SAMPLE RULES OF BEHAVIOR GOVERNING COMPUTER USE

Trustees must have rules governing the use of the trustee's computer system by the trustee's employees. These rules should explain the employee's responsibilities as a user and the penalties for noncompliance. The section on user responsibilities should at a minimum include the following:

General:

1. Use trustee information systems for lawful, official use and authorized purposes in accordance with current guidelines.
2. Do not generate or send offensive or inappropriate e-mail messages, images, or sound files. Limit distribution of email to only those who need to receive it.
3. Do not open emails from suspicious sources and do not visit untrusted web sites.
4. Protect and safeguard all trustee information, including personally identifiable information (PII), per the sensitivity and value of the data at risk, from unauthorized access, unauthorized or inadvertent modification, disclosure, destruction, denial of service, improper sanitization or use, in accordance with applicable policy, practices, and procedures.
5. Report known or suspected security incidents (including loss of PII) upon discovery of the incident to the trustee.
6. Encrypt all trustee data on transportable/mobile computers (including laptops) and removable media which contains sensitive information.
7. Use only authorized media storage devices. Download files only from known and reliable sources and use virus-checking procedures prior to use.
8. Screen-lock or log off your computer when leaving the work area and log off when departing for the day.

Passwords:

9. Change passwords at least every 90 days or more often if compromised or if directed by your supervisor; choose a password at least 8 characters in length; and use at least 3 of the following 4 characters: upper case letters, lower case letters, numbers, and/or special characters.
10. Do not share passwords with anyone.

Hardware:

11. Do not add, modify, or remove hardware accessories or networks to a computer.

Software:

12. Comply with terms of software licenses and only use licensed and authorized software.
13. Do not install any software.
14. Do not change any configurations and/or settings of the operating system and security-related software without advance approval.
15. Do not attempt to access any electronic audit trails that may exist on the computer unless specifically authorized to do so.

I acknowledge receipt of these Rules of Behavior and understand my responsibilities as identified above. This includes my responsibility to ensure protection of PII that I may handle.

_____ _____

Signature Date

_____

Printed Name