

**FINANCIAL INSTITUTION TECHNOLOGIES, INC. d/b/a  
SUNTELL  
NONPUBLIC INFORMATION SECURITY POLICY**

We understand the importance of maintaining and protecting information that we maintain about you or that we receive from you. We also understand the regulator requirements imposed on you with respect to the sharing of Nonpublic Personal Information, and we will respect and adhere to the re-disclosure and reuse rules set forth in the Interagency Privacy Regulations. When we obtain Nonpublic Personal Information for any purposes, we utilize it to accomplish the task for which we received the information. For this reason, Suntell commits to following these guidelines when handling databases and/or files from you which might contain Nonpublic Personal Information:

Information, Files, Databases, etc. will:

- Only be requested when all other alternatives are deemed ineffective or too time costly
- Be placed in a common location on Suntell's network with restricted employee access
- NOT be a part of Suntell's nightly network backup
- Only be kept during the analysis stage for the specific issue(s) they were requested

Once the task is completed, or it is no longer necessary for us to maintain the Nonpublic Personal Information, such information will be destroyed.

To ensure adherence to this policy, Suntell conducts a quarterly audit. Such audit includes a complete review of all network permissions to folders assigned to holding customer data; additional folders to ensure customer data is not being held in a non-approved location and a review of employee VM's to ensure unauthorized data is not present. Additionally, verbal reviews are conducted with employees to ensure full understanding of this policy.

Revised: 2/19/2020

Last Reviewed: 01/08/2021

