INTERNAL AGENCY RISK ASSESSMENT GUIDE

An **Internal Agency or Brokerage Risk Assessment** serves as the foundation for creating your cybersecurity policy.

This self-assessment helps you identify possible areas of data exposure, both internally and externally. It should be carried out in accordance with established written policies and procedures and have its results documented. Such policies and procedures shall include:

1. Criteria to evaluate and categorize identified cybersecurity risks or threats
2. Criteria to assess the confidentiality, integrity, security and availability of the Agency's Information Systems and Nonpublic Information (NPI), including the adequacy of existing controls for identified risks
3. Establish criteria to identify risks and how they will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

This risk assessment should be performed periodically to consider technological developments, evolving threats and changes in business operations. It should also consider the particular risks of the agency's or brokerage's operations related to cybersecurity, NPI collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect NPI.

As a first step, consider the questions below. If you are not able to answer the question affirmatively, consider the area and determine if it is an area that your agency should address.

INFORMATION SECURITY

- Are you able to detect Cybersecurity Events?
- Do you collect the information necessary to detect and respond to Cybersecurity Events?
- Do you limit user access to systems that store NPI?
- Do you have policies to ensure the security of NPI by Third Party Service Providers?
- Do you conduct penetration testing of the information systems that store NPI a minimum of once per year?*
- Do you conduct vulnerability assessments of Information System that store NPI a minimum of twice per year?*
- Is your information system able to reconstruct material financial transactions?*
- Do you use secure development practices for in-house developed applications?*
- Do all individuals accessing your internal networks from an external network utilize Multi Factor Authentication?*
- Are your paper files stored in a secure location?
- Do you allow the use of email systems not under the control of the Covered Entity (e.g. personal webmail services)?
- Do you allow the use of cloud storage services such as DropBox, Box, or Office365?

A Cybersecurity Event (as defined by the NY Cybersecurity Regulation) is any act or attempt to gain unauthorized access to, disrupt, or misuse an Information System or information stored on an Information System. Note that this can be an internal or external event.

"Internal" exposure is employee driven. The best perimeter defenses and cyber security controls can be defeated by untrained or malicious employees.

*** While all of these controls are important to a robust Cybersecurity program, if your agency qualifies for a Limited Exemption, the regulation only requires that you have programs in place that address the first 4 questions.**

Last modified: February 1, 2019 4:28 PM

INFORMATION SECURITY, CONTINUED

- Do you or do you plan to regularly review the effectiveness of the safeguards you have in place to protect NPI?

You should consider adopting a Computer Use policy that requires employees to use the same security standards when accessing agency data from non-company controlled equipment.

EMPLOYEE RESPONSIBILITY

- Have you ever conducted staff training on what information is considered NPI?
- Have you ever conducted staff cybersecurity training and training on your Computer Use policy?
- Do you or do you plan to require employees to acknowledge they have received and read the "Cybersecurity Policy"?

ASSET INVENTORY AND DEVICE MANAGEMENT

- Are employees required to adhere to the following provisions in regards to electronic assets and devices:
  - Are employees required to keep their (personal or company) cell phone in their possession or in a secured location if it has access to NPI?
  - Are employees required to password protect their mobile devices?
  - Are employees instructed not to share their passwords or access information with others?
  - Are employees instructed not to put any agency or brokerage data on thumb drives, laptops or other portable media unless authorized to do so by the Agency or brokerage?
  - If employees are authorized to put data on portable media, is said media encrypted and password-protected?
  - Is there an internal off-boarding policy to ensure employees who no longer work for the agency or brokerage do not have access to NPI?
  - Is there an internal off-boarding policy to mitigate the risk that employees who no longer work for the Agency or brokerage have taken NPI?
  - Can an employee's access to email and voicemail be immediately disabled, if needed?
  - Is there a policy to force individuals to return all agency or brokerage data upon separation?
  - Are employees required to report all actual or potential unauthorized access of NPI?

It is impossible to ensure individuals will return all agency data upon separation, but the risk can be mitigated as follows:

1. **Strategic exit interview**
2. **Departure declarations ("I have not taken your information; I have returned all devices and information, etc.")**
3. **Forensic review of agency-issued devices.**

NOTE: Computer Use polices are important here because, in addition to contractual obligations, they can be used in enforcement actions or litigation to hold former employees accountable for taking NPI.

Remote wiping will not be possible for cell phones without control of the account or device via specialized software; remote wiping of a laptop device also would require specialized systems; best defense is strong password protection PLUS encryption so data is inaccessible; best if Covered Entity keeps record of device serial number.

- Does the agency or brokerage keep an inventory of all devices that have access to your network (See Device Inventory Template)?

ASSET INVENTORY AND DEVICE MANAGEMENT, CONTINUED

- Are connected devices encrypted and password protected?
- Are devices able to be wiped if lost or stolen?
- Are storage locations of all paper that has NPI on a device locked and secured?

ACCESS CONTROLS & IDENTITY MANAGEMENT

- Is each individual able to create and reset passwords to an acceptable standard?
- Do you force password resets for everyone on a periodic basis?
- Are employees told not to share passwords?
- Are employees required to lock computer screens and other portable storage devices when not in use?
- Are employees trained on how to identify trustworthy sources and the risks of using unapproved software or applications?
- Are employees specifically trained on how to detect fraudulent emails (e.g. phishing, B2B fraud)?
- Does the Agency or brokerage restrict access to NPI on its network (e.g. file server)?
- If NPI is stored on the agency's network (e.g. on a file server), is it encrypted?
- Does the Agency or brokerage have or plan to have an internal policy on how much Nonpublic Information will be collected and stored in relation to credit card and banking information

Consider :

- **Addressing password creation standards in your Computer Use policy that establish criteria for a strong password: 11 characters including 1 number, 1 capital letter and 1 special character, etc.**
- **Prohibiting employees from sharing passwords.**

Phishing and B2B fraud bypass most internal security controls by duping the recipient. B2B fraud is on the rise and can result in significant financial damage; affects accounts payable but is typically initiated from cyber source.

SYSTEMS & NETWORK SECURITY, OPERATIONS & AVAILABILITY

- Does the Agency or brokerage utilize an email filter (hardware, software or third-party provided) to restrict and eliminate viruses?
- Does the Agency or brokerage utilize technology to restrict access to NPI?
- Does the Agency or brokerage have up-to-date network security and firewall protection on its servers, computers and mobile devices?
- Are Agency or brokerage backups password protected, encrypted, and stored off-site?
- Are outgoing emails and attachments that include NPI transmitted through a secure email system?
- In cases where consumers are entering NPI via the Agency's or brokerage's website or portal, is the connection encrypted with SSL?
- When an employee accesses the Agency's or brokerage's systems or any NPI, is the employee required to use the Agency's or brokerage's secure VPN connection?

Don't be confused! A VPN (Virtual Private Network) is typically used for employee access to internal systems. A SSL (Secure Sockets Layer) establishes an encrypted link between a web server and browser.

Last modified: February 1, 2019 4:28 PM

SYSTEM & NETWORK MONITORING

- Does the Agency or brokerage monitor its Systems for unauthorized or disruptive activity?
- Does the Agency or brokerage conduct due diligence to ensure their third-party service providers that are provided NPI have required security controls and written policies in place or does the agency plan to put this into place?

Keep in mind that a Cybersecurity event can be internal or external. The Agency or brokerage needs to choose a method of monitoring Cybersecurity events. If it is too price prohibitive to hire a monitoring firm (which is recommended), some other form of monitoring must be done.

BUSINESS CONTINUITY & DISASTER RECOVERY

- Are employees trained on how to report a potential or actual security breach?
- Within your Agency or brokerage, do you have plans for a disaster recovery?
- Are there protections for customer information included in your disaster recovery plan?

MISCELLANEOUS

- Does the Agency or brokerage have a backup generator on-site?
- Does the Agency or brokerage currently have or have plans to complete a risk assessment for each vendor or provider used?
- Does the Agency or brokerage currently keep or have plans to keep an inventory of all vendors or providers deemed acceptable by the agency or brokerage through its due diligence process?

NEXT STEP: PREPARE A CYBERSECURITY PROGRAM & POLICY

The program should be based on the results of your risk assessment. It should implement appropriate defensive infrastructure, procedures, employee training and other tactics that your agency chooses to protect your Information Systems and NPI.

To be in compliance with 23 NYCRR 500, you need to implement and maintain a written cybersecurity policy that outlines the cybersecurity program your Agency has in place.

GUIDELINES DISCLAIMER

Big I New York is providing these guidelines for conducting an internal risk assessment solely as a tool to assist agencies and brokerages in complying with New York Regulation 23 NYCRR 500. These sample guidelines are not a substitute for agencies and brokerages 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 brokerages. Therefore, it is extremely important for agencies and brokerages 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 these guidelines, 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. Any agency or brokerage that uses these guidelines agrees that Big I NY will have no liability for anything related to the use of this tool or the internal risk assessment that is conducted.

Last modified: February 1, 2019 4:28 PM