Systems Access Requirements for Non-Employees

1. Agreement

Your company has entered into an agreement ("Agreement") with a Wells Fargo & Company entity ("Wells Fargo") that requires your company and any personnel it uses – including you – to comply with certain terms and Wells Fargo policies when performing work for Wells Fargo. This document is designed to orient you to Wells Fargo's policies, and explain specific requirements you must follow connected with any access you are provided to Wells Fargo systems, facilities or data, regardless of whether you work inside a Wells Fargo facility, or remotely from any other location ("Access"). Please be aware that Wells Fargo has the right to, and will, terminate your Access without notice if Wells Fargo reasonably suspects or determines you have not complied with these requirements.

2. Policies

a) You must abide by all of Wells Fargo's security policies, standards, and procedures. Any violation of a policy, standard or procedure subjects you to loss of all Access privileges, termination as a service provider to Wells Fargo, and any other penalties or remedies as described in the Agreement.

b) You must also comply with any new policies, standards, or procedures that may be developed during the period you have Access, if Wells Fargo gives you notice of those requirements.

3. Protecting Information

a) Wells Fargo policies classify information as public, internal use, confidential or restricted (explained below). You must adhere to the restrictions regarding those classifications, and direct any questions as to data classification to the individual at Wells Fargo who supervises your work, or your liaison within Wells Fargo ("Supervisor").

b) Regarding confidential and restricted information, you must (i) secure this information at your desk when unattended, (ii) promptly remove documents with this information from printers, copiers, scanners and fax machines to prevent unauthorized viewing, (iii) erase this information from whiteboards in areas that may be viewed by others (e.g., cubicles, conference rooms).

c) You must not forward or disclose any confidential or restricted information unless the intended recipient has a Wells Fargo business need-to-know the information. Further, if the intended recipient is someone other than a Wells Fargo employee, then the recipient must be covered under a signed Non-Disclosure Form protecting the information to be disclosed prior to sending it; this fact must be confirmed by your Supervisor.

d) You must encrypt the transmission of confidential information over any non-Wells Fargo network (e.g., Internet) and any internal and external transmissions that contain restricted information.

e) You must not fax confidential information to public machines (e.g., libraries, hotel business centers, etc.).

f) You must not fax restricted information to any location.

Categories of Wells Fargo information are:

- Public: generally available to the public and/or can be disclosed to anyone without personal or professional harm (examples include marketing brochures, business cards, press releases, published annual reports)
- Internal Use: limited to Wells Fargo employees/contractors with a business need-to-know (examples include employee handbook/policies/standards, employee or customer email addresses, phone directories, organization charts,)

- Confidential: includes sensitive customer/consumer or Wells Fargo information that, if disclosed to anyone other than employees or contractors with a business need-to-know and signed non-disclosure agreement, may have a negative impact to individuals or companies (examples include customer personal information such as SSN #s, consumer credit information, employee background checks or compensation amounts, system/network configurations, unannounced strategic business or marketing plans)
- Restricted: highest level of classification that, if compromised or disclosed to any employee or contractor without a strict business need-to-know, and a signed non-disclosure agreement, would likely result in severe damage to Wells Fargo, customers or employees (examples include passwords, authentication credentials, encryption keys)

4. Disposal of Materials
   a) Record retention requirements and procedures differ by category of records, files or data, and by type of Wells Fargo information at issue. You must follow the instructions of your Supervisor or the appropriate records coordinator prior to disposing of or destroying any records.
   b) You must only dispose of records, documents or papers by depositing them in a secure destruct container (not a recycling bin) or by shredding them using an approved crosscut shredder.
   c) You must physically destroy or irretrievably erase all confidential and restricted information from electronic media.
   d) If you service or remove drives, storage, or other data bearing media from Wells Fargo raised floor and data center environments, you must do these activities in the presence of Wells Fargo security, and must follow the dual custody requirements dictated by Wells Fargo security.

5. Safeguarding Assets
   a) You must safeguard all assets assigned to you by Wells Fargo, and must only use these assets for Wells Fargo's legitimate business purposes.
   b) You must maintain the security of any desktop or laptop personal computer (PC), Smartphone, peripheral, smart card, RSA token, password, PIN or other information, and hardware or software assigned to you by Wells Fargo in order to prevent unauthorized access. You must safely store or dispose of back-up electronic copies, as well as hard-copy versions of documents.
   c) You must never leave the device unattended without shutting down, locking it, or pressing CTRL + ALT + DELETE, then ENTER, as well as physically securing the device.

6. Unauthorized Access
   a) You must wear your badge or other credentials at all times while on Wells Fargo premises, and must promptly report to your Supervisor any lost badge/credentials.
   b) You must not abuse or misuse your authority or otherwise attempt to gain access into any data processing system, facility, room or area to which you have not already been granted access as part of the services that you are performing for Wells Fargo.
   c) You must not attempt to access or possess any Wells Fargo, customer, employee, or vendor information to which you are not entitled or authorized under the Agreement or for which you do not have a business need-to-know.

7. Logon Credentials
   a) You must not give any computer password, RSA token PIN or RSA token display to any other person. You must not give the assigned logon ID to any other person unless authorized in writing by your Supervisor. You must not leave any written version of this information near the device to which it corresponds. You must inform your Supervisor of any obsolete logon ID or passwords so that they may be disabled.

b) You must not obtain, possess or use in any manner another person's logon ID or computer password, RSA token PIN or RSA token display. If you come into possession of another person's logon or computer password, RSA token PIN or RSA token display information, you (i) must immediately inform the affected individual so the logon/password may be changed, and (ii) must not keep a record of or disclose the logon/password, RSA token PIN or RSA token display to any other person.

8. Equipment

a) If required by your Supervisor in relation to the services you perform for Wells Fargo, you will be asked to use only Wells Fargo-provided equipment to access Wells Fargo systems. In this case, you must NOT (i) connect personal items (or items provided by your company, such as a company-issued laptop or other device) to the Wells Fargo network (e.g., no iPod, iTunes, iPhones, MP3 players, flash drives, etc.), or (ii) download onto Wells Fargo equipment any games or other functionality/applications.

b) If asked to use Wells Fargo-provided equipment, you must only use this equipment (i) in furtherance of the services you provide to Wells Fargo, (ii) to connect to Wells Fargo-owned and maintained networks, and (iii) to store Wells Fargo-related information and not personal or other company information.

c) You must not install software that can be used to circumvent access controls (e.g., password crackers, daemon dialers, keystroke capture software, etc.) on any on any equipment provided to you by Wells Fargo or any system or device that you use for Wells Fargo business.

d) You must not use any camera or other recording device while on Wells Fargo premises (e.g., still or video camera, cell phone, PDA) without your Supervisor's approval.

9. Securing Portable Devices

You must appropriately secure any Wells Fargo-issued devices (e.g., laptop, Smartphone) and the information on them according to the following:

a) You must only store information needed to perform a task, and must immediately delete information no longer needed for business purposes, such as emails and project files.

b) You must not allow any unauthorized individuals to access or use Wells Fargo-issued devices.

c) In the office, you must appropriately secure portable devices by locking screens and/or locking in secure cabinet.

d) *While traveling, you must keep portable devices with you, or lock them in car trunk or hotel safe. You must never place portable devices in checked luggage.*

10. Communications

a) You must not use Wells Fargo e-mail or the Internet for reasons other than to conduct Wells Fargo business.

b) You understand that all information sent via the Wells Fargo systems is considered to be the property of Wells Fargo, and understand that all communications may be viewed or monitored.

c) *You must not participate in any non-Wells Fargo chat rooms, blogs, or message boards, and must not conduct* any online gambling or any illegal activity while using Wells Fargo equipment. You must not view, or forward, any pornographic images or material on Wells Fargo equipment.

d) You must not circulate email-based spam or other chain letters; instead, you must forward such email to the email.misuse@wellsfargo.com mailbox.

e) You must not forward emails warning of new viruses or viral attacks to other individuals on the Wells Fargo system; instead, you must forward such emails to the Wells Fargo Security Operations Center (SOC).

f) You must not respond to phishing e-mails requesting private information such as credit card, SSN #s or bank account numbers; instead, you must send these emails to ReportPhish@wellsfargo.com.

g) You must not solicit or distribute unapproved non-work-related information, such as requests for charitable or political causes.

11. Incidents and Reporting

a) You must promptly report information security incidents. An information security incident may include, but is not limited to, the following situations: a Wells Fargo-issued PC or laptop, Smartphone or other storage device is stolen; Wells Fargo, customer, consumer or personnel information is modified, destroyed, lost, misdirected or taken in any unlawful action such as a theft or burglary; any unauthorized use or attempted misuse of personal authenticators, terminal sessions, or equipment.

b) You must immediately report any security incident to your Supervisor and to Wells Fargo Security Response Center (SRC) by either calling 877-494-9355, option 3, or 001-480-437-7599 for international callers who do not have 877 service. You can also send email to CompromisedData@WellsFargo.com. If you prefer to report the incident anonymously, you may instead contact the Ethics Line at 1-800-382-7250 or online at www.tnwinc.com/webreport.

12. Privacy

a) Wells Fargo provides a Privacy Policy Disclosure to each individual customer when information is initially gathered or a new account is opened. The main tenets of that policy are:
   a. Wells Fargo does not sell customer information to third parties.
   b. Wells Fargo does not share customer information with outside parties who may wish to market their products to our customers.
   c. Within the Wells Fargo companies, we safeguard customer information carefully.

b) If your work for Wells Fargo will bring you into contact with Wells Fargo customers or customer data, you must adhere to Wells Fargo's Privacy Commitments to its customers (as noted above)
   i. You must work with your Supervisor to ensure that you understand and can comply with the Wells Fargo Privacy and Solicitation Policy.
   ii. You must not, by act or omission, sell or otherwise make available customer information to third parties or share customer information with outside parties who may wish to market their products to Wells Fargo's customers.

c) Wells Fargo provides its customers with choices about how their information may be shared for marketing and other purposes.
   i. You must not share any customer information without first receiving the approval of your Supervisor.
   ii. Wells Fargo automatically observes a temporary 30-day waiting period for new customers before sharing any information across affiliate lines for marketing.

d) You agree to honor customer preferences for marketing purposes. Individual consumers and businesses can choose not to be contacted by Wells Fargo for marketing purposes, even if they're not a customer. The contact options are:
   - Do Not Call
   - Do Not Mail
   - Do Not E-mail

All solicitation preferences expressed by Wells Fargo customers and non-customers are stored on Hogan CIS.

13. Telephone Solicitation

a) You must ensure that in all work you do for Wells Fargo, all sales and marketing practices comply with state and federal telemarketing laws. All telemarketing lists must be scrubbed and cannot be used past their expiration date. Expiration dates vary depending on the type of campaign. It is Wells Fargo's policy to scrub business customer call lists against the National Do Not Call (DNC) Registry and state Do Not Call lists in order to remove home-based business phone numbers from the campaign. Any concerns you have regarding solicitation policies *must be directed to your Supervisor.*

b) You acknowledge that Cell phones and Caller ID have the following unique telemarketing requirements.
   i. Cell Phones.it is against Wells Fargo's policy to knowingly call a customer's cell phone for solicitation purposes without Group Risk Officer approval, unless the customer has given express consent to call that cell phone number. Cell phones cannot be called using an auto-dialer for any purpose without express consent.
   ii. *Caller ID.all telemarketing calls, including calls made to business customers, must be made from an* "approved phone" that transmits the caller's name and phone number. This includes sales calls made for Wells Fargo business purposes from a team member's home or cell phone.

14. E-mail

Any e-mail that promotes Wells Fargo's products and services must comply with Wells Fargo's e-mail policy requirements and state and federal laws. Before sending e-mails to customers or prospects, you must confirm with your Supervisor whether it is an acceptable business practice, and review the e-mail requirements and guidelines included in the Privacy *and Solicitation Policy.*

Please note that requiring contractors to sign the Systems Access Agreement is not a contractual requirement but it is considered a "best practice".

*I have reviewed and will comply with the Systems Access Requirements as stated in this document.

*Managed Resource Legal Name Naqibullah Rahmatyar

MRS Work Order #_____

Managed Resource Signature w/ Date of Signature N Rahmat 1-23-2022