[*Organization*]

Data Privacy and Security Policy

Drafting Note
This Policy is to serve as a **guideline** for receivers and guaranty associations.

Statement of Policy

It is the policy of the [*Organization*] to protect against the unauthorized access, use, corruption, disclosure, and distribution of non-public personal information (as further defined in the [*Organization*]'s adopted Data Privacy and Security Procedures ("Procedures") in its possession, and to comply with all applicable state and federal laws and regulations regarding such information. The [*Organization*] shall hold non-public personal information in strict confidence and shall not release or disclose such information to any person except as required or authorized by law and only to such persons who are authorized to receive it. The [*Organization*] shall not utilize any non-public personal information for any purpose other than the administration of a receivership or in the event that it assists a regulator in the supervision of an insurer. In furtherance of this policy, the [*Organization*] shall adopt procedures for the administrative, technical and physical safeguarding of all non-public personal information. The [*Organization*] shall ensure that an entity retained by it, or any other entity that utilizes information provided by the [*Organization*] to carry out its responsibilities, shall have signed and agreed to abide by the terms of the Data Privacy and Security Policy or shall have adopted a data privacy and security policy that is substantially similar to the [*Organization*] policy.

Privacy Officer

The [*Organization*] shall appoint an Information Security Officer to review and maintain the Procedures and monitor compliance with the guidelines set forth in the Procedures.

Management and Training

1. Access to non-public personal information shall be limited to authorized users who need to have access to carry out the [*Organization*]'s responsibilities as it relates to that information.
2. Each employee and authorized user with access to non-public personal information shall annually sign a copy of the [*Organization*]'s Data and Privacy Security Policy and Procedures and agree to abide by its terms.
3. Except as required by law, when the [*Organization*] provides non-public personal information to third parties, it shall first provide a copy of this Data Privacy and Security Policy and require the third party to certify that it has read the policy and agrees to comply with applicable provisions, or that it has a substantially similar data privacy and security policy and that it will comply with the applicable provisions of its policy with respect to the non-public personal information provided.
4. The [*Organization*] will perform a background check as further defined in the [*Organization*]'s human resources policies on employees with access to non-public personal information. Any third party with access to non-public personal information must certify that it has performed a background check on its employees who have access to the [*Organization*]'s non-public personal information.
5. The [*Organization*] will have in place a succession plan for key persons in the event of a disruption to normal business processes.

6. The [*Organization*] shall ensure to the greatest extent possible based on the size of the organization that there is a clear separation of duties to prevent important management controls from being overlooked. Segregation of duties as defined in the Procedures will preserve the integrity, availability, and confidentiality of information assets by minimizing opportunities for security incidents, outages and personnel problems.
7. The [*Organization*] shall train employees and other authorized users in the use and maintenance of security procedures.
8. Violations of the data privacy and security policy may result in disciplinary action up to and including termination of employment.

Information Systems

The [*Organization*] shall adopt procedures for protecting and maintaining the security and integrity of its information systems including network infrastructure and software design, information processing, storage, transmission, retrieval and disposal. These procedures shall address the following matters:

1. Limiting access to those individuals necessary to carry out the [*Organization*]'s role with respect to non-public personal information.
2. Limiting access to only those authorized users who shall have signed and agreed to abide by the terms of the Data Privacy and Security Policy or shall have adopted a data privacy and security policy that is substantially similar to the [*Organization*] policy..
3. Protecting physical and electronic records from unauthorized access, interception, distribution or destruction.
4. Records back-up and off-site storage procedures to prevent inadvertent loss or destruction of records.
5. Data security procedures to prevent unauthorized access or interception of non-public personal information.
6. Procedures for protecting data when changing, upgrading, or replacing servers, computers or other storage media.
7. Procedures for properly disposing of unneeded or outdated records.
8. Procedures to monitor, detect, and report upon any improper disclosure or theft of non-public personal information.
9. Procedures to periodically test and review the security procedures and maintain a record of the maintenance and review process.
10. Annual audit of procedures for compliance and effectiveness with adjustments as appropriate.

Information Security and Response

The [*Organization*] shall adopt procedures for the prevention, detection and response to unauthorized access to non-public personal information.

In the event non-public personal information is accessed by someone without proper authorization, the [*Organization*] shall immediately investigate and take appropriate remedial actions to mitigate or prevent loss or damage to affected individuals. Each situation will be evaluated separately, and based upon the potential for loss or damage to affected individuals; the [*Organization*] will take one or more of the following measures:

- Make such notifications to affected individuals as may be required by law.
- Report the incident to appropriate law enforcement officials.
- Determine the nature and cause of the security breach and implement corrective measures.