Vendor and Third-Party Service Provider Policy and Attestation

PURPOSE

The purpose of this document is to establish policy governing security requirements for selected vendors and third party service providers. All selected Greater New York Insurance Companies ("GNY") third party vendors and service providers (collectively the "SPs") are required to implement, test and continually monitor the administrative, physical, and technical controls outlined below to protect GNY data (including, but not limited to, data relating to GNY customers, data relating to any system or network under GNY control, financial data, credit information, and all employee data).

POLICY

Upon request, the SP must provide evidence of the requirements listed in either digital or written form to GNY, in addition to the attestation required on the last page of this document.

1. Authentication and Access Control

- SP must have a formal, documented process for granting and revoking access to all systems that process or store GNY sensitive data (e.g. information that is not publicly available, including, but not limited to social security numbers, drivers' license numbers, account numbers, security codes or passwords, biometric records and any information related to medical conditions).
- SP user access rights shall be strictly limited to a need-to-know basis that permits access only to the systems and resources that are required for users to perform their duties.
- All SP users with authorized access to GNY sensitive data must be assigned a unique User ID which must not be shared with any other individual.
- For single-factor authentication solutions, passwords managed by SP or implemented within SP-provided applications that are used to authenticate to systems processing or storing GNY sensitive data must meet or exceed the following minimum requirements:
    - All passwords shall have at least ten (10) characters;
    - Passwords shall contain at least one alphabetic and one non-alphabetic character (non-alphabetic characters include single digit numbers and punctuation);
    - Passwords shall not be constructed of a single word found in the dictionary;

    - Users shall not be permitted to construct passwords that are identical or substantially like passwords that they had previously employed;
    - Passwords and any application or system passwords protecting sensitive GNY data shall be changed at least every 90 days; and
    - Passwords must be hashed (with unique salts) and stored securely. In addition, any public-facing systems must use a slow hashing algorithm that implements a work factor (such as PBKDF2, bcrypt, or scrypt). Clear text storage or reliance only on reversible encryption algorithms to protect passwords is not acceptable. Authenticators used in multi-factor authentication mechanisms (such as PKI or biometrics) must be afforded the same secure storage protections.
- Access rights will be revoked immediately upon termination of any SP user with access to GNY systems or resources or if a change in job role eliminates the requirement for continued access.
- All access rights must be reviewed by SP no less frequently than once annually.
- All SP user access to systems storing GNY sensitive data must be audited and those audit records be maintained and made available to GNY upon request.

2. <u>Data Transmission Confidentiality and Integrity</u>

- All GNY sensitive data transmitted by SP will be protected with a transmission encryption solution that complies, as appropriate, with NIST Special Publications 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

    - Approved solutions are limited to those that have been issued a FIPS 140-2 Validation Certificate.
    - Data transmissions include, but are not limited to web transmissions, file transfers, and email.

3. <u>Media Protection, Sanitization and Destruction</u>

- Upon termination of the contract with GNY or at any time prior to reuse or repurposing of media used to store or process GNY sensitive data, said media must be cleared (using a DoD compliant 7-pass wipe) or purged in accordance with NIST SP 800-88.
    - If the media is to be destroyed, the method used must ensure that after destruction, the media is able to withstand a laboratory attack as outlined in NIST SP 800-88.
    - SP must provide a certificate of destruction if requested by GNY.

4. <u>Remote Access</u>

- SP must sign a Third-Party Remote Access Agreement before being granted remote access to any GNY information systems or data.
- Unless otherwise explicitly approved and documented by the GNY CIO, all remote access must occur using the GNY VPN solution (Palo Alto Global Protect client with Duo MFA) or verified secure Remote Access Services (RAS).

5. Physical Security

- In addition to the previously mentioned technical controls, SP must employ physical safeguards and visitor access controls to prevent unauthorized access to all systems and media used to process or store GNY sensitive data.

IF YOUR ORGANIZATION HAS LESS THAN 10 EMPLOYEES (INDEPENDENT CONTRACTORS COUNT AS EMPLOYEES) NUMBERS 6-8 ARE NOT APPLICABLE

6. System Security and Vulnerability Management

- SP must have a documented patch management and distribution process that ensures security patches are applied to all systems (to include servers, workstations, laptops) that process and/or store GNY sensitive data.
- All applicable security patches must be deployed within 30 days of vendor release unless otherwise discussed and approved, in writing, by the GNY CISO.
- SP must employ network security architectural components (to include, at a minimum, firewalls and network intrusion detection/prevention solutions) to adequately protect all systems processing or storing GNY sensitive data that are accessible from the internet or other public network.
- SP must employ an anti-virus solution with real-time protection and automatic updates on all systems that store or process GNY sensitive data.
- SP will ensure any web-based solutions storing or processing GNY sensitive data will adhere to security design best-practices including, but not limited to, protecting against the
Open Web Application Security Project OWASP Top 10 list of security risks.

7. Auditing

- All systems that process or store GNY sensitive data must maintain an automated audit trail that documents system security events as well as any event that results in the access, modification, and/or deletion of GNY sensitive data.
- The audit trail must, at a minimum record the following information for each event:
  - Type of event occurred;
  - When (date and time) the event occurred;
  - The source of the event;
  - The outcome (success or failure) of the event; and
  - The identity of any user/subject associated with the event.
- Audit logs must be read-only and protected from unauthorized access. Audit records documenting events resulting in the access, modification, and/or deletion of GNY sensitive data must be made available to GNY upon request.
- SP must employ a regular audit log review process (either manually or automated) for detection of unauthorized access to GNY sensitive data.

8. Awareness and Training

- SP must ensure all SP users receive regular security awareness training and are apprised of the requirements outlined within this policy.

Attestation

Except as noted below, I confirm the SP follows the requirements noted above. I am fully familiar with the items to which I am attesting to herein.

This organization has less than 10 employees (independent contractors count as employees) Yes □ No □

Exceptions:

□

____

Signature

____

Printed name

____

Title

____

Date

GNY Insurance Companies

200 Madison Ave., New York, NY 10016

ThirdPartyManagement@GNY.com