BULLETIN:

Reminder – Genworth's Policy on Cybersecurity & Cybersecurity Practices

November 23, 2022

Effective – Immediately

States – All

Contact – If you have any questions about these changes, please email DistributorITSecurityQuestions@genworth.com.

Through policies, standards, procedures, and guidelines, Genworth's Data Security & Cybersecurity Program provides a comprehensive approach to address cybersecurity risks and threats. The Cybersecurity Program addresses the goals of confidentiality, integrity and the availability of data and systems. Our Cybersecurity Program helps us meet the cybersecurity obligations required of financial services companies by regulatory bodies such as state insurance departments. As part of our Cybersecurity Program, we have developed the following required minimum and risk-based cybersecurity practices that Distributors must understand and follow to do business with Genworth.

Definitions

Distributors – third parties of all levels who promote, sell, or service Genworth's products.

Enterprise Systems – any server, appliance, application, or other technology that can access, store, process, or transmit Sensitive Information except Personal Mobile Devices.

Personal Mobile Devices – any computer (laptop or desktop), cellular telephone, tablet, drive, removable media, or other device that can be used to access, store, process, or transmit information regardless of device ownership.

Security Breach – any act or attempt to gain unauthorized access to, disrupt, or misuse Genworth's Sensitive Information or an electronic information system on which Genworth's Sensitive Information is stored.

Sensitive Information – Genworth consumer information and confidential information.

The following are the **Required Minimum Cybersecurity Practices** that must always be followed, as well as the **Risk-Based Cybersecurity Practices** that can be implemented based on risks specific to your organization.

Required Minimum Cybersecurity Practices

At a minimum, Distributors who conduct business with Genworth must follow certain rules to secure electronic Sensitive Information. These rules include:

Genworth companies include:
Genworth Life and Annuity Insurance Company, Richmond, VA
Genworth Life Insurance Company, Richmond, VA
Genworth Life Insurance Company of New York, New York, NY
Only Genworth Life Insurance Company of New York is admitted in and conducts business in New York.

361101 11/23/22

1. Deploy data encryption software on all Personal Mobile Devices that access or store Sensitive Information used for producer, intermediary, and top-level business.
2. Use physical and technological security safeguards to protect Sensitive Information in all formats (hard copy or electronic). This includes keeping paper or other physical formats secured (e.g., locked filing cabinets) with access limited to authorized personnel.
3. Remove access to Sensitive Information for former employees or contractors immediately upon termination.
4. Make your employees aware of security and privacy policies through ongoing employee training and communications.
5. Implement an annual review process for all security policies and plans.
6. Utilize appropriate disposal practices for Sensitive Information.
7. Minimize Sensitive Information kept on Personal Mobile Devices.
8. Identify an accountable individual for matters of IT/cybersecurity.
9. Perform an IT Security controls assessment, either industry-standard or self-assessment by participation in Genworth's IT Security Questionnaire.
10. Conduct vulnerability scans of Enterprise Systems.
11. Establish and implement a security and software patching schedule for all operating systems and applications.
12. Require the use of unique user IDs with strong passwords and a process to change passwords regularly.
13. Implement multi-factor authentication on all locations that can access, store, process, or transmit Sensitive Information including, at a minimum, securing computer equipment in access control facilities (e.g., lock and key or badge reader and access cards) and requiring computers to have passwords.
14. Adopt written procedures that include all of Genworth's requirements, incorporate mitigation steps, and include internal and external notification of security incidents involving unauthorized access to Sensitive Information.
15. Create a third-party management program for use with those third parties who provide you services and who have access to Sensitive Information.
16. Use commercially reasonable measures (e.g., antivirus software with automatic updates enables and an established full-disk scanning schedule) to detect and prevent malware installation on all computers.

Risk-Based Cybersecurity Practices

Distributors who conduct business with Genworth should complete a cybersecurity risk assessment appropriate to their organization and, where necessary and prudent, implement the following:

1. Monitor employee or contractor access to Sensitive Information.
2. Use intrusion detection technology or other suitable technologies and/or procedures to detect unauthorized access of Sensitive Information.
3. Employ automatic account locking after a certain number of failed login attempts.
4. Deploy data encryption mechanisms on Enterprise Systems.

Reporting of Security Breaches

Distributors shall notify Genworth of any Security Breach that (1) results in the unauthorized access to, disruption of, or misuse of, Sensitive Information or any electronic information system on which Sensitive Information is stored, or (2) materially impacts Distributor's operations or Distributor's ability to provide the services in accordance with your agreement. Required notices of a Security Breach shall be made to DataSecurityTeam.Genworth@genworth.com notwithstanding any other notice provision in the agreement to the contrary. Distributors shall provide such notice following discovery and without unreasonable delay, but in no event later than three days following discovery of the Security Breach.

Genworth counts on you, our Distributors, to protect Sensitive Information from the ever-growing threat posed to information and financial systems. If not prevented, cybercriminals can cause significant losses for consumers whose private information may be revealed and/or stolen for illicit purposes, as well as significant losses for the financial services industry. Prevention is our goal.