

[Your Agency OR BROKERAGE Name]
**Cybersecurity policy**

Date updated
4/12/24

 Template provided by our association: 

**INTRODUCTION**

# What is this?

Licensed insurance agents and brokers must comply with Part 500 of Title 23 of the New York Codes, Rules, and Regulations titled *Cybersecurity Requirements For Financial Services Companies.* One of the regulation’s sections requires them to create and apply cybersecurity policies and procedures. The Big I New York team created this template to help agencies and brokerages meet that requirement.

All agencies and brokerages, including those that qualify for the Limited Exemption under Section 500.19 of the regulation, may use this guide. Visit [www.BigINY.org/cyber](https://www.BigINY.org/cyber) to determine if your agency qualifies.

# How do I use it?

* Review each of the template’s sections to see if they apply to your agency’s operations.
* Modify provisions that apply to your agency to make them more precise, if necessary.
* Delete provisions that do not apply to your agency.

Some pages contain sections labeled **THINGS TO CONSIDER**. These are suggestions of provisions that you may want to insert if they apply to your agency’s operations. However, they do not apply to all agencies. For example, some apply to agencies that do business in multiple states. If your agency does business only in New York, you can skip those suggestions.

Once you are satisfied with the written policy:

* Insert your agency’s name on the front page.
* Save a copy electronically where all individuals who use your computer systems can retrieve it.
* If you wish, print copies.
* Distribute print and/or electronic copies to all users of your computer systems.
* Instruct those users to review it.
* Enforce it as written.
* Review and revise it as necessary at least once a year. As your business changes, you may need to review and revise more often.

# Important THINGS TO REMEMBER

* This is not a “one size fits all” template. Provisions that apply to a 200-person agency might not apply to a three-person agency, and vice versa. Do not use this template as written. Customize it to reflect your agency’s operations and the things you need to do to protect the agency and its clients.
* Keep your policy easily accessible for:
	+ Users of your computer systems to refer to, and
	+ Giving it to the New York State Department of Financial Services upon their request.
* The federal Gramm-Leach-Bliley Act (implemented in New York as Insurance Regulations 169 and 173) requires licensed entities to provide annual privacy policy statements to customers and consumers. Review your privacy policy statements to ensure that your cybersecurity policy backs up the promises you’ve made in them.
* The Big I New York team will update this template as changes warrant. We created this update in response to the November 2023second amendment to the regulation. Check [www.biginy.org/cyber](http://www.biginy.org/cyber) on occasion to see if we have published a new update.
* This template will help you comply with the regulation. It will also help you protect your agency and your clients. For the sake of your agency’s future and the people and businesses you insure, we urge you to spend some time customizing it and ensuring that your computer users follow it.

#  Document definitions

In this description of this agency’s cybersecurity policies and procedures, certain words and phrases have specific meanings. You can recognize them in the text because the words start with capital letters. We have listed them below, all but two in alphabetical order. Check back here to verify what those words and phrases mean.

**You** or **Your** means an Authorized User of this agency’s Computer Systems.

**We**, **Our,** and **Us** means this insurance agency, [INSERT AGENCY’S NAME].

**Authorized User** means any person we have authorized to access our Computer Systems and electronic data. Examples include people we hire to be:

* Employees.
* Vendors.
* Consultants; and
* Independent contractors.

[NOTE: If your agency qualifies for the limited exemption, the next definition is optional.]

**Board of Directors** means this agency’s elected or appointed board of directors.

**Chief Information Security Officer (CISO)** means the person responsible for:

* Overseeing and implementing our Cybersecurity Program, and
* Enforcing the provisions of this Cybersecurity Policy.

**Computer Systems** means sets of electronic devices (that We or others own) that:

* Can accept, store, process, and transmit information; and
* Use software for processing, storing, retrieving, and transmitting data.

Devices that may be part of Our Computer Systems include:

* Desktop and laptop computer workstations.
* Tablet computers such as iPads or Surface devices.
* Smartphones.
* Desktop telephones.
* Printers.
* Copiers.
* Fax machines; and
* Any other electronic device capable of connecting to a computer network.

**Cybersecurity Incident** means a successful or unsuccessful act or attempt to access, disrupt, or misuse our Computer Systems or electronic data. We consider it to be a Cybersecurity Incident only if:

* It impacts Us and federal or state law requires us to notify law enforcement authorities.
* It is likely to harm a significant part of Our normal operations; or
* It results in Us suffering a ransomware attack on a significant part of our computer systems.

**Cybersecurity Policy** means Our policies and procedures, as described in this document, for protecting Our Computer Systems and the NPI We have stored on them.

**Cybersecurity Program** means a program to keep Computer Systems and the NPI stored on them confidential, available, and complete. A Cybersecurity Program includes:

* The electronic devices that we use to receive, process, and transmit information.
* The software that those devices use for those functions.
* Electronic devices and software designed to protect Computer Systems and NPI; and
* The organization’s Cybersecurity Policy.

**GDPR** means the European Union General Data Protection Regulation as explained at <https://gdpr.eu/>.

[NOTE: If your agency qualifies for the limited exemption, the next definition is optional.]

**Independent Audit** means an audit of our Cybersecurity Program that auditors from inside or outside the agency conduct. The auditors conducting the Independent Audit will be free to make decisions. This agency, its owners, and its employees will not influence the auditors’ decisions.

**ISO/IEC-27000** means the International Organization for Standardization’s Family of Standards for managing and securing confidential information as explained at <https://www.iso.org/standard/iso-iec-27000-family>.

**Multi-Factor Authentication (MFA)** means a process whereby an authorized user cannot gain access to our Computer Systems without inputting at least two of these types of verification factors:

* A factor the user knows, such as a password.
* A factor the user possesses and must retrieve, such as a string of numbers; or
* A physical feature of the user, such as the person’s eyes or face.

**New York Financial Services Cybersecurity Requirements Regulation** means Part 500 of Title 23 of the New York Codes, Rules and Regulations (23 NYCRR 500,) as cited at <https://www.dfs.ny.gov/industry_guidance/cybersecurity>.

**NIST SP 1300** means the National Institute of Standards and Technology – *NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide* at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf>.

**NIST CSF 2.0** means the National Institute of Standards and Technology’s Cybersecurity Framework 2.0 as described at <https://doi.org/10.6028/NIST.CSWP.29>.

**Non-Public Information (NPI)** means information that We possess in our Computer Systems that:

* Is not Public Information, and
* We do not want to make freely and easily available to people who are not Authorized Users.

This information includes:

* Our business information that would harm our business if someone other than an Authorized User were to change, disclose, or access it.
* Information about individual people that someone other than an Authorized User could use to identify them. This information includes the person’s name, number, or other identifier combined with another piece of information that is unique to that person. For example:
	+ Han Solo, Social Security number 111-11-1111.
	+ Han Solo, New York driver’s license number 111 111 111.
	+ Han Solo, agency account number 11 1111 111 1.
	+ Han Solo, Visa card number 1111 1111 1111 1111.
	+ Han Solo, bank checking account personal identification number (PIN) 1111.
* Information about people, other than their age or gender, created or derived from a health care provider about:
	+ Past, present, or future health conditions the person or a family member has experienced.
	+ The person’s receipt of health care; and
	+ The person’s payments for health care.

**OWASP** means the Open Web Application Security Project (<https://owasp.org/>.)

[NOTE: If your agency qualifies for the limited exemption, the next definition is optional.]

**Penetration Testing** means assessing Our Computer Systems’ security by attempting to skirt or overwhelm its security features. We perform the test by authorizing certain Authorized Users to attempt to penetrate the systems and their databases. These Authorized Users may attempt to penetrate the systems from inside or outside of them.

**Public Information** means information about individual people that We have reason to believe is legally available to the public because it came from:

* Government records;
* Media that is widely and easily accessible; or
* A disclosure that a law required someone to make.

We consider information to be public if the individual involved has had an opportunity to opt out of having the information shared publicly and has not opted out.

**Risk Assessment** means the process of examining Our Computer Systems to:

* Identify, measure, and prioritize the cybersecurity risks to Our operations, property, employees, clients, other organizations, and critical infrastructure; and
* Identify tools, processes, rules, and other methods to reduce or eliminate the risks.

[NOTE: If your agency qualifies for the limited exemption, the next definition is optional.]

**Senior Officer** means the principal of this agency or another person he or she has designated to be responsible for Our Cybersecurity Program.

**Secure Socket Layer (SSL) Tunnel** **VPN** means a secure computer networking technology. It uses an encrypted data channel to enable an individual using a Web browser to securely access multiple services on a network. See <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf> for more information.

**SOC2 and/or SOC for Cybersecurity** mean the Service Organizations Controls for Certified Professional Accountants standards as described at <https://www.aicpa-cima.com/topic/audit-assurance/audit-and-assurance-greater-than-soc-2>.

**System Administrator** means an Authorized User whom We have authorized to perform functions in our Computer Systems that:

* Relate to security; and
* We do not allow other Authorized Users to perform.

These functions may include:

* Adding, changing, or removing Authorized Users’ accounts; and
* Making changes to the Computer Systems’ configurations.

**Third-Party Service Provider (TPSP)** means a person or organization that:

* We do not own.
* That does not own Us.
* Is not under common ownership with Us by someone else.
* Is not an entity of any government.
* Provides services to Us; and
* As part of those services, maintains, processes, or otherwise has access to Our NPI.

[NOTE: If your agency qualifies for the limited exemption, the next definition is optional.]

**Transport Layer Security (TLS) Encryption** means a technology designed to provide communications security over a computer network. For more information, read the Agents Council for Technology article [*Protect Your Clients with Secure Email Using TLS*](https://www.independentagent.com/ACT/Pages/planning/SecurityPrivacy/ACT_1208.aspx).

**Virtual Private Network (VPN)** means a process for creating a secure connection between either a computing device and a network or between two networks. A VPN uses an insecure connection (that is, the public internet) to create a secure connection.

#  INFORMATION SECURITY

The purpose of this Cybersecurity Policy is to create effective:

* Administrative
* Technical
* Electronic, and
* Physical

safeguards to protect:

* Non-public information (NPI)
* Our premises’ physical security, and
* The integrity of Our Computer Systems.

This Policy describes Our procedures for electronic and physical methods of:

* Accessing
* Collecting
* Destroying
* Protecting
* Storing
* Transmitting, and
* Using

Our clients,’ employees,’ and Our NPI. It also describes how Authorized Users may use Our Computer Systems. We have based our procedures for using Our Systems on what we consider to be appropriate uses. We have also considered laws and regulations that may apply.

In creating and applying this Policy, we have Identified risks that we can foresee. These include risks from inside and outside this agency to the:

* Security
* Confidentiality, and
* Integrity

of records, electronic and paper, containing NPI.

We have also:

* Judged how likely the threats are to occur and how dangerous they are, given how sensitive the NPI is.
* Evaluated whether the policies, procedures, and safeguards we are using now are sufficient to minimize the threats.
* Created and employed safeguards, as laws and regulations may require, to minimize the threats.
* Acted to monitor how effective the safeguards are.

We will annually review and re-evaluate all security measures this Policy describes. We will also do so when:

* Applicable laws or regulations change, or
* When Our business activities change.

We may change this Policy at any time. We will try to give advance notice of any changes to Authorized Users, but we cannot promise that we will do so.

#  EMPLOYEE RESPONSIBILITY

Each employee of this agency is responsible for:

* Carefully reading
* Understanding, and
* Adhering to

this Policy. We will train each employee with access to NPI on this Policy as necessary.

#  CHIEF INFORMATION SECURITY OFFICER [or INFORMATION SECURITY COORDINATOR]

NOTE: Substitute “an information security coordinator (ISC)” for “chief information security officer” if your agency does not have a CISO.

NOTE: Designate the CISO or ISC by position instead of name. That way the agency will not have to change the policy if the personnel changes.

We have designated a chief information security officer (CISO.) The CISO oversees this Policy’s implementation.

The CISO:

1. Implements this Policy.
2. Tests and evaluates its safeguards.
3. Reviews its security measures either:
* Annually, or
* When laws, regulations, or Our business activities change.
1. As necessary, trains employees who can access NPI.
2. Applies measures to secure:
* Our Computer Systems and
* NPI

that Third-Party Service Providers can access or hold.

# A blue circle with a lock in it  Description automatically generated RISK ASSESSMENT

We cannot design an effective Cybersecurity Program unless We know what Our risks are. To determine the types and severity of Our cybersecurity risk, We will conduct a cyber risk assessment:

* At least once per year between January 1 and March 31, or
* More often if Our business changes or We become aware of new cybersecurity threats.

The CISO [INSERT “ISC” IF YOUR AGENCY DOES NOT HAVE A CISO] or individuals he or she may designate will conduct the risk assessment.

The assessment will contain two parts:

1. Identifying and Classifying the Risks and Threats, including:

* **Internal threats** from Authorized Users and devices and software We use in Our business.
* **External threats** from members of the public and malicious code.

We will classify each risk or threat as follows:

* **Low** – the threat is unlikely to disrupt Our operations in a significant way.
* **Moderate** – the threat may cause a noticeable disruption in Our operations.
* **Severe** – the threat is likely to disrupt Our operations in a significant way or even halt them.

We will further classify each risk or threat as:

* **Acceptable** – one that We do not need to eliminate or reduce.
* **Unacceptable** – one that We must eliminate or reduce.

2. Assessing Our Computer Systems and NPI, including their:

* Confidentiality.
* Integrity.
* Security, and
* Availability.

We will compare Our existing cybersecurity controls to the unacceptable threats we face. We will classify each control’s adequacy as:

* **Poor** – the control is unlikely to prevent a Cybersecurity Incident.
* **Adequate** – the control does the minimum to prevent a Cybersecurity Incident.
* **Superior** – the control is more likely than not to prevent a Cybersecurity Incident.

#  DATA GOVERNANCE & CLASSIFICATION

### SPECIAL PROTECTION FOR NONPUBLIC INFORMATION

We and Our Authorized Users will accord NPI the highest level of confidentiality.

Examples of NPI are any of the following combined with an individual’s first name or initial and their last name:

1. Social Security number.
2. Driver’s license number.
3. Passport number.
4. State-issued identification card number.
5. Financial account number.
6. Credit or debit card number.
7. Identifiers the individual uses to make financial transactions such as access codes and PIN codes.
8. Health information.
9. Unique biological or behavioral characteristics.

We will treat all of these (other than the last item) as NPI.

### WHERE WE STORE NONPUBLIC INFORMATION

We store NPI in several places. They may be on or off Our premises. We may create and maintain the NPI, or third parties may do so on Our behalf. These places may include:

1. Paper and electronic information on clients and employees stored in:
* Desks.
* File cabinets.
* Storage closets.
* Desktop and laptop computers.
* Mobile computing devices.
* Our computer servers or those of Our vendors.
1. Backup copies of Our electronic data stored anywhere offsite.
2. The premises of TPSPs that have access to Our data.

This Policy’s purpose is to protect Our NPI from unauthorized access, distribution, and/or use.

No Authorized User may distribute, communicate, or store any of Our NPI on or through any social media websites or services. There are no exceptions to this rule.

DATA RETENTION

We will retain NPI that is personally identifiable or health information on current clients so long as they remain Our clients.

Where We have offered quotes for one or more policies but did not obtain the business, we will retain those types of NPI associated with those quotes [ENTER “IMMEDIATELY” OR CHOOSE ONE OR MORE OF THE FOLLOWING.]

|  |  |
| --- | --- |
| Indefinitely |  |
| Personal auto insurance |  for 3 years |
| Homeowners insurance | for 3 years |
| Personal watercraft insurance | for 3 years |
| Personal inland marine insurance  | for 3 years |
| Commercial auto insurance  | for 3 years |
| Other coverages | for 3 years |

[NOTE: THESE ARE JUST EXAMPLES THAT YOU ARE NOT REQUIRED TO USE. YOU CAN SELECT YOUR OWN TIMEFRAMES.}

We will follow these retention schedules except where:

* Relevant laws or regulations require us to retain them beyond those schedules, or
* Where We lack the ability to dispose of the records because the vendor from whom we have obtained our agency management system has not given us that ability.

Authorized Users must follow Our document retention schedule and requirements. Authorized Users will destroy paper and electronic records, when it is time to do so, in ways that make reading or reconstructing them impossible.

We use a commercial shredding company for destroying paper documents unless the CISO directs otherwise. The CISO will coordinate discarding of any electronic or computerized devices that can store electronic data. Any Authorized User discarding these devices must take care to render hard drives or other storage media unreadable.

**THINGS TO CONSIDER – OTHER STATES’ LAWS**

If your agency does business in multiple states, review those states’:

* Breach notification laws.
* Privacy laws, and
* Insurance laws and regulations.

Do this also for states where your Authorized Users reside if they hold NPI. Verify that your policy’s definition of NPI meets those states’ requirements.

State privacy laws typically require businesses to keep individuals’ information confidential. State data breach notification laws typically require them to notify:

* Affected individuals.
* Regulators, and/or
* Law enforcement

if someone improperly accesses this information.

Information about other states’ laws is available on the [Other States page](https://www.biginy.org/discover/ac/pages/cybersecurity/otherstates/default.aspx) in the [Cybersecurity section](https://www.biginy.org/discover/ac/Pages/Cybersecurity/default.aspx) of the Big I New York website.

**THINGS TO CONSIDER – HIPAA**

Review the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. There are circumstances where HIPAA’s rules for treating Protected Health Information (PHI) may apply to an insurance agency. The [U.S. Centers for Medicare & Medicaid Services](https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf) has information on these rules.

**THINGS TO CONSIDER – NPI STORAGE**

Identify every place your agency stores NPI to make sure you are:

* Effectively managing and protecting it, and
* Making it accessible only to those who need it to do their jobs.

Also, consider whether keeping the NPI in all these places is necessary or even storing it is necessary. If you decide not to keep it, follow your cybersecurity policy and relevant laws and regulations to destroy it. The methods could include:

* Shredding paper records.
* Securely deleting or erasing electronic records.
* Other secure methods.

#  ASSET INVENTORY & DEVICE MANAGEMENT

1. At all times, Authorized Users:

* Should keep mobile electronic devices (smartphones, tablets, or others) with access to NPI in:
	+ Their possession
	+ A secure location.
* Must not share passwords or other access information with others.
* Must keep mobile electronic devices password-protected when they are not using them.

2. Without Our authorization, Authorized Users must not put any of Our electronic data on:

* Thumb drives.
* Laptops.
* Other portable media, drives or devices.

3. If We have given authorization to store Our electronic data on these media and devices, Authorized Users should:

* Encrypt the data, and
* Password-protect the media and devices.

4. If an Authorized User separates from Our employment, the employee must:

* Immediately prior to or at the time of termination, return to Us all Our NPI or other information stored in paper or electronic form.
* Return to Us all keys, identifications, access codes, and/or badges.
* Not retrieve Our NPI.

5. We will follow Our human resources policies when an employee separates from employment. We will disable that individual’s access to Our email and voice mail accounts and transfer it to other employees. We will de-activate those accounts when We deem appropriate.

6. Employees must report all actual or suspected unauthorized access, use, or disclosure of NPI to the CISO.

7. We will keep records of the location and the possessor of all Our electronic assets (devices and software.) The CISO [INSERT “ISC” IF YOUR AGENCY DOES NOT HAVE A CISO] will maintain a spreadsheet or similar type of journal for this purpose. The records will include:

* The type of asset.
* Who owns it if not Us.
* The name of the Authorized User who possesses it.
* Its location.
* How concerned We should be if We could not locate it.
* The date manufacturer or vendor support for it will end.
* How quickly We need to recover it should it go missing.

To ensure that Our records are up to date, We will update and validate these records at least [PICK ONE – DAILY/WEEKLY/MONTHLY/QUARTERLY/SEMI-ANNUALLY/ANNUALLY/OTHER PERIOD.]

8. When We decide to dispose of or replace assets:

* The Authorized User who possesses it must return it to Us as soon as reasonably possible.
* The CISO [OR “ISC”] will securely delete all NPI from the asset or verify that another has done so.
* Dispose of the asset in a manner that permits recycling of it or its components wherever possible.

#  ACCESS CONTROLS & IDENTITY MANAGEMENT

### Internal Controls

We will take the following measures to defend against internal risks to Our NPI records’ security, confidentiality, and integrity.

1. Authorized Users must input a user identification (ID) factor and password to access Our Computer Systems.
2. Authorized Users of Our mobile electronic devices should be able to use them only after inputting a password. We prefer that Authorized Users encrypt their passwords, if reasonably feasible.
3. Authorized Users will have unique ID factors.
4. Passwords must be a minimum of [INSERT DESIRED NUMBER OF CHARACTERS HERE.] They should include a mix of upper- and lower-case letters, numerals, and special characters.
5. Authorized Users must not leave electronic records containing NPI unattended and unsecured. If a User needs to leave the computer with these records open, even briefly, he or she must lock the computer screen.
6. Without advance specific authorization, Users may not:
* Remove paper files from Our premises, or
* Access electronic files remotely.

Users who have obtained authorization must maintain NPI records’ security.

1. We expect Authorized Users to log off or lock computers when they leave them unattended for:
* Breaks.
* Lunch.
* Meetings, or
* When they are out of the office.

We will configure computers to lock up or terminate sessions after ten (10) minutes of inactivity.

1. Unless Authorized Users have good reason to believe that received information came from a trustworthy source, they must not open any:
* Email attachments.
* Links, or
* Applications.

This rule also applies to information from personal email accounts. Users must not use Our equipment to access any applications or other software unless We have approved it.

1. We will retain only the last four digits of credit card numbers. We will not retain bank routing numbers, personal bank account numbers and checks. In accordance with applicable laws and Our business practices, We will destroy all credit- and banking-related information that We choose not to retain.

### External Controls

In addition to the measures We take to protect NPI records from internal risks, We will take these measures to protect against external risks.

1. Our employees must ensure that Our premises are locked when unattended.
2. Our employees will escort visitors to the agency.
3. Unless they are Authorized Users, We will not permit visitors to access Our Computer Systems or property that may contain NPI.
4. Unless they are Authorized Users, We will prevent visitors from wirelessly accessing Our Computer Systems using their own electronic devices.
5. We will employ security measures to prevent members of the public from accessing Our wireless networks remotely.
6. We will maintain servers and other equipment on Our premises in secure locations.
7. We will maintain servers and other equipment on Our premises at a temperature between 50- and 82-degrees Fahrenheit (10 and 28 degrees Celsius.)
8. We will keep filing cabinets that store confidential paper documents locked.
9. Our employees will not leave electronic devices that contain NPI unattended in public places.

### REMOTE ACCESS

We will implement a Virtual Private Network (VPN) and Multi-Factor Authentication (MFA) for any Authorized User who may access Our Computer Systems from outside Our premises. No one may access Our Computer Systems without first entering at least two forms of identifying information and logging in to the VPN.

#  SYSTEMS & NETWORK SECURITY,  OPERATIONS & AVAILABILITY

1. We will use hardware, software, or third-party provided email filter. We will use the filter to help stop malicious computer code from reaching Our Computer Systems. Malicious computer code includes:
* Viruses
* Spyware
* Ransomware
* Other malware.
1. In addition to other appropriate security measures, We will maintain on Our Computer Systems up to date:
* Computer network and firewall protection, and
* Operating system security patches.
1. We will maintain on Our Computer Systems malware protection with up-to-date patches and virus definitions. We will update this protection daily or more frequently if possible.
2. We will keep all backups of our electronic data:
* Password-protected.
* Encrypted, and
* Stored in secure offsite locations.
1. Authorized Users sending NPI via email should ensure that:
* Sending it by email is necessary, and
* They are following this Policy to send it securely.
1. Before we permit a consumer to enter a password or submit NPI to our Computer Systems, We will create a Secure Socket Layer (SSL) tunnel between Our website and the consumer.
2. When an Authorized User attempts to access Our Computer Systems or NPI from a remote location outside Our premises, We will provide a Virtual Private Network (VPN) to enable them to do so securely. We will require Users to use Multi-Factor Authentication (MFA) to log in to the VPN.
3. Employees must not access Our Computer Systems or NPI using home computers or other non-agency equipment without Our written authorization. We will determine whether such access meets Our security requirements. Employees must not store, save, copy, or otherwise retain any NPI on any non-agency equipment.

**THINGS TO CONSIDER – SOFTWARE UPDATES**

Implement procedures to set deadlines for installing updated software.

**THINGS TO CONSIDER – EMAILING NPI**

Because it is easiest for both sender and receiver, use TLS Email Encryption where the recipient can accept it. If that is not possible, try:

* A proprietary email solution if the recipient can accept it.
* Sending a password-protected file. Under this method:
	+ The recipient receives the password separately from the message containing the file, and
	+ Only the recipient would know what is in the password.

Be aware that state laws may still require you to send a breach notification if you send a password-protected file to an incorrect email address.

#  SYSTEMS & NETWORK MONITORING

We will monitor Our Computer Systems and equipment for:

* Authorized Users’ activities, and
* Cybersecurity Incidents.

We will use hardware, software, and/or procedures to record and report these activities and Incidents. In addition, We will install and maintain hardware and software designed to protect Our Computer Systems from malicious computer code such as:

* Computer viruses.
* Malware, and
* Ransomware.

[NOTE: The regulation does not require agencies that qualify for the Limited Exemption to implement the previous measures.]

At least once per year, We require employees to take cybersecurity awareness training. We will either purchase training courses or direct employees to publicly available courses. All training will:

* Address the risks of fraudulent impersonation (also known as “social engineering,”) and
* Reflect the risks We identified in Our most recent Risk Assessment.

We will evaluate TPSPs who can access NPI to ensure that they:

* Have written data security policies.
* Have essential security controls in place.
* Give Us written commitments to safeguard and store Our NPI using security controls at least as strong as Ours; and
* Inform us of any actual, suspected, or potential confidential data breaches.

**THINGS TO CONSIDER – STATE LAWS**

Verify that TPSPs’ commitments comply with:

* Your agency’s policy.
* State security breach notification laws, and
* Other privacy laws and regulations.

#  BUSINESS CONTINUITY & DISASTER RECOVERY

NOTE: The regulation does not require agencies that qualify for the Limited Exemption to create a written incident response plan. However, it does require them to report Cybersecurity Incidents to the New York State Department of Financial Services within 72 hours of determining that one occurred.

**If we suspect or know a Cybersecurity Incident has occurred:**

A security breach is when unauthorized users:

* Acquire
* Spread
* Use, or
* Delete

Our NPI. An employee who suspects or learns that a security breach may have imperiled NPI, or other confidential agency information, must inform the CISO.

NOTE: Substitute ISC for CISO if your agency does not have a CISO.

If a security breach occurs, We will:

* Assess the breach.
* Consult information security experts and/or attorneys.
* Review Our obligations imposed by laws and regulations.
* Notify carriers with policyholders potentially affected by the breach.
* Notify our cyber insurance carrier.
* If laws or regulations require Us to, or if We deem it to be appropriate, notify affected individuals and law enforcement authorities.
* Report the breach to the New York State Department of Financial Services at <https://myportal.dfs.ny.gov/>.
* Take action to contain and control the damage.
* Document those actions.
* Assign an individual to address media inquiries.
* Compose communications about the breach for affected individuals and, if necessary, the public.

**THINGS TO CONSIDER – BREACH NOTIFICATIONS**

New York General Business Law Section 899-aa requires a business that suffers a data breach to notify the New Yor State:

* Attorney General.
* Division of State Police, and
* Department of State, Division of Consumer Protection.

**THINGS TO CONSIDER – OTHER BREACH NOTIFICATION LAWS**

Information about other states’ laws is available on the [Other States page](https://www.biginy.org/discover/ac/pages/cybersecurity/otherstates/default.aspx) in the [Cybersecurity section](https://www.biginy.org/discover/ac/Pages/Cybersecurity/default.aspx) of the Big I New York website. If you suffer a data breach, check with legal counsel to find out if other laws or regulations apply. Laws in other states where you do business or have licensed employees may apply.

If the HIPAA privacy and security rules apply to your agency, its breach notification rule may apply if your data breach involves Protected Health Information. Information about this rule is available in the Big “I”’s memo titled [“HIPAA Breach Notification Rule.”](https://www.independentagent.com/legal-advocacy/SiteAssets/Members-Only/Memoranda/default/HIPAA_BreachNotificationRule092409Final.pdf)

#  Third PARTY SERVICE PROVIDER SECURITY POLICY

This Policy:

* Defines the minimum cybersecurity standards We expect Third-Party Service Providers (TPSPs) to meet, and
* Describes how We will identify and assess the risk of doing business with TPSPs.

To secure NPI that TPSPs can access or hold, We will:

* Identify Our TPSPs, if any.
* Assess the risk each TPSP poses to Our Computer Systems and NPI.
* Perform a diligent search for information about each TPSP’s cybersecurity practices.
* Document any information we uncover through the diligent search.
* Compare this information to Our minimum required cybersecurity practices.
* Informed by that comparison, decide whether to do business with the TPSP.

We require all TPSPs who wish to do business with Us to:

* Limit access to Our NPI by controlling which of their personnel have access.
* Inform Us within 72 hours of a Cybersecurity Incident that directly impacts Our Computer Systems or NPI to which they have access.
* Regularly train their personnel on cybersecurity awareness.
* Meet any other standards that state or federal laws require.

For TPSPs that are “Covered Entities” under the New York Financial Services Cybersecurity Requirements Regulation, we may also require them to:

* Encrypt Our NPI while at rest and in transit, and
* Use MFA when they access Our NPI.

**Our Process For Evaluating Third-Party Service Providers’ Cybersecurity Practices**

We require TPSPs to follow cybersecurity practices designed to protect Our NPI. We need assurance of those practices before We will do business with them. To determine whether they use these measures, We will investigate them. Until We are satisfied that We have the information We need, Our investigation may include the following:

1. Documentation that the TPSP’s practices at least meet any of these published standards:
* The New York Financial Services Cybersecurity Requirements Regulation.
* ISO/IEC-27000.
* SOC2 and/or SOC for Cybersecurity.
* NIST 7621r1.
* NIST CSF.
* OWASP.
* GDPR.
1. Documentation that a qualified third party conducted a cybersecurity vulnerability assessment or audit of the TPSP’s Computer Systems and/or relevant applications. We prefer that the documentation be no more than one year old. The results must show that:
* The TPSP’s Computer Systems contain no vulnerabilities that expose Our NPI or violate New York State laws, or
* The TPSP has taken steps to address vulnerabilities the assessment or audit uncovered.
1. Our review and acceptance of the TPSP’s representations and warranties about their practices to secure Our NPI. We expect them to practice these or more:
* MFA and other controls that limit access to relevant Computer Systems and Our NPI.
* Encryption of Our NPI while it is at rest and in transit.
* Prompt notice to us if a Cybersecurity Incident directly impacting Our Computer Systems or NPI occurs.

We may perform Our investigation by:

* Asking representatives of TPSPs to complete questionnaires that We provide.
* Obtaining governmental and other publicly available reports on a TPSP’s Cybersecurity Program.
* Obtaining from a TPSP documents that describe its Cybersecurity Program.
* Obtaining media reports regarding the TPSP’s cybersecurity practices and Cybersecurity Incident history, if any.
* Obtaining information from any other source where applicable laws and regulations permit.

We recognize that the cyber threat landscape evolves constantly. Because of this, We will conduct periodic re-assessments of the cybersecurity risks posed by Our TPSPs.

**Using Third Party Service Provider to Meet Our Cybersecurity Obligations**

We may employ a TPSP to:

* Implement Our Cybersecurity Program.
* Enforce Our Cybersecurity Policy.
* Serve as Our CISO, or
* All of these.

If We employ the services of a TPSP to perform these functions, We:

* Remain responsible for complying with New York State laws and regulations, and
* Will assign a senior agency employee to direct and oversee the TPSP’s actions.

# A blue circle with a lock in it  Description automatically generated APPLICATION SECURITY AND DEVELOPMENT AND QUALITY ASSURANCE

[**NOTE:** The regulation does not require agencies that qualify for the Limited Exemption to include this in their policies and procedures.]

When we develop any in-house software applications, We will follow the guidelines suggested by OPSWAT at <https://www.opswat.com/blog/application-security-best-practices>. We will also follow those guidelines for:

* Developing.
* Evaluating.
* Assessing, or
* Testing

the security of any applications we obtain from an external source.

The CISO [INSERT “ISC” IF YOUR AGENCY DOES NOT HAVE A CISO] or someone chosen by him or her will review and assess these guidelines at least once per year to determine the need for updates.

# A blue circle with a lock in it  Description automatically generated VULNERABILITY MANAGEMENT

NOTE: The regulation does not require agencies that qualify for the Limited Exemption to include this section in their Cybersecurity Policies.

Our Computer Systems will inevitably develop vulnerabilities to cybersecurity threats. We will not wait until we perform an annual risk assessment to find out what they are. So that we may always know how effective Our Cybersecurity Program is, We will:

* At least once per year, Conduct Penetration Testing from within and outside Our Computer Systems’ boundaries. The CISO [INSERT “ISC” IF YOUR AGENCY DOES NOT HAVE A CISO] will conduct the test or hire a qualified third party to do it.
* Run automatic scans of Our Computer Systems to discover, analyze, and report vulnerabilities. If the automatic scans do not cover some of Our Computer Systems, We will manually scan those systems. How often We will run these scans will depend on the results of Our risk assessment. However, We will run them as soon as practicable after We make any significant changes to Our Computer Systems.

The CISO [INSERT “ISC” IF YOUR AGENCY DOES NOT HAVE A CISO], upon learning of new vulnerabilities, take action to correct them as soon as possible. He or she will give highest priority to vulnerabilities that present the greatest risk or threat to Our Computer Systems and NPI. He or she will inform Our principal promptly of problems that prevent correcting a vulnerability.

TEMPLATE DISCLAIMER

Big I New York offers this sample as one tool for agencies and brokerages to use to develop cybersecurity policies. It is certainly not the only way to create one. We expect all those who use it will change it to fit their own circumstances. We do not intend it to

* Substitute for your own independent evaluation of cybersecurity issues, or
* As formal recommendations that you take any specific steps.

State laws vary in how they apply to agencies and brokerages. Each state has its own unique insurance laws and regulations. States might have data breach notification laws, privacy laws, both, or none. Carefully review the laws and regulations that apply in all states where you do business as you develop your cybersecurity policy. We worked from requirements set forth by several acts as we developed this sample, including:

* The New York financial service regulation 23 NYCRR 500, and
* The federal Gramm-Leach-Bliley Act.

These regulations impose some of the most specific and demanding requirements. Consult appropriate, competent professionals If you need or want individual advice about what to include in your policy.

With permission, we used copyrighted material from the Agents Council on Technology (ACT), the Independent Insurance Agents & Brokers of America, and Big I New York to create this document.

You can find additional information at [www.biginy.org/cyber](http://www.biginy.org/cyber).