Prudential Information Security
Terms and Conditions

Description: This document sets forth the Information Security Terms and Conditions that apply to all non-Prudential personnel being provided access to Prudential Systems and Prudential Confidential Information. These Terms and Conditions are subject to change by Prudential from time to time.

Definitions: Defined terms in this document have the meaning ascribed to them below. In the event of a conflict between the defined terms set forth in the Agreement and those in these Terms and Conditions, the defined terms in the Agreement shall apply:

a) "Agreement" means the relevant underlying governing agreement or agreements between Company and Prudential.

b) "Company" means any person or entity engaged by Prudential to provide services to Prudential or otherwise doing business with Prudential.

c) "Non-transformed Data" means any production data which has not been encrypted or otherwise rendered technically unidentifiable except by authorized individuals or processes

d) "Personal Information" means information provided by or at the direction of Prudential, or to which access was provided in the course of Company's performance of the Agreement that (i) identifies an individual (by name, signature, address, telephone number or other unique identifier), or (ii) that can be used to authenticate that individual (including, without limitation, passwords or PINs, biometric data, unique identification numbers, answers to security questions, or other personal identifiers). An individual's social security number, even in isolation, is Personal Information. Prudential business contact information is not by itself Personal Information.

e) "Prudential Confidential Information" means all business and other proprietary information of Prudential, written or oral, including without limitation the following:

- information relating to planned or existing businesses or business initiatives; organizational restructuring plans; and actual and projected sales, profits and other financial information;
- information relating to technology, such as computer systems and systems architecture, including, but not limited to, computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods;
- information that describes insurance, annuities and financial services products and strategies, including, but not limited to, actuarial calculations, product designs, product administration and management; tax interpretations, tax positions and treatment of any item for tax purposes;
- confidential information, software and material of third parties with whom Prudential conducts business;
- information about Prudential employees, personnel and premises;

- Prudential policies, procedures, and standards; and
- Personal Information.

f) "Prudential Data" means Personal Information and Prudential Confidential Information.

g) "Prudential Systems" or "Systems" means Prudential's computer systems and software.

h) "User" means any person who has access to Prudential Data and/or System(s).

Obligations: Company and Users with approved access to Prudential Systems and Prudential Data must adhere to the guidelines below. In the event of a conflict between these guidelines and the terms of the applicable Agreement, the guidelines in the applicable Agreement shall apply:

1. USER RESPONSIBILITIES. An end User is any person who has access to Prudential's Systems. A User's security responsibilities are to:

   a) Understand his/her responsibility to comply with Prudential's Information Security Control Standards and other Prudential policies, standards, guidelines and procedures regarding information security provided to Users.

   b) Report observed or suspected information security violations to the Prudential project manager, the appropriate security group and/or the Information Security Office.

   c) Maintain the confidentiality of his/her password. A User must not share his/her password, personal identification number (PIN), or token with another person.

   d) Change his or her password immediately if he/she thinks the password may have been compromised.

   e) Report any suspected misuse of a User ID or any inappropriate solicitation or use of a password.

   f) Choose a strong password that can be remembered without writing it down. Never store the password in a login script or programmable device. Review Prudential's guidelines for selecting strong passwords, which Users may obtain from your Prudential contact.

   g) Log off or lock a terminal or workstation when leaving it unattended.

   h) Ensure that only Prudential approved or licensed software is installed on his/her workstation, laptop, or the network. Non-approved\unauthorized software includes, but is not limited to hacking tools, shareware, evaluation software, etc

   i) Ensure that computers and other portable office devices (i.e. laptops, palms, PDAs, etc.) are either in sight or physically secured at all times.

   j) Ensure that the computer and other portable office devices have a password-protected screen saver.

k) If the User is developing applications, ensure that application security controls as defined in Prudential's Information Security Control Standards are complied with and company-wide change control requirements are adhered to.

l) Never connect, install, or configure equipment (including software tools) to the Prudential network without following an approved change control process and obtaining the appropriate authorization(s) from Prudential.

2. SYSTEM ACCESS (Local and Remote). System access procedures are dependent upon the types of communications services used to connect the site with Prudential's Data Processing Centers. Regulations regarding access to Prudential Systems are as follows:

a) System access instructions/procedures must be kept in a secure locked place at all times when not in use.

b) Personal computers used to access Prudential's Systems must never connect to the Internet without firewall protection or be connected to a network that does not have Internet firewall protection.

c) The User's computer must not be logically connected to two (or more) networks at the same time, when one of those networks is a Prudential network (i.e., the User is not permitted to bridge the two networks).

d) Software, instructions, and keys needed to facilitate VPN or other remote connections must be provided on a "need to know" basis only.

e) Access to computers that connect to the Prudential by remote access must be controlled in such a manner that all unsolicited Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets from the Internet are blocked. The configuration of the access control device (e.g., personal firewall, Instant Internet) must be approved by the Information Security Office.

f) Workstations (including desktops and laptops) must never be left signed on while unattended for any period of time. They must be signed off or locked when not in use.

g) All equipment that is located inside a Prudential facility or that connects to the Prudential network as a node must be able to be monitored by Prudential.

3. USER ACCESS. Protection of the Systems is dependent upon the ability to control access to the Systems. It is the User's responsibility to be certain that computer accessibility is properly secured.

a) Only those individuals whose duties require it can be provided with access to Prudential's Systems. Each User will be assigned a unique and individual user ID.

b) Use of Prudential systems must be limited to those Systems for which the User is authorized.

c) When a User no longer requires access to a System, the User must notify Prudential immediately so that user IDs and access can be removed.

4. PASSWORDS/PINS and Access Tokens. Passwords and access tokens are critical to the security of the System as they verify that anyone signing on has the authority to do so.

   a) Passwords/PINs must be changed at least every 30 days.

   b) Passwords must contain at least one alphabetic and one numeric character.

   c) The minimum length of a password is 8 characters. The minimum length of a PIN is 4 characters.

   d) Passwords must not be the same as the user ID or contain the user ID.

5. VIRUSES AND MALICIOUS CODE. All technology that directly connects to Prudential Systems must apply protective measures to safeguard Prudential Systems against viruses and malicious codes. Specifically, Prudential Systems must be protected by currently approved anti-virus software. Prudential Data must not be stored outside Prudential Systems without Prudential's specific written authorization.

   Company and its Users are responsible for:
   - Maintaining appropriate safeguards for any technology equipment that Company and its Users use to access Prudential Systems;
   - Reporting all virus incidents to Prudential's supporting Help Desk;
   - Refraining from forwarding or circulating e-mail virus warnings;
   - Ensure that current anti-virus software and virus signature files are installed and configured to scan all files introduced into Prudential Systems.
   - Ensuring Company and its Users do not disable or remove anti-virus protection for any reason. Company and its Users must prevent access to Prudential Systems by unauthorized persons; and
   - Ensuring that all electronic files that Company and its Users introduce from any source (e.g., Personal Digital Assistants, detachable media or other mobile devices) are scanned for viruses.

   Malicious code, commonly referred to as viruses, worms, or Trojans, is any software program, program component, or code introduced into a computing environment which:
   - Evades control processes;
   - Accesses, damages, compromises, or alters data without proper authorization or by improperly assuming the authority of authorized users;
   - Is intended to negatively impact computer or network operation or performance;
   - Uses the computing environment for a purpose unknown to or intended by the authorized user(s); and
   - Replicates itself or its functionality improperly.