National Life Group®

Cybersecurity Regulations

Agent Minimum Security Standards (AMSS) for agencies and agents selling National Life Products.

1. Purpose

The National Life Group (NLG) Agent Minimum-Security Standard (AMSS) establishes standards, responsibilities and compliance requirements for NLIC's contracted Agents. This AMSS describes NLG's expectations for protecting the confidentiality, integrity and availability of NLG data and assets.

2. Scope

This standard applies to all Agents/Agencies contracted with NLIC.

3. Human Resource Security

a) **Information Security Awareness**: All contracted Agents/Agencies must take information security awareness training.

4. Identity Management, Authentication and Access Control

a) **Authentication:** Agents/Agencies shall ensure that all access, by employees or contractors, to its information systems, used to provide services or supply products, shall require appropriate authentication controls that at a minimum will include:

i. Unique user ID for each user
ii. Strong passwords
iii. Reasonable password expiration periods
iv. Multi-Factor authentication will be required for remote access to any NLG Systems.

b) **System Lockouts:** wherever feasible, time-based screen and system lockouts must be employed.

c) **Need to Know:** to protect client confidentiality, Agents/Agencies shall secure all client files and private information, allowing access only to those with a demonstrable need to know.

d) **Access Termination:** Agents/Agencies shall develop and maintain a process designed to ensure that user access is revoked upon termination of employment, or contract for contractors. NLG should be notified of an agent's termination.

TC109385(0819)1

5. Physical and Environmental Security

a) **Secure Physical Facilities:** Agents/Agencies shall ensure that all of their systems and other resources are located in secure physical facilities with access limited and restricted to authorized individuals only.

6. Information Protection Processes and Procedure

a) **Anti-Malware:** Agents/Agencies shall ensure that all information systems are protected by up-to-date anti-malware software.

b) **Wireless Access Control:** Agents/Agencies shall ensure that wireless network access is protected, including at a minimum:

i. All wireless network access over which NLG data will be transmitted will be password protected.

ii. Wireless network access for guest access should be segregated from the business network.

c) **Patching:** Software publishers often release updates that improve data security. Agents/Agencies must keep software up to date with current officially released versions.

7. Data and Privacy Security

a) **Encryption at Rest:** Agents/Agencies shall ensure that all laptops, mobile devices, and removable media, including those that are owned by agent employees or contractors, that may be used to store, process, or transport NLG data are encrypted.

b) **Encryption During Transit:** Encryption during transit must be employed at all times when handling NLG non-public data.

c) **Use of Third Parties:** Businesses are increasingly utilizing 3rd Party CRM, Marketing, and other outside resources to run their business. No agent is authorized, directly or indirectly to divulge to a third party without permission, information obtained through any professional dealings with policyowners or prospects. Any potential unauthorized disclosure, distribution, reproduction or use of Customer Information may cause irreparable harm and Agents/Agencies agrees to report it to National Life Group's Chief Information Security Officer immediately upon discovery. i. An exception is made for 3rd Party IT support vendors that may incidentally have access to the above information.

d) **Secure Disposal:** Agents/Agencies shall ensure that all media that may be used to store, process, or transport NLG data is disposed of in a secure manner.

e) **Unauthorized Disclosure:** Other than to law enforcement or as otherwise required by law, Agents/Agencies may not make or permit any statements concerning security incidents involving NLG non-public information, information systems or assets to a third-party without the written authorization of NLG's Legal Department.

f) **Audit Rights:** Agents/Agencies shall grant NLG the right to audit Agents/Agencies, upon reasonable notice and at NLG's expense, to verify that Agents/Agencies are in compliance with these requirements.

g) **Legal and Regulatory Requirements:** Agents/Agencies shall employ technical and organizational security measures no less strict than is required by applicable regulations and laws.

h) **Cyber Insurance:** While not a requirement of these minimum standards, NLG highly encourages all Agents/Agencies to retain adequate cyber insurance relevant to the possible damages that may be caused by a data breach.

Exceptions

a) ANY exceptions to this policy must be approved by the CISO, or an appointed delegate.

Definitions

Term	Definition
Non-Public Information	Nonpublic Information shall mean electronic information, not publicly available, which is "Business Related Information," "Identifying Information," or "Health Information."
Business Related Information	Business Related Information means confidential information which if accessed in an unauthorized way or tampered with, could have a materially adverse impact on NLG.
Identifying Information	Identifying Information means information about an individual, such as name or other identifier, which is in combination with social security number, driver's license number (or non-driver ID number), account number or credit or debit card number, any security code permitting access to an individual's financial account, or biometric records, can be used to identify such individual.
Health Information	Information other than age or gender created by or derived from a health care provider that relates to physical, mental or behavioral health condition of an individual or his or her family, the provision of health care to the individual, or the payment for health care to any individual.