data that is defined as "private data" referenced in the "scope" section of this policy is unauthorized.

Upon adoption of this policy and annually thereafter, member libraries will be notified of the data points specifically unauthorized and notified to take action to remove these data points from

the LMS and file servers if presently in use. The notification will further inform the library that any unauthorized data stored in the LMS and on file servers is done so at the sole liability of the member library.

Data Minimization for Member Libraries
Data minimization in this regard refers to reducing the amount of private data as defined by the NYS SHIELD Act stored in electronic form on these systems.

It is generally accepted that libraries use one or more of the unauthorized data points to eliminate duplicate registrants, to verify residency or other registration purposes. The intent of this policy is not to dissuade a library from continuing to use these data points for that purpose, but rather to ensure that the library will not store it in the shared LMS and create a point of compliance.

It is further recommended that member libraries take inventory of all private data stored in any other electronic systems and to implement practices of data minimization to reduce the impact of NYS SHIELD Act compliance in the event of breach or potential breach on any system used by the member library.

Data Stored on WLS Systems for Internal Human Resource Management:

WLS stores multiple instances of data defined as private information protected by the NYS SHIELD Act for the purpose of managing human resources as both active personnel and retirees. This data includes, but is not limited to, Social Security ID numbers and bank account information. WLS will follow the OSC guidelines for securing access to these information resources.

Should a breach or potential breach occur, employees and/or retirees whose data may have been impacted by such a breach will be notified of such compromise by hand-delivered letter with acceptance acknowledgement or certified mail with return receipt.

Data Minimization
Human resources staff will make every effort to practice data minimization. In this context data minimization refers to keeping as few electronic records as possible that contain data points defined as private as referenced in the scope section of this policy.

Internal Compliance Audits
The Data Security Coordinator or their designee shall be granted access necessary to conduct periodic reviews, to take place no less frequent than annually, to ensure compliance with the access control guidelines set forth by the OSC and the data minimization guidelines herein.

Approved: September 29, 2020