

[[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 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.

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

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