SAMPLE – Privacy Policy for Agencies

Purpose

The purpose of security and privacy standards are to protect all sensitive and confidential information entrusted to and created by {Agency Name}. {Agency Name} respects the privacy of all customers by finding the balance between the privacy interests of the customer and individuals who have a legitimate business need to access, use, and share information as legally permitted.

Privacy Statement

{Agency Name} values and respects the customers and their commitment to them is to put privacy and security standards in the forefront of business operations. It is essential customers, potential customers, associates, and other stakeholders trust sensitive information given to {Agency Name} will be handled with integrity and discretion. Therefore, such information should only be shared with those who have a business need for it. {Agency Name} is responsible for being compliant with carrier policies and regulatory requirements regarding the protection, collection, destruction, use, and release of such information.

Confidential and Sensitive Customer Information

Confidential and sensitive customer information includes, but is not limited to:

- Driver's license number
- Social Security number
- Name with address
- Medical information
- Credit card number
- Bank account number
- Policy or account number
- Financial information
- Commissions information or payment structure
- User IDs, PINs and passwords
- Audit reports
- Confidential internal communications

Medical Information

Medical information is defined as an individual's medical history, diagnosis, mental or physical condition, or medical treatment by a health care professional. {Agency Name} is responsible for protecting all personal health information per HIPAA and privacy regulations. {Agency Name} must not disclose any health information except to those who need the information to perform their core job function.

Create a Secure Work Environment

{Agency Name} will always activate the computer's screen saver function when they are away from the computer. This is accomplished by pressing **Ctrl+Alt+Delete**.

Sensitive and confidential information will be **disposed of in the shred bin, not the trash can, or secured in a desk prior to leaving for the night.**

Passwords

All passwords will be secured. Passwords will not be left on desks, sticky notes, under keyboards, or any other hiding place. No one should ask to obtain or change a user ID/password other than the person associated with the user ID. Exceptions to this include business need, extenuating circumstances, or legal situations.

Leaving a Voicemail

Sensitive information such as medical, health, or financial information will not be left on an answering machine or on voicemail.

Faxing Information

Faxes should only be sent if there is a business relationship and/or all parties have consented as required. Any time documents are faxed, Social Security numbers will be deleted or the first five digits replaced with X's. Exceptions are allowed only when a state or federal law requires the Social Security number to be on the document.

All documents left on the fax machine at the end of the night will be shred.

Email

Secure email should be used when transmitting sensitive and confidential information.

Privacy in the Workplace

{Agency Name} reserves the right to inspect all offices, workstations, desks, file cabinets, and storage areas to confirm sensitive information is properly stored. {Agency Name} reserves the right to monitor, access, and disclose all information on any devices used for business purposes with or without prior notice. This includes electronic messages and internet usage utilizing {Agency Name} owned property and/or systems.

Securing Information on Portable Devices

Anyone who have access to agency emails on a cell phone are responsible for the physical security of these devices. These devices will be secured by requiring a user id and password or a security code/PIN to unlock the device.

Lost Equipment

To ensure client information is not compromised, it's critical all lost or stolen equipment including laptops, cell phones or any other device containing customer information is **reported immediately** to {Agent Name}.

Data Breaches

{Agency Name} is responsible for protecting customer information. It's important to report any suspected data breach immediately. Data breaches can happen easily if extra caution is not used. It's important to be diligent when handling sensitive information and use secure email when required.

Reporting Breaches

Sensitive information believed to have been obtained by an unauthorized person must be reported to {Agent Name}. {Agency Name} will follow all applicable notification laws and HIPAA requirements concerning breach of sensitive information.

Confirmation of Commitment

{Agency Name} prides itself on being an agency built on trust and ethical business practices. Making sure all sensitive information is handled with integrity is of the highest priority. Each person plays a vital role in creating a culture that includes security and privacy diligence.

_____ / / ____ _____ / / ____

Agent Signature & Date Employee Signature & Date