

This is an Agreement (the "Agreement") between State Farm Mutual Automobile Insurance Company, its subsidiaries and affiliates ("State Farm"), having its principal place of business located at Bloomington, Illinois, and _____ (hereinafter referred to as "the Agent" or "you" or "your"), of _____.

WHEREAS, you desire to use and/or store State Farm Confidential or Customer Information on certain equipment, electronic media or software not provided to you by State Farm ("non-State Farm Equipment, Media and Software"); and,

WHEREAS, it is the desire of State Farm to permit such use and storage with respect to certain non-State Farm Equipment, Media and Software subject to the terms of this Agreement;

NOW THEREFORE, in consideration of the mutual promises herein set forth, the parties agree as follows:

1. Superseding of Previous Forms. The parties agree that this Agreement shall replace and supersede any other agreement as to the subject matter contained herein.

2. Confidential or Customer Information.

a. For purposes of this Agreement, "Confidential or Customer Information" shall include (i) any information defined as confidential information under your State Farm Agent Agreement; (ii) any information related to a customer or consumer that has been defined as "non-public personal information" as set forth in the Financial Services Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act"; (iii) any information related to a customer or consumer that has been defined as "consumer information" as set forth in the Fair and Accurate Credit Transactions Act of 2003; (iv) and any other customer or consumer information that has been identified under any other state, federal or provincial law which might relate to the privacy, handling, destruction or protection of such customer or consumer information. Confidential or Customer Information shall not include publicly available information as such term is defined by the Gramm-Leach Bliley Act or its associated regulations but shall include any list, description, or other grouping of customer or consumer information that is derived using any customer or consumer information.

b. You are reminded that you are obligated to keep strictly confidential any Confidential or Customer Information, and will take all reasonable steps to maintain the value and confidentiality of such Confidential or Customer Information, including informing your office staff of this responsibility and assuring their compliance.

3. Obligations.

a. Storage of Confidential or Customer Information: State Farm shall permit you to store Confidential or Customer Information, as defined in this Agreement, on non-State Farm Equipment, Media and Software provided that you are the sole and exclusive owner of any such non-State Farm equipment and media and that you are either the owner of or have obtained license rights to any such non-State Farm software and further provided that you comply with this Agreement and the specifications attached hereto and incorporated herein as Exhibit A.

b. Right to Audit: State Farm or its designated representative shall, upon 5 days advance written notice, have the right to access, audit or monitor your use of the non-State Farm Equipment, Media and Software and:

1. You shall cooperate fully with State Farm or its designated representative in effectuating any such access, audit or monitoring including but not limited to providing State Farm or its designated representative with access to any such non-State Farm Equipment, Media and Software;
 2. You shall cooperate fully with State Farm to resolve any audit or other findings to State Farm's satisfaction; and,
 3. You shall reimburse State Farm, upon State Farm's request, for any reasonable expenses incurred by State Farm to conduct such access, audit or monitoring.
- c. Modifications: You agree that you shall implement any repairs, upgrades, updates, modifications, maintenance, enhancements, alterations or changes to any non-State Farm Equipment, Media and Software as may be determined by State Farm in order for you to comply with the specifications attached in Exhibit A and that you shall be solely responsible for any costs that may be incurred with respect to any such repairs, upgrades, updates, modifications, maintenance, enhancements, alterations or changes.
 - d. Repairs: You agree that you will not order, permit or allow repairs to the non-State Farm Equipment, Media and Software without first obtaining the prior written approval of State Farm.
 - e. Access: You agree that you will not allow any person or entity not authorized by State Farm to access any Confidential or Customer Information.
 - e. Loss or Theft: You agree to immediately notify State Farm in the event that any non-State Farm Equipment, Media and Software which contains Confidential or Customer Information is lost, stolen, damaged, or destroyed. You further agree that you shall be solely responsible for any costs, including but not limited to identity theft protection coverage or services provided to customers, that may be incurred by State Farm that may be related to the loss, theft, damage or destruction of any non-State Farm Equipment, Media and Software which contains Confidential or Customer Information.
 - f. Court Orders: You agree to cooperate fully with State Farm in the event that State Farm must respond to any court order, subpoena, criminal investigation, government order or official decree which might include the non-State Farm Equipment, Media and Software or the Confidential or Customer Information contained thereon. This may include (i) allowing State Farm to take full possession and control of any such non-State Farm Equipment, Media and Software and (ii) State Farm providing any such non-State Farm Equipment, Media and Software to a court, governmental body or other entity as may be appropriate. You further agree that State Farm shall not be responsible for any loss or damages you may incur as a result of State Farm taking control or possession of any non-State Farm Equipment, Media and Software.
4. Term.
- a. This Agreement shall terminate immediately without further action of either party if (i) either party terminates your State Farm Agent's Agreement, unless the above termination of the State Farm Agent's Agreement or the State Farm Trainee Agent's Agreements is only for purposes of your signing a subsequent State Farm Agent's Agreement; (ii) you are no longer the sole and exclusive owner of any such non-State Farm Equipment, Media and Software.
 - b. State Farm may terminate this Agreement without cause by providing 30 days written notice. In the event of termination of this Agreement, you agree that you will use reasonable means

for the safekeeping of the non-State Farm Equipment, Media and Software until such time that State Farm may remove any Confidential or Customer Information from the non-State Farm Equipment, Media and Software.

- c. In the event of termination of this Agreement, you shall make available and accessible to State Farm any non-State Farm Equipment, Media and Software which may contain any Confidential or Customer Information and shall permit and enable State Farm to take any and all steps that may be necessary to completely remove any Confidential or Customer Information from such non-State Farm Equipment, Media and Software.
5. Amendments. State Farm may amend this Agreement and Exhibit A from time to time and:
- a. State Farm shall provide no less than 5 days written notice to you of any amendment to this Agreement or Exhibit A. Written notice shall include memorandum announcements, email, facsimile transmissions, and other means of electronic communication;
 - b. Your obligations hereunder shall apply with equal force to any such amendments;
 - c. Following any notification of any such amendment, your continued use of non-State Farm Equipment, Media and Software to store Confidential and Customer Information shall be deemed as your acceptance of any such amendment.
 - d. In the event you do not wish to agree to any such amendment you will immediately notify State Farm that you are terminating this Agreement and will immediately return all Confidential or Customer Information to State Farm Equipment and Software provided under the Agent Automation System Agreement and remove all Confidential or Customer Information from any non-State Farm Equipment, Media and Software.
6. Indemnification. The parties each expressly agree that each shall indemnify and hold the other fully harmless against any losses, damages or expenses stemming from third party claims or lawsuits (including costs and reasonable attorneys' fees), the other receives as a result of the negligent acts or omissions or misconduct of the other, or of either party's employees or agents acting within the scope of this Agreement. For purposes of this Section, the term "agents" does not mean State Farm's insurance agents.
7. LIMITATION OF LIABILITY. EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, STATE FARM SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY KIND WHATSOEVER, RESULTING FROM YOUR USE, AVAILABILITY OR UNAVAILABILITY OF THE NON-STATE FARM EQUIPMENT, MEDIA AND SOFTWARE BY YOU OR YOUR OFFICE STAFF.
8. Waiver. Any waiver by either party of a violation of this Agreement shall not imply a waiver of any subsequent violation, whether the same or different violation.
9. Miscellaneous. You may not assign this Agreement to any other person, party or entity. Nothing in this Agreement shall in any way change, alter or amend any other agreements between you and State Farm.
10. Survival. The following sections shall survive termination of this Agreement: Waiver, Limitation of Liability, Indemnification, Term Section 4.c., Confidential or Customer Information.

This Agreement shall be a contract binding upon each of the parties hereto, or any permitted successors and assigns, represents the entire agreement between parties, and cannot be amended or modified except as agreed to by each of the parties in writing. The parties agree, however, that State Farm may amend Exhibit A at any time without obtaining your agreement.

IN WITNESS WHEREOF, Agent and State Farm have caused this Agreement to be executed below. This Agreement shall become effective on the date the second of the two parties to sign executes this Agreement below.

By _____ (signature) _____
Agent Date

By _____ (printed) _____
Agent Date

By _____
Authorized Representative Date

1 Exhibit A – Requirements and Detailed Controls for Using or Storing State Farm Confidential or Customer Information on Non-State Farm Equipment, Media and Software (version 2009)

The following sections outline the controls needed to protect State Farm confidential or customer information (also called “State Farm data”) on non-State Farm equipment, media and software:

- All controls contained within this document are required.
- Many required devices and software packages may contain more configurable settings than documented below. For settings not specifically called out in the following controls, configuration discretion is left to the agent. Unless otherwise stated, the manufacturer of the devices and software packages chosen are at the discretion of the agent, with the sole requirement that all controls detailed below can be enforced by the device and/or software.
- Any electronic media that is not within the Agent Automation System Agreement and that contains State Farm confidential or customer information is considered non-State Farm equipment, media and software.
- The Agent has the responsibility to ensure that non-State Farm equipment, media and software containing State Farm data be accessed for the purpose of conducting agent business activities as needed.

1.1 Software/Application

All software used on the non-State Farm equipment, media and software must be approved by State Farm if that equipment will contain State Farm data.

Software cannot be used on non-State Farm equipment, media and software if any aspect of it will undermine the outlined controls.

Controls apply to **all** software on the non-State Farm equipment, media and software containing State Farm data, not just those applications using the State Farm data.

Default user/administrator passwords must be changed and must meet the following requirements:

- Must be unique
- Cannot be the same password used by the agent or any agent team member to access any State Farm equipment or networks
- Must be at least 8 characters long and must satisfy 3 out of 4 of the following conditions:
 - Must contain at least one upper case character
 - Must contain at least one lower case character
 - Must contain at least one numeric character
 - Must contain at least one special character

- Passwords may **not** be:
 - Based on personal information which someone could easily guess or obtain (e.g., State Farm alias, all or part of a name or nickname, telephone numbers, date of birth, etc. . .).
 - A word from any dictionary in any language.
 - Sequential in number or letter combination (e.g., “12345678”).

The software/application must be configured to update the underlying product at least once a month if the capability exists.

With the exception of querying manufacturer for updates, the ability to send data back to the software manufacturer must be disabled (example: error reports, usage metrics, etc. . .).

All product updates must occur via port 80 http or 443 https.

1.2 Data

An agent’s non-State Farm equipment, media and software must **not**:

- Store or allow access to State Farm data from any mobile devices of any type, except for approved laptops that meet controls contained within this document.
- Include the storage or use of financial/credit card account number, including the CVV/CVV2 code, passwords/PIN, mother’s maiden name, medical information, health policy information, digital or electronic signatures, biometrics (e.g., voiceprint) or images that include the previously listed data.
- Allow State Farm data to be transferred to/from non-State Farm equipment, media and software via any transferable media (CD, DVD, USB jump drive, external drive, etc. . .), except for encrypted backups by approved vendor, as specified by controls contained within this document.

1.3 Network/Systems Connectivity

An agent’s non-State Farm equipment, media and software must **not**:

- Provide Web hosting, e-mail hosting, or other public-facing services (i.e., operating as a Web site, Web server, e-mail server, etc. . .).
- Allow the transfer of State Farm data to/from the non-State Farm equipment, media and software via any network connection except for encrypted backups by approved vendor as specified by controls within this document.
- Allow remote access to/from the non-State Farm equipment, media and software unless specifically needed by contracted and approved vendor to perform maintenance/updates.
 - Note:** This includes, but is not limited to, remote desktop connection software, vendor services, etc . . .
- Be connected, in any fashion, to State Farm’s network or network infrastructure.

1.3.1 Systems Maintenance/Administration

For purpose of supporting the agent's non-State Farm equipment, media and software, the vendor contracted by the agent will meet these listed items.

- Vendor will establish a static IP for Internet connectivity with the Agent's office.
- Vendor will create a Branch Office Tunnel model of connectivity with Agent's office.

1.3.2 Managed IPS/IDS Services

Internet access is permitted on non-State Farm equipment, media and software containing State Farm data if the agent will establish a Managed IPS/IDS Service.

This managed service is not to have any access to the internal network or data on the non-State Farm equipment, media and software owned by the agent. Also all connectivity between the managed services and the agent non-State Farm equipment should be considered as a public network and not to be treated as an extension of the agent's non-State Farm equipment.

This managed service will have the minimum capabilities/features associated between the service and the non-State Farm equipment, media and software.

- Encrypted communication between non-State Farm equipment and the managed IPS/IDS service
- Capability of IDS/IPS and event collection
- Policy management and administration; this includes the ability of the agent to request changes to the security policies associated with IPS/IDS functionality
- If devices/appliances are used then device upgrade and patch management are to be established as is indicated in other sections of this Exhibit
- Comprehensive reporting; on-demand and scheduled
- Real time reporting and alerting on defined thresholds for all security events exceeding baseline
- Customer (Agent) notification of major security, health, intrusion events
- Identify potential threats and block source IP addresses of known attack origins
- Receive and implement threat advisories and implement new rules as Internet threats occur or change

1.4 Wireless Access Point

A Wireless Access Point (WAP) is a hardware device that connects wireless devices together to form a wireless network.

The following configurations are required of the WAP:

1.4.1 Administrative Password

The administrative password provided with the Wireless Access Point must be changed from the default and must meet the following requirements:

- Must be unique
- Cannot be the same password used by the agent or any agent team member to access any State Farm equipment or networks
- Must be at least 8 characters long and must satisfy 3 out of 4 of the following conditions:
 - Must contain at least one upper case character
 - Must contain at least one lower case character
 - Must contain at least one numeric character
 - Must contain at least one special character
- Passwords may **not** be:
 - Based on personal information which someone could easily guess or obtain (e.g., State Farm alias, all or part of a name or nickname, telephone numbers, date of birth, etc. . .).
 - A word from any dictionary in any language.
 - Sequential in number or letter combination (e.g., “12345678”).

1.4.2 Remote Administration

The ability to administer the Wireless Access Point remotely must be disabled from the public WAN port (i.e., Internet).

1.4.3 Service Set Identifier (SSID)

The SSID for the Wireless Access Point must be changed to a non-identifiable ID.

Note: The use of STATEFARM, STATE FARM, SF, any State Farm trademark, last names or any derivations of the former as the SSID is prohibited.

1.4.4 Encryption

Wi-Fi Protected Access (WPA or WPA2) must be used.

TKIP or AES encryption algorithm must be used.

A complex key of at least 20 characters with at least one special character must be used.

1.4.5 Firmware

The firmware for the Wireless Access Point must be updated at least quarterly if updates are available.

1.5 Wireless Client

A wireless client is any device that connects wirelessly to a Wireless Access Point.

All wireless clients must use the same wireless system control (WPA or WPA2) and encryption algorithm as chosen in the WAP configuration.

1.5.1 Ad hoc/Peer to Peer

Wireless client cannot be used in ad hoc or peer-to-peer mode.

1.5.2 Automatic connections

Disable automatic connection to un-trusted wireless networks.

1.6 Hardware Firewall

A hardware firewall is a device positioned between network segments to deny, allow, and proxy traffic. A hardware firewall is required, and installation of this device must be between the public Internet and any non-State Farm equipment, media and software or networks that contain State Farm data. All traffic entering from, or exiting to, the Internet must pass through a hardware firewall device.

The following configurations are required of the hardware firewall before being connected to the public Internet.

1.6.1 Rule Sets

Inbound

The hardware firewall must be set to deny all inbound traffic.

Note: An additional firewall rule can be applied to give a specific vendor the ability to temporarily administer their software remotely. This rule must be removed once administration is complete.

The following requirements must be met when applying the rule:

- Must specify source IP
- Must specify destination IP
- Must be restricted to 1 port

The vendor will send written notification and supply the port to be opened. This rule must be removed no later than 48 hours after administration is complete.

Outbound

The hardware firewall must be set to deny all outbound traffic, with the exception of the ports listed below.

- UDP 53 (Domain Name Server)
- TCP 80 (World Wide Web HTTP)
- TCP 443 (HTTP over TLS/SSL)
- TCP 25 (e-mail)
- TCP 110 (e-mail) or TCP 995 (secure e-mail)

1.6.2 Administrative Password

The administrative password provided with the hardware firewall must be changed from the default provided by the manufacturer and must meet the following requirements:

- Must be unique
- Cannot be the same password used by the agent or any agent team member to access any State Farm equipment or networks

- Must be at least 8 characters long and must satisfy 3 out of 4 of the following conditions:
 - Must contain at least one upper case character
 - Must contain at least one lower case character
 - Must contain at least one numeric character
 - Must contain at least one special character
- Passwords may **not** be:
 - Based on personal information which someone could easily guess or obtain (e.g., State Farm alias, all or part of a name or nickname, telephone numbers, date of birth, etc. . .).
 - A word from any dictionary in any language.
 - Sequential in number or letter combination (e.g., "12345678").

1.6.3 Remote Administration

The remote administration of the hardware firewall, by the approved vendor established by the agent, is allowed provided it is accomplished via controls established in section 1.3.1 of this Exhibit.

1.6.4 Network Address Translation (NAT)

Network Address Translation via the hardware firewall must be enabled. The subnet address created for the Local Area Network (LAN) must be different than the subnet for the Wide Area Network (WAN).

1.6.5 Port Forwarding

The ability to do "Port Forwarding" (forwarding a network port from one network node to another) via the hardware firewall must be disabled at all times, except when vendor administration is needed.

1.6.6 Demilitarized Zone (DMZ)

Usage of the DMZ feature of the hardware firewall is prohibited.

1.6.7 Firmware

The firmware for the hardware firewall must be updated at least quarterly, if updates are available.

1.7 Software Firewall

A software firewall is an application installed on a workstation or server to deny and allow traffic to pass through. In addition to the hardware firewall, a software firewall is also required on all workstations and servers.

The following configurations are required of the software firewall:

- The software firewall must be configured to update the underlying product at least once a month.

1.7.1 Rule Sets

Inbound

The software firewall must be set to deny all inbound traffic.

Note: An additional firewall rule can be applied to give a specific vendor the ability to temporarily administer their software remotely. This rule only applies to equipment with software that the vendor is remotely administering. This rule must be removed once administration is complete.

The following requirements must be met when applying the rule:

- Must specify source IP
- Must specify destination IP
- Must be restricted to 1 port

The vendor will supply the port to be opened. This rule must be removed once administration is complete.

Outbound

The software firewall must be set to allow all outbound traffic.

Note: Restricting outbound traffic on the software firewall is not required, but will increase the protection. It can be done at the agent's discretion.

1.7.2 Administrative Password

The default administrative password (provided with the software firewall) must be changed from the default, and must meet the following requirements, if technically feasible:

- Must be unique
- Cannot be the same password used by the agent or any agent team member to access any State Farm equipment or networks
- Must be at least 8 characters long and must satisfy 3 out of 4 of the following conditions:
 - Must contain at least one upper case character
 - Must contain at least one lower case character
 - Must contain at least one numeric character
 - Must contain at least one special character
- Passwords may **not** be:
 - Based on personal information which someone could easily guess or obtain (e.g., State Farm alias, all or part of a name or nickname, telephone numbers, date of birth, etc. . .).
 - A word from any dictionary in any language.
 - Sequential in number or letter combination (e.g., "12345678").

1.7.3 Product Updates

If capable, the software firewall must be configured to update the underlying product at least once a month.

If automatic update capabilities don't exist, a procedure must be established to make manual checks for product updates.

1.8 Antivirus Software

Antivirus software is a class of software that scans hard disks for viruses on a computer. Antivirus software is required on all workstations and servers.

The antivirus software used must be chosen from an approved antivirus software vendor, as identified on the US-Cert.org Web site: http://www.cert.org/other_sources/viruses.html.

The following configurations are required of the Antivirus software:

1.8.1 Virus definition/product updates

The antivirus software must be configured to update the virus definitions automatically and be scheduled for daily updates.

The antivirus software must be configured to update the underlying product at least once a month.

Disable the ability to send virus data back to the software manufacturer.

All product updates must occur via port 80 http or 443 https.

1.8.2 Scanning Configurations

The antivirus software must be configured to perform an automated full scan weekly (at a minimum).

The antivirus software must be configured to enable access protection/real-time scanning.

The antivirus software must be configured to automatically delete viruses upon detection.

The antivirus software must have rootkit detection.

1.9 Antispyware Software (Malware)

Antispyware software is a class of software that scans hard disks and removable media for malicious software and spyware.

The antispyware software used must be chosen from an approved antispyware software vendor, as identified on the US-Cert.org Web site: http://www.cert.org/other_sources/viruses.html.

The following configurations are required of the antispyware software:

1.9.1 Antispyware Definition/Product Updates

The antispyware software must be configured to update the antispyware definitions automatically and be scheduled for daily updates.

The antispyware software must be configured to update the underlying product at least once a month.

Disable the ability to send spyware data back to the software manufacturer.

All product updates must occur via port 80 http or 443 https.

1.9.2 Scanning Configurations

The antispyware software must be configured to perform an automated full, deep scan weekly (at a minimum).

The antispyware software must be configured to enable access protection/real-time scanning.

The antispyware software must be configured to automatically delete spyware upon detection.

1.10 Operating System Configuration

Only the following operating systems are acceptable:

- Microsoft Windows XP Professional
- Microsoft Windows Vista Home
- Microsoft Windows Vista Professional
- Microsoft Windows Server 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

All operating systems must have the most recent supported service pack installed on them, along with all applicable security updates. No beta or evaluation versions of an operating system are allowed.

All third-party, non-driver, non-Microsoft applications must be removed from the base system. Approved applications may be installed after all policy/base configurations outlined in this document have been made.

In order to facilitate the required vendor audit, all non State Farm Equipment, Media and Software computing equipment must have the Microsoft Baseline Security Analyzer installed prior to use by agents or team members.

1.10.1 Account Policies

Password Policy

Configure the **Enforce Password History** setting to a value of 4 passwords.

Configure the **Maximum Password Age** setting to a value of 90 days.

Configure the **Minimum Password Age** setting to a value of at least 2 days.

Configure the **Minimum Password Length** setting to a value of 8 or more.

Configure the **Passwords Must Meet Minimum Complexity Requirements** setting to **Enabled**.

Account Lockout Policy

Configure the **Account Lockout Duration** setting to a value of, at most, 30 minutes.

Configure the **Account Lockout Threshold** setting to a value of no more than 6 attempts.

Configure the **Reset Account Lockout Counter After** setting to a value of at least 30 minutes.

Configure the OS to automatically disable user accounts when not used for 60 days.

Audit Settings

Out of box Systems Event Logs must remain enabled.

Configure each log to a minimum size of 32MB.

Select **Success** or **Failure** for each of the following:

- Account Logon Events
- Account Management Logon Events
- Policy Change

Select **Failure** for each of the following:

- Object Access
- Privilege Use

Mark System Events: **Enable**

User Rights

Terminal Services must be restricted to administrators.

Terminal Services can only be used on servers where direct access is not possible.

Security Options

Each user must have a unique account. User accounts cannot be shared.

End user accounts used for daily activities must be members of the Users account, but not in an account that allows for elevated access.

Each user that requires administrative access must have an additional unique account with administrative privileges.

Configure the Accounts as follows:

- Disable the **Everyone** account; it cannot be used for any purposes.
- **Authenticated Users** only.
- **Guest Account Status** setting to **Disabled**
- **Administrator Account Status** setting to **Disabled**

Specify a new name in the Accounts as follows:

- Rename the Administrator account.
- Rename Guest account.

Each user must know only his or her own password. Passwords cannot be shared.

The default administrative password must be changed. The new password must meet the following requirements:

- Must be unique
- Cannot be the same password used by the agent or any agent team member to access any State Farm equipment or networks
- Must be at least 8 characters long and must satisfy 3 out of 4 of the following conditions:
 - Must contain at least one upper case character
 - Must contain at least one lower case character
 - Must contain at least one numeric character

- Must contain at least one special character
- Passwords may **not** be:
 - Based on personal information which someone could easily guess or obtain (e.g., State Farm alias, all or part of a name or nickname, telephone numbers, date of birth, etc. . .).
 - A word from any dictionary in any language.
 - Sequential in number or letter combination (e.g., "12345678").

The password used must be different on every workstation/server (administrator account).

Timeout Settings

The OS will be set to lock the workstation after 20 minutes of inactivity.

1.10.2 Network Policies

Anonymous connections must be disabled.

Network listening services not provided by software on the approved list must be stopped or uninstalled.

Minimum session security for NTLM SSP based (including secure RPC) clients:

- Require message integrity
- Require message confidentiality
- Require NTLMv2 session security
- Require 128-bit encryption

1.10.3 Logon Policies

OS must be configured not to display last signed on username.

OS must be configured to force CTRL-ALT-DEL for interactive logons.

OS must be configured to disable automatic logons.

All workstations and servers must be secured by being locked or logged off when unattended.

Setup logon prompt: "System requires authorization. Unauthorized access is illegal."

Password-protected screen savers will be set to 30 minutes or less to automatically protect unattended workstations.

1.10.4 Directory Structure

All disks must use NT File System (NTFS).

Do not store LAN Manager Hash value on next password change. Set to **Enable**.

LAN Manager Authentication Level: **NTLM Responses Only**.

1.10.5 Operating System Updates

Automatic Update must be configured to automatically download and install critical Windows Updates daily.

All other updates from windowsupdate.com, including optional and hardware, must be installed monthly.

1.11 Microsoft SQL Server 2005

For agents that contract with an approved vendor, the agent office must have Microsoft SQL Server 2005 installed, setup, and integrated with windows security and with the prospecting application in use on the non-State Farm equipment housing State Farm data.

The minimum version of SQL Server 2005 will be the Workgroup Edition.

Agent will ensure that expedient updating and patching of SQL Server 2005 will occur as is discussed in other software/hardware requirements in this Exhibit.

1.12 Physical Security

Agent office must subscribe to a centralized monitoring system.

1.12.1 Workstation/Server Controls

All workstations, laptops, and servers with State Farm data must not be stored in common areas (example: a team member's occupied desk is not a common area. A break room, fax room, lobby, reception area, or unoccupied desk is a common area.

All servers with State Farm data must be housed in an area with controlled access (examples of controls that would meet this requirement are a locked room, locked cabinet, or locked closet). Agents must maintain control of these locked areas.

All workstations, laptops, and servers with State Farm data must use a workstation physical security device (examples of controls that would meet this requirement are a cable with lock or workstation locking systems).

Use a visitor log to maintain a physical assessment trail of visitor activity/access to locked server area.

Servers must not be viewable from public areas.

1.12.2 Network Control Devices

All network control devices (i.e., Wireless Access Point or Firewall) must not be housed in a common area. See above examples of common areas.

1.13 Data Backup

Automated data backup procedures must be implemented and must meet all requirements documented below. All equipment or media that store or use State Farm data in any capacity must be backed up. Data Base Application logs must be backed up. Backup software provided by Symantec must be used.

1.13.1 Frequency

A full backup of the entire physical hard disk must be performed every week. Incremental backups must be performed every night.

1.13.2 Storage Location

Backups must be stored on removable electronic media. The backup must be stored away from the original device and in a separate, secured location, (e.g., an office safe, locked box, locked cabinet or similar storage in a different area).

Backups must be protected so that access is restricted to only authorized individuals.

1.13.3 Retention

Each full backup must be kept as a separate copy on different electronic media for at least 8 weeks.

Each unit must contain the full backup and the six following incremental backups (example: Sunday's full backup is stored with Monday through Saturday's incremental backups as one archived unit).

1.13.4 Encryption

All electronic media that contains State Farm data must use encryption as a means of protecting the State Farm data. Symmetric key must be a minimum of 256 bits. A backup of the key must be stored away from the original device and in a separate, secured location. This location must be a room separate from the backup and non-State Farm equipment, media and software where the backup originated. The key cannot be stored on a floppy disk.

Keys must be protected so that access is restricted to only authorized individuals.

A proprietary encryption algorithm cannot be used to encrypt the backups.

An NIST-approved encryption algorithm must be used. The following Web site defines the NIST-approved encryption algorithms: <http://csrc.nist.gov/CryptoToolkit/tkencryption.html>

1.13.5 Media

The following electronic media are acceptable and must only be used for backup: tape, DVD, and external hard drive used specifically for backups.

1.14 Whole Disk Encryption

All non-State Farm equipment, media and software that contain State Farm data must use a whole disk encryption solution that meets the following requirements:

1.14.1 Encryption

The whole disk encryption solution can leverage either an asymmetric or symmetric key, as long as the key strength meets the following requirements:

- Asymmetric key must be a minimum of 1024k.
- Symmetric key must be a minimum of 256 bits.
- A backup of the key must be stored away from the original equipment or media and in a separate, secured location. The key cannot be stored on a floppy disk.
- Keys cannot be stored with a third-party vendor.
- Keys must be protected so that access is restricted to only authorized individuals.
- A proprietary encryption algorithm cannot be used to encrypt the backups.
- An NIST-approved encryption algorithm must be used. The following Web site defines the NIST-approved encryption algorithms:
<http://csrc.nist.gov/CryptoToolkit/tkencryption.html>
- The hard disk encryption product used must have achieved the BITS Tested Mark certification: http://www.bitsinfo.org/c_bits_tested_mark.html

1.15 Data Disposal/Hardware Repair

Before returning, deleting or decommissioning your non-State Farm equipment, media and software that, at any point in time, contained State Farm data, you must contact Chuck Hanan for instructions.

Before deleting any State Farm Data from your non State Farm Equipment, Media and Software, please contact Chuck Hanan for instructions.

All repairs must occur onsite.

1.16 Procedures

1.16.1 Agent Team Member Exit Procedures

When an agent team member discontinues his or her employment relationship with the agent, the following must occur:

- The wireless encryption key must be changed.
- Their user account(s) must be removed from all workstations/laptops/servers, according to the user access inventory.
- Administrative passwords that the exiting employee has knowledge of must be changed.
- Exiting agent team member must have all accesses to equipment, media and software that contain State Farm data removed.

1.16.2 Inventory

An inventory must be conducted on all non-State Farm equipment, media and software that contain State Farm data. The inventory must include the following information:

- Manufacturer
- Model
- Serial

For equipment, a list of users that have access and/or accounts established must be recorded and maintained. This inventory of user accesses must also articulate who has knowledge of what administrative passwords. However, passwords should not be contained in the inventory.

This inventory must be protected so that access is restricted to only authorized individuals.

1.16.3 Lost or Stolen Non-State Farm Equipment, Media and Software

If non-State Farm equipment, media and software that contains State Farm data is thought to be lost or stolen, a full inventory must be conducted and the event must be reported to your AFE, and you must complete an Information Security Review Request (ISRR).

In addition, if non-State Farm equipment, media and software that contains State Farm data is thought to be stolen, a police report must be filed.

1.16.4 Password Management

Wireless encryption key must be changed every 90 days in accordance with password policies.

Hardware Firewall password must be changed every 90 days in accordance with password policies.

WAP password must be changed every 90 days in accordance with password policies.

1.16.5 Document Shredding

All printed documents containing State Farm data related to this environment must be cross-cut shredded when disposed.

1.17 E-mail Usage

Outbound e-mail usage is allowed.

Incoming e-mail increases the risk a computer will be infected with viruses, spyware and malevolent software.

E-mail-borne threats can infect an environment, bypass the controls and endanger agent applications and State Farm data. Incoming e-mail and Web browsing are key ways others use to infect your computer, steal your information, monitor your activities and use you to infect others. Incoming e-mail ranks high as a carrier of viruses, spam and phishing threats and the agent should avoid allowing incoming e-mail if possible. If an agent chooses to allow incoming e-mail, their anti-virus and anti-spyware software must be configured to examine each incoming e-mail at a high level of scrutiny and eliminate any e-mail-borne threat. The agent should also take a defensive approach to all incoming e-mail (not opening e-mail without knowing the sender, immediately deleting spam e-mails without opening, never linking to Web sites provided within e-mails, etc. . .).

Auto preview functionality must be disabled.

E-mail account used must be POP3 secured when technically feasible.

Registered representatives of SFVPMC are prohibited from sending securities related text or instant messages and from sending e-mails through their own non-member e-email address or other third party/non-State Farm issued systems or while in chat rooms or social networking sites.

1.18 Vendors

Agents may engage the services of vendors as outlined in other sections of this Exhibit. However, all vendors must be approved by Corporate Agency per agent per service. All vendors performing services for an agent must have a contract. For the purpose of this agreement, the contract between the agent and vendor may require State Farm Mutual to be an intended beneficiary. There may also be additional items that must be included in the contract between the agent and the vendor, such as the right to audit or perform system vulnerability tests on the vendor.

Please contact Chuck Hanan for current contract language which must be included in the contract between the agent and the approved vendor.