[YOUR AGENCY NAME]

CYBERSECURITY POLICY

DATE UPDATED
04/12/17

Note: Refer to the “How to” guide on page 11 for tips on customizing this policy.

DOCUMENT DEFINITIONS

"**Policy**" refers to the Information Security Policy.

"**Agency**" refers to [insert agency name here].

"**Clients**" refers to the Agency's clients, former & prospective clients.

"**Information System**" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

"**Nonpublic Information**" shall mean all electronic information that is not Publicly Available Information and is:

1. Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;
2. Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;
3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

"**Passwords**" refers to a string of characters that, when possible, is at least 8 characters long and contains at least three of the following: upper case letter, lower case letter, a number, a special character (%, &, #, etc.).

"**Person**" means any individual or non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

"**Third Party Servicer Providers**" refers to a person that is not an affiliate of the Agency that provides services to the Agency and maintains, processes or is otherwise permitted access to Nonpublic Information through its provision of services to the Agency.

INFORMATION SECURITY

This Policy for [Agency] (herein after referred to as "Agency") is intended to create effective administrative, technical, electronic and physical protections to safeguard the personal information of the Agency's Clients and employees, the Agency's proprietary and confidential information, the physical security of our premises, and the integrity of our electronic systems so that they are best positioned to function smoothly without interruption.

This Policy sets forth the Agency's procedures for electronic and physical methods of accessing, collecting, storing, using, transmitting, destroying, and protecting Nonpublic Information of Clients, the Agency and/or Agency employees and also the use of the Agency's Systems by Agency employees and any authorized third parties, as deemed appropriate and/or required by applicable laws and regulations.

In formulating and implementing this Policy, we have:

1. Identified reasonably foreseeable internal and external risks to Agency's security, confidentiality and/or integrity of electronic, paper or other records containing Private Information
2. Assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the Nonpublic Information
3. Evaluated the sufficiency of existing Agency policies, procedures, and other safeguards in place to minimize those risks
4. Designed and implemented an approach that puts safeguards in place to minimize those risks, consistent with the requirements of applicable laws/regulations
5. Included regular monitoring of the effectiveness of those safeguards

All security measures contained in this Policy shall be reviewed and re-evaluated annually or when there is a change in applicable laws or regulations or in the business activities of Agency. The Agency reserves the right to modify this Policy at any time, with or without prior notice.

EMPLOYEE RESPONSIBILITY

It shall be the responsibility of each Agency employee to carefully read, understand and adhere to this Policy. Each employee with access to Nonpublic Information shall receive training as necessary on this Policy.

INFORMATION SECURITY COORDINATOR

The Agency has designated [VP of Information Technology (or other title designated for this responsibility)] A as the "Information Security Coordinator" to oversee implementation of this Policy.

The Information Security Coordinator will be responsible for:

1. Initial implementation and maintaining responsibility for implementation of this Policy;
2. Appropriate testing and evaluation of this Policy's safeguards;
3. Reviewing the security measures in this Policy annually or when there is a change in applicable laws or regulations or in business activities of Agency; and
4. Conducting training as necessary for all Agency employees with access to Nonpublic Information.
5. Implementing policies and procedures to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers

DATA GOVERNANCE & CLASSIFICATION

SPECIAL PROTECTION FOR NONPUBLIC INFORMATION

Nonpublic Information is to be accorded the highest level of confidentiality by the Agency and employees.

Examples of Nonpublic Information include, but are not limited to - first name and last name, or first initial and last name, and any one or more of the following:

1. Social Security number
2. Driver's license number, passport number, or state-issued identification card number
3. Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password
4. Personal or protected health information
5. Biometric records

The information listed in 1-4 above, even if it is not connected with a name, should each be treated as Nonpublic Information. B C

WHERE NONPUBLIC INFORMATION IS STORED

The Agency and its employees recognize that the Agency possesses Nonpublic Information in the following places, whether in the Agency's premises or off site, and whether created or maintained by Agency or third parties on behalf of Agency:

1. Hard copy and electronic files on Clients and employees, located at desks, in file drawers, storage areas and on the Agency's Systems
2. Personnel files, Form I-9s, benefits information, payroll information, and direct deposit information for employees wherever located, including but not limited to hard copies at desks, in file drawers and other storage areas, and in electronic form on the Agency's Systems
3. Off-site back-ups, in any form
4. Third Party Service Providers entrusted with Nonpublic Information from the Agency

This Policy is intended to protect Nonpublic Information possessed by the Agency from unauthorized access, dissemination and/or use.

Nonpublic Information may not be disseminated, communicated or stored on or through any social media websites or services, at any time or for any reason. D

Employees will adhere to the Agency document retention schedule and requirements. When it is appropriate to destroy Agency records, paper and electronic records containing Nonpublic Information must be destroyed in a manner in which they cannot be read or reconstructed.

Unless otherwise directed by the Information Security Coordinator, a commercial shredding company will be used to destroy paper documents. When computers, digital copiers, scanners and/or printers with electronic storage capacity, or portable electronic devices and media are discarded, such disposal should be coordinated with the Information Security Coordinator, and care needs to be taken to ensure that the hard drives or other storage media are destroyed in a manner that all data becomes unreadable.

ASSET INVENTORY & DEVICE MANAGEMENT

1. Employees should keep mobile electronic communications devices (such as PDAs, smart phones, etc.) with access to Nonpublic Information in their possession or in a secured location at all times, and Employees will not share passwords or other access information with others.
2. Employees will not put any Agency data on thumb drives, laptops or other portable media, drives and devices unless authorized by the Agency. If so authorized, the thumb drives, laptops or other portable media, drives and devices should be password-protected and encrypted, and the portable mobile electronic communications devices and laptops should be password-protected and encrypted.
3. Employees that no longer work for the Agency must: (1) return to Agency all Agency information (including, but not limited to, any Nonpublic Information) in any form, whether stored on computers, laptops, portable devices, electronic media, or in files, records, work papers, cloud- or web-based storage, etc.; (2) return all keys, IDs, access codes and/or badges; and (3) not access Nonpublic Agency information (including, but not limited to, any Private Information).
4. In accordance with the Agency's human resources manual, access by the former employee to Agency email and voice mail accounts can be immediately disabled and access transferred to other Agency staff to assure a continuity of work, and inactivated when determined appropriate by Agency.

5. Employees are required to report all actual or potential unauthorized access to, use of or disclosure of Nonpublic Information to the Information Security Coordinator.

ACCESS CONTROLS & IDENTITY MANAGEMENT

INTERNAL CONTROLS

1. Agency computers will require a user ID and password and Agency mobile devices should require a password (and be encrypted, if reasonably feasible). Employee log-ins and passwords should be appropriately strong (with the minimum number of characters and other elements required by the Agency's Systems).
2. Electronic files containing Nonpublic Information will not be left accessible to others, such as on computers or portable storage devices accessible (e.g., computer screens must be locked when an employee using such files leaves his or her computer, even briefly). Paper and electronic files must not be removed from the Agency premises or accessed remotely unless specific authorization has been provided in advance, and then, the security of that Nonpublic Information must be maintained.
3. Employees are expected to log off or lock their computers when they leave them unattended (such as when on breaks, at lunch, in a meeting or out of the office). The Agency will implement controls to terminate computer sessions and/or lock computers after a predetermined time of inactivity (e.g., 10 minutes).
4. Employees should not open any email attachment, link, or application where the employee does not reasonably believe the information expected to be accessed is from a trustworthy source. Employees will not use Agency equipment to access any application or software not approved by the Agency.
5. To combat internal risks to the security, confidentiality and/or integrity of records containing Nonpublic Information, the following measures will be taken:
6. The Agency will retain only the last four digits of credit card numbers and will not retain bank routing numbers, personal bank account numbers and checks, and all credit- and banking-related information not retained will be destroyed in accordance with applicable law and Agency-designated business practices.

EXTERNAL CONTROLS

In addition to the measures taken to combat internal risks, the following measures will be taken to minimize external risks to the security, confidentiality and/or integrity of records containing Nonpublic Information:

1. Visitors to the Agency will be escorted within the office and will not have access to Agency computers or property that may contain Nonpublic Information. Guests' wireless access should be fire-walled off from the Agency's Systems.
2. The Agency will maintain security measures so that its wireless networks cannot be accessed remotely by the public.
3. Servers and other equipment at the Agency's premises containing Nonpublic Information will be maintained in a secure location.

SYSTEMS & NETWORK SECURITY, OPERATIONS & AVAILABILITY

1. The Agency will employ an email filter (hardware, software, or third-party provided) that works to restrict and eliminate viruses, spyware and other malware before getting to Agency desktop and portable computers.
2. The Agency will maintain up-to-date network and firewall protection and operating system security patches on its Systems, servers and desktop and laptop computers, as well as other security measures deemed appropriate.
3. The Agency will maintain security software, which includes malware protection with up-to-date patches and virus definitions, on its Systems and its servers, desktop and laptop computers, and all mobile devices, which is updated as frequently as possible, but at least daily. **E**
4. All back-ups will be password-protected and encrypted and kept in a secured location off site.
5. Agency employees should use care in communications (e.g., outgoing email and attachments) to ensure: first, that the Nonpublic Information needs to be sent by email and, if so, that it is transmitted using secure email in accordance with Agency policy. **F**
6. The Agency will create a secure SSL tunnel between its website and the consumer before allowing the consumer to enter any Nonpublic Information or to enter a password.
7. When an employee accesses Agency Systems and/or Nonpublic Information from a remote location, the Agency's secure SSL connection must be used (such as Virtual Private Network (VPN), GoToMyPC, LogMeIn).
8. Employees should not access Agency Systems or Nonpublic Information using non-Agency equipment (e.g., a home computer) unless authorized by the Agency and provided with appropriate firewalls and virus protection, and done through the Agency's secure SSL connection. Employees will not store any Nonpublic Information on any non-Agency equipment.

SYSTEMS & NETWORK MONITORING

1. The Agency will monitor its Systems and equipment for any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System, including but not limited to implementing hardware, software and/or procedural mechanisms to record and report activity for the Systems and equipment.
2. The Agency will exercise due diligence in making sure third-party service providers that are provided Nonpublic Information have the requisite security controls and written policy in place, provide the Agency a written commitment to safeguard and store Nonpublic Information with at least the same level of security controls as the Agency maintains (as outlined in this Policy), and advise the Agency as to any actual, suspected or potential breaches of Private Information. **G**

BUSINESS CONTINUITY & DISASTER RECOVERY

IF A BREACH OF NONPUBLIC INFORMATION (CYBERSECURITY EVENT) OCCURS OR IS SUSPECTED

A security breach occurs when there is an unauthorized acquisition, dissemination, use or loss of Nonpublic Information. Each employee shall be responsible for notifying the Information Security Coordinator whenever he or she learns that there has been or may have been a security breach that may have compromised Nonpublic Information or other Agency information about Clients, employees or Agency business.

The Agency will take the following actions in the event of a security breach:

a. assess the security breach
b. consult counsel
c. review the requirements of the applicable state laws and regulations
d. notify the carriers whose policyholders insured through the Agency may have been affected by the event
e. notify the carrier for the Agency's cybersecurity coverage
f. notify individuals, regulatory and law enforcement authorities (if and as required and further as deemed appropriate by Agency management) [H]
g. take and document corrective actions to contain and control the problem
h. identify who will address any media inquiries
i. draft the content of all communications regarding the event for potentially affected individuals and, if appropriate, the public [I]

FOOTNOTES / ADDITIONAL INFORMATION

A The Information Security Coordinator can be designated by position in the Agency's Policy, rather than by name, so staff changes do not automatically necessitate changes to the Policy.

B Agency should carefully review security breach notification and privacy laws, as well as insurance laws/regulations, in all states where it does business, as well as in the states in which individuals on which Agency holds Nonpublic Information reside, to make sure this definition of Nonpublic Information encompasses all of those laws/regulations. The privacy laws typically require that the business keep confidential the information that an individual gives it. The Nonpublic Information identified above are the kinds of information elements that typically trigger state security breach notification laws, which require notification of the affected individuals, regulators, etc., as well as other statutory requirements, in the event of a breach of Private Information. Click here for a list of the state security breach notification laws, as published by the National Conference of State Legislatures.

C Note on HIPAA: Agency should also carefully review the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules to assure compliance with any requirements that are applicable, such as regarding the treatment of Protected Health Information (PHI). For further information on HIPAA and its privacy and security rules, see https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

D The Agency should carefully identify every place in which it maintains Nonpublic Information to make sure it is identified and thus properly handled and protected, and so it is stored and accessible only to those with a need to access it to do their jobs.

The Agency should also determine whether it truly needs to keep that Nonpublic Information in all the places it exists, or at all, and if not, the unneeded information should be properly destroyed (e.g., paper documents shredded, and electronic materials destroyed or securely deleted (including electronic back-ups) in accordance with the Agency's Policy and any applicable laws.

E Agency should set procedures that define the time frames when new software versions relating to each element of its Systems must be implemented.

F The use of TLS email encryption is strongly recommended where the carrier or client can accept it. This results in the friendliest workflow for both the sender and the receiver. Otherwise the email can be sent using a proprietary email solution (if the carrier or other party will accept it) or password-protected file (such as a password-protected PDF), where the password is delivered separately from the email containing the file and consists of information that only the end user will know. For more information on TLS email encryption, see the FAQs at http://www.independentagent.com/Resources/AgencyManagement/ACT/Pages/policyning/SecurityPrivacy/ACT_TLSFAQ.aspx

Also note that password protecting a file may not be sufficient to avoid triggering a security breach under the state security breach notification laws if sent to the wrong place or recipient.

G These third party service provider commitments need to track the requirements of applicable state security breach notification and other privacy laws and regulations, as well as the Agency's Policy.

H In New York under Section 899-aa of the General Business Law you must notify (3) NYS offices: the NYS Attorney General, the NYS Division of State Police and the Department of State's Division of Consumer Protection in addition to the Superintendent of the Department of Financial Services as required under Regulation 23 NYCRR 500.

I See http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx for links to the various security breach notification laws, and counsel for the Agency also should be consulted to determine if other laws or regulations are applicable. Laws of the states in which the Agency conducts business, as well as laws of the states in which individuals affected by a security breach reside, may apply to a particular security breach.]

Agents who are subject to the HIPAA privacy and security rules should be aware of HIPAA's breach notification rule, which may apply in the event of a breach of information protected under HIPAA. A summary of the HIPAA breach notification rule can be found in a memo titled, "HIPAA Breach Notification Rule," which is available to Big "I" members who log in to http://www.independentagent.com click on "Big I Resources" & select "Legal Advocacy" and Memoranda/FAQs."

HOW TO CUSTOMIZE THIS

CYBERSECURITY POLICY

WHAT IS THIS?

The IIABNY team created this template to help agencies easily comply with the requirement to have a cybersecurity policy in place August 28, 2017.

This is a guide for agencies including those qualifying for the New York Regulation 23 NYCRR 500 "Limited Exemption." Visit **iiabny.org/cyber** to determine if you qualify.

HOW DO I USE IT?

- Review each section of the policy and add your information to the yellow fields.
- You will notice several **footnotes** inserted throughout the document, marked by **blue letters**. These correspond to additional information (rollover to view or refer to blue boxes in footnote section) to help you customize the section, if needed.
- If desired, delete pages 9-12 from your document as they are simply customization aides.
- Once customized: save the document in a safe place, print a copy for your records and review with staff.
- It is important to execute the items listed in the policy.

IMPORTANT NOTES

1. Federal and state privacy laws and regulations typically provide that the particular administrative, technical, electronic and physical safeguards a business incorporates into its security program be appropriate to the size and complexity of the business and the nature and scope of its activities. Thus, it is important for agencies to customize this prototype policy to the nature and scope of its business activities.
2. It is critical for Agency to actually implement all of the elements it includes in its Cybersecurity Policy (whether it means incorporating new technologies, procedures, workflows, training, monitoring, audits, etc.), because it is likely the agency's policy will be referenced by regulators or in future lawsuits should a security breach occur. It is also important for agencies to carefully review the privacy statements that they provide to consumers and that they safeguard the confidentiality of all of the information they commit to protect in these statements.
3. Just as agencies are encouraged to review and re-evaluate their cybersecurity policies on an annual basis, this prototype policy should be considered a living document and will need to be updated regularly as new security risks become known or reasonably expected.
4. This policy is directed toward "employees" throughout. If the Agency uses independent contractors as well as employees, the Agency will need to broaden the policy to cover this group, such as by substituting "Agency Users" for "employees" wherever the term appears and defining "Agency Users" to include all categories of the Agency's workers.

TEMPLATE DISCLAIMER

March 1, 2017 - IIABNY is providing this prototype cybersecurity policy solely as a tool to assist agencies and brokers in creating a policy appropriate and customized for their agency. This sample is not a substitute for agencies and brokers independently evaluating any business, legal or other issues, and is not a recommendation that a particular course of action be adopted. State security breach notification and privacy laws, coupled with insurance laws and regulations, impose varying requirements on agencies and brokers. Therefore, it is extremely important for agencies and brokers to carefully review applicable laws and regulations in all jurisdictions where they do business in structuring their specific security policies. We have worked from the requirements in New York Regulation 23 NYCRR 500 in formulating this prototype policy, because the New York regulation imposes some of the most specific requirements. If specific advice is required or desired, the services of an appropriate, competent professional should be sought.

Additional information may be found at **iiabny.org/cyber**

Version: 20170412