Information Security Briefing Checklist

Section 1-- Agreement required by all Wells Fargo contractors

Please indicate your understanding and acceptance of each of the following information security requirements by placing an "x" in the box to the left of each heading:

☐ Classification of Information (Public, Internal Use, Confidential, Restricted)

- Know the classification(s) of the Information with which you work. Internal Use, Confidential and Restricted Consumer and Customer Information must be handled properly (as outlined in the remainder of this document). If you have questions, please ask your Manager.
- Understand how to properly mark/label the Information processed by your department.

☐ Distribution of Information

- Do not send or post information classified as Internal Use, Confidential or Restricted via the Internet or any other external network or by any other means (including personal websites, web logs ['blogs'], postal mail, phone and FAX) without proper authorization and security.
- Failure to properly protect consumer/customer or company information can result in significant consequences - including financial loss to consumers, Wells Fargo or its customers, loss of consumer/customer privacy and/or business, damage to Wells Fargo's reputation, potential legal action, subsequent system Intrusion, etc.
- Information distributed outside of Wells Fargo to third parties must be covered by an executed Agreement - such as a Non-Disclosure Agreement (NDA) or contract- that includes the proper non-disclosure language.
    - Such agreement(s) must be approved by the respective Information owner(s) as well as the Law Department or Contract Services.
    - Some NDAs may apply only to specific transactions; so, do not assume that you are covered just because there is an NDA

☐ Record Retention and Destruction/Disposal of Information

- Please be aware of the record retention policies of your department (for specific forms, files, records, etc. - what, where, how retained and for how long).
- Know the destruction and disposal methods used by your department.
    - Obsolete documents/forms containing Internal use, confidential and restricted information must be placed ln a secure shredding bin or shredded
    - Physically destroy or irretrievably erase all internal use, confidential or restricted data from electronic media (computer hard drives, CD-ROMs, diskettes, tapes, etc.) before disposal.
    - Incorrectly disposing of information processed by your department can result in significant consequences - including financial loss to consumers, Wells Fargo or its customers, loss of consumer/customer privacy and/or business, damage to Wells Fargo's reputation, potential legal action, subsequent system Intrusion, etc.

☐ Ensuring "Need to Know"

- Access to information by contractors should be determined based on business need (I.e., "need to know" in order to perform their job function).

- Contractors requiring access to Wells Fargo Information and/or resources must execute an appropriate NDA, Services Agreement or contract containing the proper non-disclosure language.
- Managers are required periodically to certify user IDs and/or access rights for users in their respective cost center(s)/AU(s) granted access to Wells Fargo resources.
- Be suspicious of any request or demand to ignore established identification procedures normally required to obtain access to information.

O Reporting and Monitoring

- Report to your Manager and Talent Management Specialist any unauthorized attempts to obtain information.
- Report to your Manager and Talent Management Specialist any suspected fraud or misuse of Wells Fargo information or resources.
- Report information security incidents or breaches to include theft or loss of information to your Talent Management Specialist
- Be aware that activities using Wells Fargo communication resources (phones, computer systems, email, etc.) are subject to monitoring at any time.

O Physical Security

- Do not leave company, consumer or customer information in a manner where it can be viewed by unauthorized persons - this includes video displays on computer monitors, documents left on desktops after work hours, etc.
- Secure information when not in use or under the control of an authorized person.
- The use of cameras In Wells Fargo facilities is not permitted without your Manager's approval.
- Challenge people who are not recognized as normally having access into a Wells Fargo work area. (This may be done in a respectful manner by simply asking, "May I help you?")
- If badges are used to control access to Wells Fargo facilities, use them properly and wear them where they can be seen easily by other team members - no tailgating (allowing someone to follow you through an entry when not permitted).
- Report immediately the loss of an access badge to your Talent Management Specialist and Manager so it can be deactivated in the access system.
- Follow the rules for obtaining badges for guests and visitors.

Section 2-- Agreement required by all contractors using computers or other electronic devices to obtain access to Wells Fargo networks, systems, applications or data (applicable headings may vary depending on Individual roles and responsibilities).

Please indicate your understanding and acceptance of each of the following information security requirements by placing an "X" in the box to the left of each heading or in the box to the right if not applicable:

O Password Construction and Protection O Not Applicable

- Use properly constructed passwords that….
  - are at least 8 characters in length
  - use at least 3 of 4 of the following character elements: lower-case letters, upper-case letters, numbers, or special characters - e.g., "Pksca57y" or "psca#57y"
  - do not include dictionary words or names of persons, places or things that might be guessed easily
- Additional "Do"s and "Don’t"s regarding passwords:

- Do not share your password(s) with anyone - including system and network administrators, as well as Managers.
- Do change your password(s) at least every 60 days
- Do change your password(s) if you suspect a compromise has occurred
- Do secure your password(s) properly if written down- e.g., on your person or within a locked container, not readily identified or labeled as a password

O Use of Internet O Not Applicable

- Be aware that use of the Internet is a privilege based on business need and should not be abused. (With proper management approval, limited appropriate personal use may be permitted during breaks, before and after scheduled work hours, etc.).
- Personal use must be appropriate and not for any purpose that violates the company's values.
- Exercise sound Judgment when downloading from or otherwise communicating via the Internet (see Virus Protection and Use of Email, below)
- Do not use audio or video streaming services or websites unless approved based on "business need"
- Do not download or forward digital video or audio flies -e.g., MP3s, MPGs, WMVs, etc. - as these activities may violate copyrights and can subject the user and Wells Fargo to legal penalties.
- Use only software that has been approved by Wells Fargo and is either owned by or properly licensed to Wells Fargo.
- All activities using Wells Fargo computing resources are subject to monitoring at any time.

O Virus Protection O Not Applicable

- Antivirus software is required on all desktop and laptop systems.
- Update virus definitions weekly (auto-update should be enabled If it is a feature of the software).
- You are responsible for making sure that antivirus systems are installed, active and up-to-date on your PC at all times (whether they are automatically or manually updated).
- All downloaded files and/or email attachments should be scanned prior to opening, saving, or execution (all auto-protect features should be enabled to ensure that this is done).
- Do not open email attachments or click on Internet links from untrusted sources.
- If you encounter a virus, notify the source of the infection (If known). If the virus cannot be repaired by antivirus software or for assistance in disinfecting a system, contact your technical support

O Use of Email and Instant Messaging O Not Applicable

- Be aware that use of email or Instant Messaging within Wells Fargo is a privilege based on business need and should not be abused (With proper management approval, limited appropriate personal use may be permitted during breaks, before and after scheduled work hours, etc.). Personal use must be appropriate and not for any purpose that violates the company's values.
- Do not access Web-based external, personal email or other email accounts - MSN, Hotmail, Yahoo, AOL, etc. - while connected to Wells Fargo networks.
- When communicating outside of Wells Fargo, your email/messaging address identifies you as a Wells Fargo team member; therefore, always give proper consideration to what a message says and to whom it is sent
- Email messages and attachments containing Confidential or Restricted information must be encrypted if sent outside of Wells Fargo.
- Do not send Confidential or Restricted information via Instant Messaging (since these on-line messages cannot be encrypted).
- Do not send attachments via Instant Messaging.

- Do not circulate email based "chain letters - It Is against Wells Fargo policy. Report all chain letters or other inappropriate use of email to either your Manager or local Technical Support and Talent Management Specialist.
- Immediately Report any threatening or harassing email/ messages
- Do not forward email messages warning of "new" viruses to other team members. If you receive such email messages from any source other than Wells Fargo Systems Communications or Virus Support, forward it to local technical support.
- Contact your local technical support if you need help dealing with spam (Junk email). (Most spam is easily identifiable and can be deleted without opening the email.)

O Laptops and Portable Devices O Not Applicable

- Secure laptops and other portable computing devices when not in use (preferably locked away and out of sight).
- Use security devices (cables and locks) when feasible and appropriate (this includes when travelling and when at work)
- When travelling, secure laptops and other Wells Fargo Information - always keep the laptop in your possession.
- When travelling store the laptop in hotel room safes if available
- Do not configure any portable computing device containing Confidential or Restricted information to “auto-login” (always manually enter your User ID and password to activate the device)
- Confidential or Restricted Information stored on a laptop/PDA must be encrypted.
- Do not enable the wireless capability of any portable computing device unless properly secured
- Report the loss or theft of any portable computing device immediately to your Manager and Talent Management Specialist

O Remote Access O Not Applicable

- Be aware that remote access is a privilege based on business need and should not be abused.
- Use only equipment (e.g. PC's, laptops, etc.) and software which is owned/leased and managed by Wells Fargo.
- Login to Wells Fargo systems for only as long as needed
- Protect any data stored and/or used at the remote workstation/site
- Protect remote access tokens and passwords and immediately report possible compromise and loss.
- Employ hard disk encryption, up-to-date anti-virus software, and an enabled personal firewall on all computers used for telecommuting
- When using wireless networking in combination with broadband service -e.g., satellite, DSL or cable modem for remote connection to Wells Fargo, ensure that 128-bit encryption is enabled for both the wireless access point (router or modem) and the wireless card on your computer.

O Systems Responsibilities O Not Applicable

(Applicable to System Administrators and System Support Personnel)

- Review the security plan(s) for the Information system(s) and application(s) with which you work,
- Be aware of the security requirements for the system(s) and application(s) for which you are responsible -e.g., maintain and review security logs, monitor system for intrusion and misuse, etc.).
- Be aware that no connections can be made to a Wells Fargo network without an approved security plan.

O Systems Development Responsibilities O Not Applicable

(Applicable to personnel Involved in the life-cycle of an information system- i.e., initial development through production and system modification)

- Follow Wells Fargo lnformation security policies/standards when planning, developing and maintaining Information systems.
- Do not create malicious software code - viruses, back doors, etc.

Violations of Information security policy may result in corrective action, up to and including termination of employment and/or criminal prosecution.

I certify that I have been briefed regarding my responsibilities to protect consumer, Wells Fargo proprietary and customer Information and that all questions I have regarding these responsibilities have been answered. I understand and agree to follow the security policies, rules and procedures covered in this briefing, that apply to my Job duties. Furthermore, I understand my responsibility to report unauthorized attempts to obtain information to my Manager and Talent Management Specialist.

Employee Name: _____

Employee Signature: _____

Note: This document contains basic requirements and guidelines relative to Wells Fargo Information Security policies. For further explanation on points contained in the checklist, please visit:
- http://formsonline.homestead.wellsfargo.com/forms/InformationSecurityPrimerforManagers.pdf
- http://policyworks.homestead.wellsfargo.com