# Data Breach Preparation, Prevention, and Response Policy

Commented [RK1]: Policy drafted by System Attorney. Edited by Ron, Bob, Dan, and Kathryn.

## Purpose

To promote the mission of the System, operate in harmony with the ethics of the American Library Association and New York Library Association, and ensure compliance with applicable laws, the System shall follow the below-stated policy and procedure regarding data breach preparation, prevention, and response.

It shall be the policy of the System to ground its conditions and practices for data security and privacy with awareness of the shifting landscape of obligation and exposure created by its evolving services to member libraries and changing laws and regulations.

## Conditions

The System is a cooperative library system that operates and provides the following data-related services under the following conditions to member libraries:

| Service | Role of System | Set by |
|---|---|---|
| Integrated Library System ("ILS") | Owner and responsible party | State law, regulation, and the System's "Systems Access and Confidentiality of Library Records Policy" |
| E-mail service to member library employees | Service provider to member | System's procedure and "Systems Access and Confidentiality of Library Records Policy." |
| Members' self-contained computer networks | Service provider to member | INSERT |
| Access to databases | Service provider to member | State law, regulation, and the System's "Systems Access and Confidentiality of Library Records Policy" |
| IT purchasing | Service provider to member | The System's "Procurement Policy" |

*For avoidance of doubt:*

- *The aggregated content and operating system of the ILS is a System asset; the System owns and is responsible for the security of the contents;*

- *The e-mail ETC are services provided by the System to its members; the members own and are responsible for the contents;*
- *The members' self-contained computer networks are…*

## Data Security Practices

As a "small" business that owns or licenses computerized data which includes private information of a resident of New York, the System develops, implements, and maintains reasonable safeguards to protect the security, confidentiality, and integrity of the private information including, but not limited to, disposal of data.

To accomplish this goal, the System maintains a data security program that includes the following:

1. designates one or more employees to coordinate the security program;
2. identifies reasonably foreseeable internal and external risks;
3. assesses the sufficiency of safeguards in place to control the identified risks;
4. trains and manages employees in the security program practices and procedures;
5. selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
6. adjusts the security program considering business changes or new circumstances;

and implements reasonable technical safeguards such as the following, in which the person or business:

1. assesses risks in network and software design;
2. assesses risks in information processing, transmission, and storage;
3. detects, prevents, and responds to attacks or system failures; and
4. regularly tests and monitors the effectiveness of key controls, systems, and procedures;

and implements reasonable physical safeguards such as the following, in which the person or business:

1. assesses risks of information storage and disposal;
2. detects, prevents, and responds to intrusions;
3. protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and
4. disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

## Data Breach Disclosure Practices

A. Data Breach impacting the System's services to members

With respect to services it provides to members as a vendor (meaning that, as contemplated by General Business Law 39-F, the System maintains a member's "computerized data which includes private information which the System does not own or control"), the System shall notify the member who owns the information of any breach of the security of the system immediately

following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

B. Data Breach impacting System-owned and System-controlled data

The System shall disclose any breach of the security of a system it owns, operates and controls following discovery or notification of the breach in the security of the system to any resident of New York state whose **private information** was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the integrity of the system.

The notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation; if such delay is required, notification shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

Regardless of the method by which notice is provided, such notice shall include contact information for the System, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

In the event that any New York residents are to be notified, the person or business shall notify the state attorney general, the department of state and the division of state police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons. In the event that more than five thousand New York residents are to be notified at one time, the System shall also notify consumer reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected persons.

## Data Breach Response Practices

In the event of a "data breach," "data compromise," "identity theft," "computer attack," or "cyber extortion threat" insured under this coverage form, in addition to the notification response outlined in "Data Breach Disclosure Practices," above, the System will:

1. Notify the police if a law may have been broken.
2. Notify its insurance carrier as soon as practicable, but in no event more than 60 days after the "personal data compromise," "identity theft," "computer attack," or "cyber extortion threat." This will include a description of any property involved.

3. As soon as possible, give the carrier a description of how, when, and where the "personal data compromise," "identity theft," "computer attack," or "cyber extortion threat" occurred.

These practices shall be reviewed on an annual basis to ensure the System is considering the requirements of the carrier in crafting its response.

## Definitions

This policy uses the following definitions:

1. "**Personal information**" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

2. "**Private information**" shall mean either:

    a. personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:
        i. social security number;
        ii. driver's license number or non-driver identification card number;
        iii. account number, credit, or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;
        iv. account number, credit, or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
        v. biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity;

    or

    b. a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

    "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

3. "**Breach of the security of the system**" shall mean unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of private information maintained by a business. Good faith access to, or acquisition of, private information by an employee or agent of the business for the purposes of the business is not a breach of the security of the

system, provided that the private information is not used or subject to unauthorized disclosure.
In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person or a person without valid authorization, such business may consider, among other factors, indications that the information was viewed, communicated with, used, or altered by a person without valid authorization or by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:

a. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
b. indications that the information has been downloaded or copied; or
c. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

4. "**Unauthorized access incident**" means the gaining of access to a "computer system" by:

   a. An unauthorized person or persons; or
   b. An authorized person or persons for unauthorized purposes.

5. "**Affected Individual**" means any person who is the System's current, former, or prospective customer, client, member, owner, student, director, or employee and whose "personally identifying information" or "personally sensitive information" is lost, stolen, accidentally released, or accidentally published by a "personal data compromise" covered under this Coverage Form. This definition is subject to the following provisions:

   a. "Affected individual" does not include any business or organization. Only an individual person may be an "affected individual."
   b. An "affected individual" must have a direct relationship with your interests as insured under this policy. The following are examples of individuals who would not meet this requirement:

      i. If you aggregate or sell information about individuals as part of your business, the individuals about whom you keep such information do not qualify as "affected individuals." However, specific individuals may qualify as "affected individuals" for another reason, such as being an employee of yours.
      ii. If you store, process, transmit, or transport records, the individuals whose "personally identifying information" or "personally sensitive information" you are storing, processing, transmitting, or transporting for another entity do not qualify as "affected individuals". However, specific individuals may

qualify as "affected individuals" for another reason, such as being an employee of yours.

iii. You may have operations, interests, or properties that are not insured under this policy. Individuals who have a relationship with you through such other operations, interests or properties do not qualify as "affected individuals". However, specific individuals may qualify as "affected individuals" for another reason, such as being an employee of the operation insured under this policy.

6. "**Computer attack**" means one of the following involving the "computer system":

   a. An "unauthorized access incident";
   b. A "malware attack"; or
   c. A “denial of service attack” against a “computer system.”

7. "**Computer system**" means a computer or other electronic hardware that is owned or leased by the System and operated under the System's control.

8. "**Cyber extortion threat**" means a demand for money from the System based on a credible threat, or series of related credible threats, to:

   a. Launch a "denial of service attack" against the "computer system" for the purpose of denying "authorized third party users" access to your services provided through the "computer system" via the Internet;
   b. Gain access to a "computer system" and use that access to steal, release or publish "personally identifying information", "personally sensitive information" or "third party corporate data";
   c. Alter, damage or destroy electronic data or software while such electronic data or software is stored within a "computer system"; or
   d. Launch a "computer attack" against a "computer system" in order to alter, damage, or destroy electronic data or software while such electronic data or software is stored within a "computer system.”

9. "**Denial of Service Attack**" means an intentional attack against a target computer or network of computers designed to overwhelm the capacity of the target computer or network in order to deny or impede authorized users from gaining access to the target computer or network through the Internet.

10. "**Malware Attack**" means an attack that damages a "computer system" or data contained therein arising from malicious code, including viruses, worms, Trojans, spyware, and keyloggers. "Malware attack" does not mean or include damage from shortcomings or mistakes in legitimate electronic code or damage from code installed by the System or a member.

11. "**Personal Data Compromise**" means the loss, theft, accidental release, or accidental publication of "personally identifying information" or "personally sensitive information" as respects one or more "affected individuals".