Information Systems Security and Usage Policy

Information Security

September 4, 2007, Ver. 2.0

Confidential

OVERVIEW

StanCorp Financial Group, Inc. and its subsidiaries (the “Company”) provide access to information systems to employees, contractors, and vendors so they can successfully conduct their day-to-day business activities. This *Information Systems Security and Usage Policy* describes users’ obligations in using the Company’s information systems.

SCOPE

This policy applies to employees, contractors, and vendors of the Company (“users”) who are granted access to information systems so they can successfully conduct their day-to-day business activities. This policy supersedes the previous version named “Automated Systems Use Policy version 1.1”

ACCESSING AND USING INFORMATION SYSTEMS

- Whenever you access and use Company information systems, you are consenting to apply and follow in full the contents of this policy and all applicable Company policies. Failure to adhere to these policies will result in disciplinary action that may include termination of employment. In the case of violations of law, civil or criminal prosecution may result.
- Incidental personal use of the Company’s information systems (including use of the telephone or use of a company computer to access a personal e-mail account) is permissible only if consistent with this policy and only if such usage does not interfere with job performance, does not deny other users access to information systems, and does not incur significant costs. Under no circumstances may Company systems be used for personal benefit or private gain, including any non-Company business, consulting or charitable endeavors.
- Users must not use profanity, obscenities, or derogatory remarks in any e-mail message, blog posting, chat session or any other electronic technologies for any reason, even if done with a humorous or ironic intent, as it may be deemed harassment. Further information can be found in the Company’s *Guide to Business Conduct* on StandardNet » Business Conduct.
- The access granted to users to the Company’s information systems is a privilege, not a right. The Company may monitor, limit, restrict, deny, or extend access to its data and information systems, and the Company conveys no expectation of privacy or confidentiality to users.
- By using the Company’s systems, including telephones, users consent to the logging, monitoring, and recording of all electronic communications.
- Users must not perform any activity on the Company’s information systems which could damage the reputation of the Company.

- It is a violation of company policy to view, store, print, or redistribute any document or graphic file that could be offensive to others. Examples include communications, jokes, images, or media files which contain racial, gender, religious, nudity or sexual content.
- Users of the Company's information systems are responsible for all activities that occur using their accounts. Passwords must not be shared or stored in non-secure locations, except for a legitimate business purpose as granted by management.
- Passwords are to be complex in order to make them difficult for somebody else to guess. Suggestions on how to construct complex passwords may be found on StandardNet » Information Security » Tutorial: Use Smart Passwords
- All users are required to use a password-protected screensaver.
- All users must lock their computer (using the **Windows key + L**) if they leave for more than 15-minutes.
- All users must log off from and if possible power down their workstations at night. In some cases you may be required to leave your computer on overnight, but under no circumstances leave your system logged on. Always have the password protected screensaver turned on or log off from your system.
- It is prohibited to attempt to change a setting on your desktop computer that is not identified as a user option unless authorized by the Service Desk.
- It is prohibited to disable services (such as antivirus), add services that will block systems access by IT staff (such as personal firewalls), or change services unless you are authorized to do so by the Service Desk.
- Always store Company equipment in a secure location, including while on travel.
- All users must prevent Confidential or Restricted information such as personally identifiable information (SSN, health information, etc.) from being viewed while in their workspace. If possible, put all Confidential and/or Restricted information in a locked drawer or overhead. If this is not possible, all users must make certain that no Confidential or Restricted information is visible by someone passing their workspace.

CLASSIFICATION OF DATA AND INFORMATION

All company data and information will have one of the following three classifications.

Data and Information Classification	Description
Public	Information that may be widely distributed and is publicly available or is considered public domain. Examples of this would be: • Sales brochures • List of sales offices and addresses • Externally listed job openings
Confidential	Internal data and information that is not readily available to the public, and requires more control on access and disclosure to prevent potential loss to the organization or an individual. Initially, **all data and information is classified as Confidential** until management determines another classification is more appropriate. Examples of this would be: • Names of Customers • Internal Documents and Manuals • Personally Identifiable Information (PII) or Protected Health Information (PHI) on our customers and employees, such as address, SSN, or medical records.
Restricted	Information that needs to be closely controlled by limiting access to specific parties within the Company. This data and information may be available to only a few individuals or groups/teams. Examples of this would be: • Unannounced financial results • Information about potential mergers or acquisitions • Unannounced sales or claims trends

For more information on the handling and labeling of data and information, see Information Security Standard section "7.2 Information Classification Standard."

USE OF COMPANY E-MAIL SYSTEMS

- If an e-mail message contains Confidential or Restricted information, users must not forward it to another recipient unless (1) the other recipient is authorized to view the information or (2) the original sender approves the forwarding.
- E-mail messages are not a secure means of communication. Accordingly, users must be careful about the inclusion of Confidential or Restricted information in e-mail messages.
- E-mail messages must not be automatically forwarded to addresses outside the Company.
- E-mail systems are not intended to be used as permanent storage. Users must move business e-mail messages and attachments to a network server for permanent storage.

Further information on the Company's policy on Information Protection can be found on StandardNet under StandardNet » Business Conduct » Guide: Privacy and Confidentiality.

USE OF THE INTERNET

- The Company reserves the right to monitor and record all electronic communications. Existing security systems are capable of recording each Internet site visit, each chat and newsgroup visit, and each e-mail message or file transfer into and out of the company's internal networks.
- Users may participate in newsgroups or chats for legitimate business purposes if they apply the following standards:
  - Users must refrain from any unauthorized advocacy of any type and must refrain from the unauthorized endorsement or appearance of endorsement by the Company of any commercial product or service not sold or serviced by the Company.
  - Only those who are authorized by management to speak on behalf of the Company may do so to the media, in public gatherings, to a newsgroup, or chat room participants.
  - Users are prohibited from discussing Confidential or Restricted company information, customer data, trade secrets, or any other material covered by existing company policies and procedures in any public forum on the Internet such as chat groups, newsgroups, weblogs (blogs), etc.
- The Company retains the copyright and other intellectual property rights to any material posted to any public forum by any user in the course of their duties.
- Internet systems usage must align with the intent and spirit of the following:
  - Individuals may not use Company information systems for personal gain or advocacy.
  - Do not deliberately propagate any computer virus, worm, or Trojan horse program.
  - Do not knowingly violate any laws and regulations that affect the Company or user.
  - Do not knowingly download or distribute copyrighted software, data, or media files.
  - Do not knowingly disable or overload any Company computer system or network.
  - Do not knowingly circumvent any system intended to protect the privacy or security of another user.
  - Do not engage in on-line instant messaging (such as Internet Relay Chat) regardless of the services used.
- Transferring files into and out of the Company brings the risk of transferring computer viruses. Due to this risk, it is against Company policy for users of the Company's Internet facilities to engage in the following:
  - Do not download, upload, or transfer files using Peer-to-Peer (P2P) file sharing applications.
  - Do not download audio or video files unless there is an explicit business-related use for the material.
  - Do not open suspicious attachments from the Internet or from external e-mail systems.
  - Do not visit Internet sites that you are unfamiliar with or that have been provided to you from an untrustworthy source.

COMMUNICATING COMPANY INFORMATION

Information must only be shared based on the recipient's legitimate need to know for business reasons and in accordance with the Company's data and information classification levels.

- Unsolicited communications are to be treated with caution and not responded to unless the sender has been verified.
- Communications received in error are to be kept confidential and properly destroyed.
- Information obtained from Internet sources must be verified before being used for business purposes.

SOFTWARE LICENSING

- All users of company owned, leased, or controlled information systems must observe all license and contractual agreements affecting the use of a system's hardware or software.
- Use of software licensed to the Company on a non-company owned computer is prohibited unless approved by the IT Support Services group.

PROTECTING INFORMATION SYSTEMS

- All employees are responsible for the proper and secure use of Company-supplied equipment and services.
- Users must not test or attempt to compromise any security mechanism unless specifically authorized to do so by the Information Security Department.

  For example, users must not attempt to compromise anti-copying mechanisms built into commercial software.
- Users are prohibited from possessing on company premises, or using on or against company information systems, software or other tools which are designed to compromise information security (for example, password cracking software).

INFORMATION AND PHYSICAL MEDIA HANDLING

All users of the Company's information systems must manage the creation, storage, updating, copying, and deletion of data and information files in a manner that safeguards and protects the confidentiality, integrity, and availability of such files.

- Removable computer media such as CD-ROM's, USB portable drives, etc., are to be treated with care and protected from loss or disclosure of contents. This media must be properly handled and destroyed and when possible the contents should be encrypted or password protected.
- To ensure proper disposal, all documents which might potentially contain confidential or restricted information and all other media must be destroyed in a secure manner when no longer required.
- To comply with information handling procedures, all information and documentation is to be processed and stored according to the three Information Security Data and Information Classification levels.
- Handling Confidential or Restricted information:
  - When possible, passwords must be placed on information or documentation before sending to a printer.
  - Verify the receiver is available before sending a fax.
  - Such information must not be left on any external answering machine or voice mail system.

WORKING AWAY FROM THE OFFICE

Users traveling on business or working away from the office and who are in possession of the Company's assets are responsible for the security of the assets and the information they contain.

When users are working away from the office with laptops, mobile devices, cell phones, home machines, and PDAs, they are responsible for the security of the business equipment and information stored on these devices.

EQUIPMENT SECURITY

- Do not remove any Standard equipment from the work place unless you have prior management permission.
- Damage, loss, or theft of equipment must be reported immediately to the Service Desk at 971-321-8355.

REPORTING INFORMATION SECURITY INCIDENTS AND WEAKNESSES

All suspected information security incidents or weaknesses must be reported promptly to the Information Security Department.

Questions regarding this document can be directed to the Information Security Department via e-mail at infosec@standard.com.

RELATED DOCUMENTS

Description	Location
Information Security Policies	StandardNet » Information Security » Information Security Policies http://home.standard.com/business/information-security/is-policies.html
Information Security Standards	StandardNet » Information Security » Information Security Standards http://home.standard.com/business/information-security/is-standards.html
Further information can be found in the Company's *Guide to Business Conduct*	StandardNet » Business Conduct. http://home.standard.com/manuals/bus_conduct/index.html

FUNCTIONAL ROLES AND RESPONSIBILITIES

Audience Who is bound by this policy?	All employees, contractors, and vendors of the Company	
Policy Author Who is the one person designated to write this policy?	Director, Information Security	
Policy Owner Who has primary responsibility for developing this policy?	Director, Information Security and Director, Business Conduct	
Policy Authorized by Who approves this policy for publication?	Director, Information Security and Privacy Officer	
Grants Exceptions Who authorizes exceptions to this policy?	Director, Information Security, Director, Business Conduct or Privacy Officer	
Responsible Organization Organization that has functional responsibility for this policy.	Division:	Information Technology
	Department:	Information Security

REVISION HISTORY

Version	Date	Description of Changes
1.0	01/31/05	Original Policy (named "Automated Systems Use Policy")
2.0	09/04/07	Substantial changes based on new Information Security Policies published March 24, 2007; new file name following the Policy and Procedures Initiative's directions in the "Draft Guidelines for File Naming (8/23/07)."