AGENCY CYBER GUIDE 1.0

Agents Council for Technology
Agency Cyber Guide 1.0

Tools for Compliance and Protection in today's world of Data Breach and Cybercrime

July, 2017

act™
AGENTS COUNCIL FOR TECHNOLOGY

Compliance and Protection Roadmap:

In the section immediately below, we are providing you with details on each of 12 Cybersecurity Regulations, as well as resources to address those. The regulations detailed are:

1) Risk Assessment
2) Written Security Policy
3) Incident Response Plan
4) Staff Training and Monitoring
5) Penetration Testing/Vulnerability Assessment
6) Access control Protocol
7) Written Security Policy for 3rd-Party Service Providers
8) Encryption on Non-Public Information
9) Designation of CIO
10) Audit Trail
11) Implementing Multi-Factor Authentication
12) Procedure for Disposal of Non-Public Information

Independent insurance agents & brokers deal with sensitive client information every day. For many insurance transactions, consumers must disclose confidential personal information that they would not normally or willingly disclose even to close personal friends. This puts the burden on agents and brokers to properly collect and protect this information which means complying with state and federal regulations as well as adhering to customer service best practice standards. **Handling sensitive information is now one of the most critical responsibilities faced by the modern insurance agency.**

Admittedly, technology significantly contributes to the ease of data collection and reduces the time required to write and service policies. But if not addressed properly, these improvements also create risks and exposures that could mean potential catastrophe for agents. Federal and state acts such as **Gramm-Leach-Bliley Act** ("GLBA"), the **New York Department of Financial Services**, and other emerging regulatory requirements or recommendations to protect consumer information but that are also in the agents' best interest. These acts and regulations can be tedious and onerous to address given the multifaceted responsibilities agents encounter daily. But agents need to make compliance a priority.

The Agents Council for Technology (ACT) in cooperation with independent agent distribution entities has created this **Agency Cyber Guide** for Big "I" independent agents and brokers. The tool includes a list of the major Federal and State regulations with clear descriptions and resources to address each one. Some of these resources are free through ACT and other entities while some are at cost to the agency. ACT envisions this tool is to be a point-in-time "best practices" resource. Given the swift nature of change in technology and the increasing sophistication of cybercrime, this tool will be updated on a periodic basis.

Here is a high-level overview of the GLBA security measure regulations:

1. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and systems to prevent employees from providing customer information to unauthorized individuals who seek it through fraudulent means;
2. Access restrictions at physical locations containing customer information;
3. Encryption of electronic customer information, including when in transit or in storage on systems where unauthorized individuals may have access;
4. Procedures to ensure that customer information system modifications are consistent with an organization's information security program;
5. Dual control procedures, segregation of duties and employee background checks for employees with access to customer information;

6. Monitoring of systems and procedures to detect actual and attempted attacks on or intrusion into customer information systems;
7. Response programs for when an organization suspects or detects that unauthorized individuals have gained access to customer information systems;
8. Measures to protect customer information from destruction, loss or damage by environmental hazards or technological failure;
9. Training for staff to implement the security program; and
10. Regular testing of the key controls, systems and procedures of the security program.

Data breaches of large commerce businesses are in the news every day. In reality, small- to medium-sized agencies are not immune. Data breaches are occurring just as often in small businesses, and the results can be disastrous! Having to communicate to your entire client base that your system—which contains their sensitive personal data—trusted personal data - has been lost to hackers or cybercrime, can cripple a small business.

It is critical that agents and brokers:

1. understand these requirements
2. begin to comply and protect
3. follow the road map to fully address all areas that apply to them

Costs and Penalties for Noncompliance:

Statistics show that 50% of small and medium-sized business have suffered a cyberattack in the last 12 months (through YE 2016)—this number will increase. The U.S. National Cyber Security Alliance found that 60 percent of small companies are unable to sustain their businesses six months after a cyberattack. According to the Ponemon Institute, the average price for small businesses to recover after their businesses have been hacked stands at $690,000. And for middle market companies, it's over $1 million.

But the costs are not just relegated to lost business. **Non-compliance with any of these regulations may come with a substantial penalty.** Penalties can vary by state, as do the data breach communication requirements. Penalties can be assessed as:

- Civil penalties per resident affected and/or per breach,
- Additional penalties for actual economic damages,
- Noncompliance also punishable by other state-specific deceptive trade practices laws, or as prescribed by a state attorney general.
- It is important to note that the law that applies is not the state where the breach occurred, nor the state where the agent/broker is located, but the jurisdiction of the person whose data was breached.

There are also required timelines for responses. These may carry penalties for each day of failure to provide notice of security breach. Bottom line: Non-compliance and lack of action can cost businesses dearly.

Here are the primary regulations along with resources for agencies to use to comply. ACT recognizes that this is a point-in-time snapshot, so we have developed a process to update this document as individual regulations—as well as federal and state laws—change.

Regulations, Descriptions, Resources

- Note that all regulations listed are critical to comply with GLBA, which also covers other emerging regulation such as NY DFS. These are considered "best practices" for agency security.
- Agencies doing business in the state of New York may apply for an exemption under the NY DFS 23 CRR 500 Act for some of the regulations. However, GLBA still applies. Details on NY DFS exemption eligibility and application are in the 'Appendix' section at the end of this document.

1. Risk Assessment

A risk assessment is the identification of hazards that could negatively impact an organization's ability to conduct business. These assessments help identify inherent business risks and provide measures, processes and controls to reduce the impact of these risks to business operations. The assessment should include a risk mitigation checklist.

Resources:

- ACT/CIS 'Cyber Hygiene Toolkits' For hardware & software, the ability to Count, Configure, Control, Patch: Click here to access
- StaySafeOnline.org

2. Written Security Policy

A security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. It can also be referred to as a 'written information security policy" or "WISP".

The document must detail your agency's operations for security, governance, inventories, controls, continuity and disaster planning and systems monitoring. This includes internal and external mitigation policies.

Primary Resource

- ACT Cybersecurity Policy Template

Resources:

- Information Shield
- FCC – Cyber Security Planning Guide
- NetGen Data Security

3. Incident Response Plan

An incident response is an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The goal is to handle the situation in a way that limits damage and reduces recovery time and costs while complying with federal and state regulations. This includes communication/notices to state superintendent upon detection of a cybersecurity event and communication to customers, insurers, and third-party service providers.

This is part of an overall written security plan (see item #2 above).

Resources:

- Mintz-Levin 2017Apr Data Breach Guidelines by State
- NCSL Security Breach Notification Laws by State
- Guidance for Incident Response Plans
- NetGen Data Security

4. Staff Training & Monitoring

This is a critical regulation. Even if all other areas are in compliance, one misstep by agency personnel can expose data due to malware, phishing and other incursions. ACT strongly recommends that all businesses—regardless of size—comply with this regulation.

Resources:

- Phishme.com – Phishing simulator for agency training
- KnowBe4 – Staff security awareness training
- Cybersecurity employee training guidelines from Travelers – Click here
- NetGen Data Security

5. Penetration Testing and Vulnerability Assessment

Penetration testing (also called pen testing) is the annual practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. This should be done internally and externally.

Vulnerability Assessment is a biannual process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network or communications infrastructure.

Resources:

- Tutorials: Differences/Details between Penetration Testing and Vulnerability Assessments
- Veracode - Vulnerability Assessment and Penetration Testing
- Illumant Security Assessment Services - Vulnerability and Penetration testing

6. Access Control Protocol

This responds to regulations requiring restricted access to non-public Information, including PII, PHI, PCI.

Resources:

- FTC.Gov - How to Comply with the 'Privacy of Consumer Financial Information Rule' of the Gramm-Leach-Bliley Act

7. Written Security Policy for Third-Party Service Providers

These are written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

Note: The NAIC refers to this an "information security program."

Resources:

- NetGen Data Security

This is an evolving issue, with regulatory guidance to come.
Note: These elements for the NY DFS regulations do not take effect until Mar 1, 2019. We expect for guidance on this soon and will update this resource.

8. Encryption of Non-Public Information

Encryption is the process of encoding a message so that it can be read only by the sender and the intended recipient.

Non-Public Information refers to all electronic information that is not publicly-available information and for insurance purposes refers to PII (personally identifiable information), PHI (protected health information), and PCI (payment card industry data security standards).
This regulation describes the need to encrypt and protect this data when in storage and when transferred between the insurance agency and its policyholders (email)

Resources:

- What is Data Encryption, How to Get Started
- Comparison of the Best Data Encryption Software - 2017
- ACT – TLS email encryption FAQs
- ACT - Protect Your Clients with Secure Email Using TLS
- ACT – IA Carriers with TLS Secure Email Enabled

Note: There is an exemption to this requirement, however it requires a waiver request to be submitted annually.

9. Designation of Chief Information Officer

This is the title required by NY DFS for some agencies doing business in New York.; nationally this role can be viewed as 'Data Security Coordinator'.

Resources:

- Agency CIO definition and duties (from NY DFS regulation 500.05, page 5)

10. Audit Trail

An audit trail (also called audit log) is an electronic trail that gives a step-by-step documented history of a transaction. It enables an examiner to trace the financial data from general ledger to the source document (invoice, receipt, voucher, etc.). The presence of a reliable and easy to follow audit trail is an indicator of good internal controls instituted by a firm, and forms the basis of objectivity.

For agencies, using your agency management system (with all other interfacing systems) provides a solid foundation for an audit trail.

Resources:

- NIST (Nat'l Institute of Standards & Technology) on Audit Trails

11. Implementing Multi-Factor Authentication

Multifactor authentication (MFA) is a security system that requires more than one method of authentication from different categories of credentials to verify the user's identity for a login or other transaction.

One example is a policyholder logging into an agency website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the policyholder's phone or email address.

Resources:

- SBC.com: Protect Your Small Business with Two-Factor Authentication
- CIO.com: Making Multi-Factor Authentication Easy to Use

12. Procedure for Disposal of Non-Public Information

As with encryption, this regulation refers to all electronic information that is not publicly available, including PII, PHI and PCI.

Improper document destruction is often a downfall of small business security.
Regulations on this vary by state. Agents doing business in multiple states should adhere to the highest level of requirements. Keep in mind, there is a difference between complete disposal of information, and simply deletion.

Resources:

- Nat'l Conference of State Legislatures (NCSL) - Data Disposal Laws by State

Also, please contact your agency management system provider for their disposal protocol.

APPENDIX

Additional details on laws driving regulations listed in the ACT Agency Cyber Guide:

- Gramm-Leach-Bliley Act
- NAIC Cybersecurity Recommendations
- NY DFS 23 NYCRR 500 Regulations

  NOTE: For some of the regulations listed in section 500.19 of the NY DFS regulations, agencies doing business in the state of NY can apply for an exemption. In general, qualifying agencies have fewer than 10 employees, or less than $5,000,000 gross annual revenue in each of the past three fiscal years, or less than $10,000,000 in year-end total assets.

  **However, it is strongly encouraged that agencies review and work to comply with these regulations, as they are strong tenets of a solid, effective agency security environment.
- Gramm-Leach-Bliley Privacy Law for Producers

Additional insurance solutions:

- NY Exemption Filing information via IIABNY
- Cybersecurity Vendors and Offerings
- Big "I" Cyber Resources

Following are resources for selling Cyber Security Liability Insurance Policies :

**Do not confuse these with agency security processes detailed in this document prior to this section.

- Big 'I' Markets - Cyber Liability Solutions
- A Buyer's Guide to Cyber Insurance – McGuire/Woods

ACKNOWLEDGEMENTS

ACT would like to thank the following individuals from the Security Issues work group who provided the input and guidance to make this Cyber Guide a reality: Bill Larson, Erin Odell, Jerry Fox, Joe Doherty, Kathleen Weinheimer, Paul Peeples, Rachel Tuller, and Wes Bissett.

AGENTS COUNCIL FOR TECHNOLOGY

Driving technology forward for independent agents

CHANGING NATURE OF RISK
"Moving from trends to critical action."

HOW DO YOU PROTECT YOUR AGENCY'S DATA?

eSignatures BEST PRACTICES & INDUSTRY RECOMMENDATIONS
ACT eSignatures Work Group
act.

The Agents Council for Technology encourages the independent agency system to implement consistent and innovative workflows. Be part of a forum of agents, carriers, and vendors working together to create best practices and help the industry implement consistent technology.

Volunteer for a virtual workgroup:

- Security
- Future Issues
- Changing Nature of Risk
- Customer Experience
- E-Signature
- Small Commercial Lines Rating

ACT NOW! independentagent.com/ACT

act.™
AGENTS COUNCIL FOR TECHNOLOGY

Trusted Choice® | Independent Insurance Agents & Brokers of America, Inc.

Independent Insurance Agents & Brokers of America, Inc.
127 South Peyton Street, Alexandria, VA 22314
800.221.7917