POLICY
Information Privacy: Acceptable Use of Confidential Information

BOARD, HOME OFFICE AND SALES ASSOCIATES

1. DESCRIPTION
Individuals entrust WoodmenLife with Nonpublic Personal Information to allow us to Market or provide products and services or as a part of the employment or contracting process. In addition, Associates are provided Nonpublic Business Information in order to do our jobs. It is our obligation to protect the privacy and confidentiality of all Confidential Information. All such Confidential Information must, at all times, be secured and safeguarded. All Confidential Information may be accessed, Used and Disclosed only in accordance with WoodmenLife policy, procedures, standards and guidelines.

2. PURPOSE
WoodmenLife is committed to conducting its business in an ethical manner consistent with its Mission, Vision and Values. Keeping Confidential Information, secure and restricting the access, Use and Disclosure of such information for appropriate purposes only is an absolute requirement.

3. SCOPE
As a condition of continued appointment, employment or contracting, all Associates must abide by the provisions of this policy. We recognize that no policy can cover every circumstance or situation that will arise. In cases of doubt, Associates should seek the advice of the Privacy Official or the Legal Department.

4. POLICY AND PROCEDURE
A. Associates shall, at all times, safeguard the confidentiality, privacy, integrity and security of all Confidential Information.

B. Associates may only access and use Confidential Information in conjunction with their assigned positions or contract responsibilities.

1. Such access and Use shall be on a "Need to Know" basis and in strict accordance with WoodmenLife policies, procedures, standards and guidelines. Associates may not access, copy, reproduce or use Confidential Information in any other manner, or for any other reason.

2. Associates may only discuss or share Confidential Information with other Associates who have a Need to Know as dictated by their positions or contract responsibilities.

C. Associates may not Disclose Confidential Information to anyone except in strict accordance with WoodmenLife policies, procedures, standards and guidelines.

1. Associates are required to verify the identity and the authority of a person requesting Confidential Information from WoodmenLife in accordance with WoodmenLife's policies, procedures, standards and guidelines.

2. Sales Associates may not Disclose Nonpublic Personal Information except as follows:

a) To the certificate owner (or applicant). If the certificate owner/applicant is not the insured, only information related to the certificate or application can be disclosed.

b) To the insured. If the insured is not the certificate owner, only information related to the insured can be disclosed.

c) To the beneficiary/claimant, as necessary to process a claim.

d) To a payor, but only information related to billing transactions.

e) To paramedics or health care providers to schedule required underwriting tests or exams.

f) As permitted by the Advantage Contract.

g) To any other person or entity with prior approval of the Home Office.

3. Home Office Associates may not Disclose Nonpublic Personal Information except as follows:

a) To the individual to whom the information relates.

b) To the certificate owner or applicant.

c) To a person acting in a fiduciary or representative capacity on behalf of the individual (e.g. lawyer, CPA, tax accountant, guardian, attorney-in-fact, or trustee).

d) To a certificate payor, but only such certificate information relating to billing, processing, clearing, transferring, reconciling or collection of amounts charged or otherwise paid.

e) To a beneficiary or claimant for purposes of claim processing only.

f) To a funeral home for purposes of claim processing or if the funeral home possesses a contract right (e.g. assignment).

g) If the individual authorizes release of such information in writing (examples include authorization to release value information to a social services agency or to a funeral home in a situation other than as described above).

h) To a Sales Associate with a Need to Know.

i) To Third Party Service Providers who provide services to and on behalf of WoodmenLife with a Need to Know.

j) As otherwise allowed by law. Examples include: as necessary and required to underwrite or for certificate placement, certificate service functions, claims adjudication or processing, in connection with billing, settlement, administration of consumer disputes and inquiries, merger, transfer or exchange of all or part of a business or operating unit, transferring, reconciling or collection of amounts paid, to investigate or report fraud, misrepresentation or criminal activity, institutional risk control including security, reinsurance, auditing, to agencies that are rating WoodmenLife, persons who are assessing WoodmenLife's compliance with industry standards, to WoodmenLife's attorneys, accountants and auditors, law enforcement agencies, state insurance authorities and other regulators, pursuant to governmental reporting, to comply with federal, state or local law, to respond to the legal process.

4. WoodmenLife has agreements with Third Party Service Providers who use Confidential Information in the provision of services to and on behalf of WoodmenLife. These agreements include provisions that require the Third Party Service Provider to safeguard Confidential Information. If an Associate has any information regarding the misuse, unauthorized Disclosure, alteration or improper destruction of Confidential Information by a Third Party Service Provider, such information must be promptly reported to the Privacy Official or the Legal Department.

D. Associates must limit their access, Use and Disclosure of Confidential Information to that which is "Minimally Necessary."

1. For routine Disclosures for insurance functions, the Minimum Necessary information to be disclosed shall be the information customarily required within the industry to accomplish the purpose of the Use or Disclosure.

2. For non-routine Disclosures, the Minimum Necessary information must be identified by the Legal Department.

E. Limits on the reuse and redisclosure of Nonpublic Personal Information

1. WoodmenLife's Uses or Disclosures of Information received from a nonaffiliated financial institution such as a bank, securities firm, other insurance company, broker or agent for processing, servicing or administering a WoodmenLife certificate/service are limited to the following purposes:

a) WoodmenLife may Disclose the Information to affiliates of the financial institution from which WoodmenLife received the information;

b) One affiliate of WoodmenLife may Disclose the Information (except as prohibited by the Fair Credit Reporting Act or other law) to another affiliate of WoodmenLife but that affiliate may only Use or Disclose the Information to the extent permitted by the affiliate that was the original recipient of the Information; and

c) WoodmenLife may use or Disclose the Information in the ordinary course of business carry out the activities for which WoodmenLife received the information.

F. Restrictions on the Sharing of a WoodmenLife Certificate Number for Marketing Purposes

1. WoodmenLife shall use the following guidelines for restricting the sharing of certificate numbers with nonaffiliated third parties for marketing purposes.

2. WoodmenLife will not, directly or through an affiliate, Disclose, other than to a consumer reporting agency, a certificate number to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to one of our customers. There are certain exceptions to these general guidelines/standards.

3. Exceptions:

    a) WoodmenLife may Disclose a customer's certificate number to a Third Party Service Provider in order for the third party to provide marketing services to WoodmenLife. However, the service provider may not initiate changes to the certificate and they must agree to only use the information for WoodmenLife's marketing purposes.

    b) WoodmenLife may Disclose a customer's certificate number to a Sales Associate in order for the Sales Associate to perform marketing services for WoodmenLife's products or services.

    c) WoodmenLife may Disclose a customer's certificate number to a nonaffiliated third party ("vendor") in a fraternal program or to an affinity or similar program as long as we have previously identified the vendor to our customers when they entered the program.

G. Associates shall promptly report any suspected violation of the law or this policy (i.e., unauthorized Disclosure, misuse, alteration or improper destruction of Confidential Information. An Associate does not have to be sure that something is against the law or WoodmenLife policies before reporting it. Associates need only report first-hand information; this means that the Associate saw the action or directly knows about it. It is not usually necessary or helpful to report rumors or second-hand information. Associates may also report any general concerns or complaints regarding WoodmenLife's privacy policies or compliance with the terms of such policies. Reports may be made by writing or talking to a supervisor, division/department head, the Privacy Official, or the Legal Department. When reporting concerns or suspected violations, WoodmenLife encourages Associates to identify themselves, since this makes full investigation of concerns more successful. However, an anonymous report will also be accepted. WoodmenLife will not retaliate against any Associate who, in good faith, reports a suspected violation.

H. Upon termination of employment or contract with WoodmenLife, Associates shall return all originals, copies, reproductions and summaries of any Confidential Information. Further, upon termination, Associates shall continue to protect the confidentiality and privacy of all Confidential Information.

    1. Such obligation to protect the privacy and confidentiality of Nonpublic Business Information shall not extend to any information which:

        a) Becomes publicly available without the Associate's breach of any confidentiality obligation.

b) Becomes known to the Associate from an independent third party.

c) Is independently developed by the Associate.

2. The obligation to protect the privacy and confidentiality of Nonpublic Personal Information shall continue but not extend to any information which:

a) Becomes publicly available without the Associate's breach of any Nonpublic Personal Information.

b) Cannot be used to identify the subject of the information (e.g. through aggregation or deidentification).

I. Concerning Individual Rights

1. WoodmenLife will provide certain rights required by law for customers and former customers. In order to assure that these rights are not compromised, all Associates must be aware of these rights and the following duties and responsibilities:

a) Access to Nonpublic Personal Information. Customers have the right to access, inspect or receive a copy of all Personal Information that WoodmenLife retains on their behalf. If a customer requests access to their information, other than routine servicing requests, refer the person to Customer Service. If an Associate receives a written WoodmenLife form requesting access, the form must be promptly forwarded to Core Operations Compliance and Customer Support.

b) Amendments to Nonpublic Personal Information. Customers have the right to request WoodmenLife to make amendments to their Personal Information. If a customer requests amendment to their information, refer the person to Core Operations Compliance and Customer Support. If you receive a written WoodmenLife form requesting amendment, the form must be promptly forwarded to Core Operations Compliance and Customer Support.

c) Accounting for Disclosures (only Health Plans and certain states for all lines). Customers have the right to request an accounting of Disclosures we make of their Personal Information. If a customer requests an accounting, refer the person to Core Operations Compliance and Customer Support. If you receive a written WoodmenLife form requesting

an accounting, the form must be promptly forwarded to Core Operations Compliance and Customer Support.

d) Restriction (Only Health Plans): If a customer requests (orally or in writing) a restriction on Uses and Disclosures of their Nonpublic Personal Information, promptly forward the request to the Core Operations Compliance and Customer Support.

e) Confidential Communications (Only Health Plans): If a customer requests to receive communications from WoodmenLife by alternative means or at alternative locations, refer the person to Customer Service. If you receive a written WoodmenLife form requesting communications by alternative means or at alternative locations, the form must be promptly forwarded to Core Operations Compliance and Customer Support.

f) Complaints. Customers have the right to file a complaint with WoodmenLife if they believe their privacy rights have been violated. If a customer requests to file a complaint, refer the person to the Privacy Official or the Legal Department. If you receive a written WoodmenLife complaint form, the form must be promptly forwarded to the Privacy Official or the Legal Department.

g) No Retaliation.

(1) No Associate may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any person who exercises their rights. Such rights include filing a complaint to WoodmenLife, the Secretary of the U.S. Department of Health and Human Services (Health Plans only) or a state insurance regulator or testifying, assisting or participating in an investigation, compliance review, proceeding, or hearing under federal law on privacy.

(2) Health Plans Only. WoodmenLife and any Associate of WoodmenLife may not retaliate against any person for opposing any act or practice made unlawful by the federal privacy law, provided:

a) The individual or person has a good faith belief that the practice opposed is unlawful.

b) The manner of the opposition is reasonable.

c) Opposing the act or practice does not involve a Disclosure of protected health information in violation of federal law.

5. DISCIPLINARY ACTION

Violation of this policy is subject to disciplinary action up to and including termination. Misuse or misappropriation of Confidential Information may be reported to law enforcement officials or regulatory entities and may result in civil or criminal penalties.

6. DEFINITIONS

See Addendum A. Information Privacy and Information Security Policies Glossary.

Addendum A

Information Privacy and Information Security Policies Glossary

Policy Content

The following reference tables are provided to help identify applicable policy(ies) to reference based on need:

Information Privacy Policies:

Policy/Standard	Content
Information Privacy: Acceptable Use of Confidential Information	Acceptable access, Use and Disclosure of Confidential Information
Information Privacy: Internal Use of Protected Health Information	Access, Use and Disclosure of Protected Health Information
Information Privacy and Security: Education and Training	Training Requirements relating to protection of Confidential Information
Privacy and Security Incident Reporting	Privacy and Security incident reporting and privacy/security incident response requirements.
Third Party Service Provider's Known or Suspected Security Incident or Improper Access, Use, Disclosure, Alteration or Destruction of WoodmenLife's Confidential Information Standards	To provide reporting procedures to the Chief Security Official and the Privacy Official of a third party service provider's improper access, use, disclosure, alteration, destruction of confidential information.

Information Security Policies:

Policy/Standard	Content
Acceptable Use (Policy only)	Acceptable and unacceptable use of Information Resources
Anti-Malware	Ensure all Assets are protected by Anti Malware systems
Application Development	Secure Software Development Life Cycle (SDLC) expectations

Policy/Standard	Content
Asset Configuration	Securing and maintaining Assets utilizing recommended hardening specifications
Asset Management	Ensure Assets are identified appropriately, and the proper security controls are utilized
Change Control	Ensure resource changes are documented, authorized, and performed in a controlled manner
Cloud Computing Services Acceptable Use (Policy only)	Ensure Confidential Information is stored and managed properly, and provider contracts are comprehensive
Contingency Planning	The development, maintenance, and testing of contingency plans
Data Classification and Handling (Policy only)	Data Classification, protection and handling expectations
Disposal (Policy only)	Ensure the proper disposal, destruction or reuse of Information Resources
Encryption	Implementation of proper encryption controls
Identity, Access, and Account Management	Protecting WoodmenLife assets through identity, access and account management
Instant Messaging	Approved methods for utilizing IM (aka Chat) tools
Incident Response (Policy only)	Security incident reporting and security incident response requirements
Stewardship (Policy only)	To provide protecting security and privacy of all information.
Maintenance and Patching	Maintenance/patching expectations of all Information Resources
Media Protection	Outline media protection requirements for Users
Mobile Device Acceptable Use (Policy only)	Acceptable and unacceptable use of mobile devices
Monitoring and Auditing	Ensure appropriate monitoring and auditing of all Information Resources
Network Connection	Ensure a secure Network and all connections to that Network
Physical and Building Security Policy (Policy only)	Required physical safeguards to protect WoodmenLife's facilities
Remote Access	Defines secure remote access requirements
Risk Management	Risk management program expectations
Security of Confidential Information (Policy only)	Required physical and technical safeguards to protect Confidential Information
Third Party Management	Ensure 3rd Party Providers are contractually bound to protect Confidential Information

DEFINED TERMS

The following definitions apply to all Information Privacy and Information Security Policies and Standards. Any variations to definitions will be noted within the individual Policies and/or associated Standards.

Air-gapped: A network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. The name arises from the technique of creating a network that is physically separated (with a conceptual air gap) from all other networks.

Asset(s): Any tangible Information Resource that can be used to create, maintain, store, transport, access, process, or modify Confidential Information.

Associate(s): Those persons considered "Associates" include: all Home Office, Regional Office Administrative, Community Outreach, and Sales associates, WoodmenLife's group health plan administrative workforce, and those persons employed via leasing arrangements through WoodmenLife, except where a conflicting policy exists in any WoodmenLife subsidiary company.

Board: Members of the National Board of Directors.

Cloud Services (aka "Cloud Computing): The utilization of Internet-based servers or information technology hosting that is not managed by WoodmenLife for Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), social networking applications, file-storage services, and other similar services. Key features are ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction.

Confidential Information: Any information that is marked or designated as confidential or attorney client privileged or that reasonably should be understood to be confidential given the nature of the information and the circumstances of Disclosure. Confidential Information shall include, without limitation, i) Nonpublic Business Information, ii) Nonpublic Personal Information, and iii) Protected Health Information (PHI).

Contractor: An individual or entity contracted to perform services for WoodmenLife.

Data: Factual information used as a basis for reasoning, discussion, or calculation in both physical and electronic forms.

Data Classification: A framework used to describe and quantify the amount of protection required for Data.

Data Owner: Associate (usually within divisional or department management) with authority for specified Data and responsibility for establishing controls for its generation, collection, security, dissemination and disposal. Data Owner is responsible for:

a. Classifying the Data;
b. Establishing the rules for appropriate use of Data;
c. Deciding who has access to Data and what type of access they get; and
d. Establishing retention rules and oversees the destruction of Data when no longer needed.

Disclosure, Disclose or Disclosed: The release, transfer, provision of access to or divulging in any other manner to persons not employed by or working within WoodmenLife.

Electronic Devices: WoodmenLife owned and/or managed devices including PCs, Servers, Laptops, Smartphones, and Tablet computers.

Encryption: The transformation of Data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

Encryption Key Management: The procedures for managing keys used in the Encryption process. This includes dealing with the generation, exchange, storage, use, destruction and replacement of keys.

Health Plan: Long term care, daily hospital supplement and Medicare Supplement certificates or any other Health Plan WoodmenLife may issue or renew, as that term is defined by federal law.

Information Resources: Data and anything that can be used to store, transport, or manipulate data. Such resources include data, computer Workstations, software, telephone systems, e-mail, Internet, internal networks, mainframes, and servers.

Instant Messaging: An Internet protocol (IP)–based application that provides communication between people using a variety of different device types. The most familiar today includes Jabber, M365 Chat, Gmail Messenger and Facebook Messenger.

Internal Email: Emails that are sent through WoodmenLife's virtual private network; both the sender and the recipient have a "WoodmenLife.org" email address.

Least Privilege: Giving a User ID or System Account ID only those privileges which are essential to perform its intended function.

Malware: Software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, and spyware.

Management Accounts: An administrator account that is included by the manufacturer of an Asset intended to facilitate setup and management of the Asset. These usually have the same account name and a default password that is well known.

Market/Marketing: To make a communication about a product or service that encourages recipients to purchase or use the product or service.

Media: Any technology (including devices and materials) used to store Data. Some examples of Media are external hard drives, removable drives (such as Zip disks), CD-ROM or CD-R discs, DVDs, flash memory, and USB drives.

Minimum Necessary or Minimally Necessary: Confidential Information that is reasonably necessary to accomplish the intended purpose of the access, use or disclosure.

Mobile Code: Mobile code is any program, application, or content capable of movement while embedded in an email, document or website.

Mobile Device: Any portable electronic device having the capability to access, store, record, and/or transmit text messages, images/video, or audio data. Examples of such devices include, but are not limited to: cellular phones, smartphones, iPads, tablets, and smart watches.

Named Individuals: Associates who are identified and documented as authorized to access Restricted Use Information.

Need To Know: Necessary in order to provide products or services or to fulfill position or contract responsibilities.

Network: All the Assets required to connect Information Resource together to enable the sharing of Data. Some examples of these Assets are Firewalls, Switches, Routers, Wireless Infrastructure Devices, and Internet connections.

Non-Health Plan: Life insurance, disability, annuity or cancer products or any other plan that is not a Health Plan as that term is defined by federal law.

Non-Health Plan Function: Any WoodmenLife activity related to the marketing, issuance, servicing or administration of any Non-Health Plan, e.g., life insurance, annuity, cancer or disability products.

Nonpublic Business Information: Nonpublic information of WoodmenLife that is of value to WoodmenLife or, the tampering with which, or unauthorized Disclosure, access or Use of which, could cause a material adverse impact to the business, operations or security of WoodmenLife. Business Information includes, but is not limited to: WoodmenLife policies and procedures; System requirements; Operating environments; System and subsystem architecture diagrams; Dataflow diagrams; Unpublished financial data and marketing campaign materials; and WoodmenLife strategy documents.

Nonpublic Personal Information: Nonpublic information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular living or deceased person or household.

Nonpublic Personal Information includes, but is not limited to:

A. Personally identifiable information that an individual provides or WoodmenLife otherwise obtains and maintains in connection with a product or service between WoodmenLife and the individual;
B. Contact information - such as name, address, phone number, email address, and account name;
C. Health information - such as any past, current, or potential future information about physical, mental, or behavioral health conditions;
D. Financial and insurance information - such as financial information provided on an insurance application, certificate account balance or benefit information, certificate payment history, certificate number, claim number, information from a consumer report, bank account or credit account number, salary information, commission statements, certificate account tax information;
E. Medical information - such as past, current, or future information about health insurance information, claims information, treatment information, treatment locations, and payment information;
F. Government identifiers – such as driver’s license number, social security number, or passport number;
G. Biometric information - such as fingerprints and exercise data;
H. Information that would enable access to an account - such as usernames, passwords, security codes, and access codes;
I. Online identifiers - such as IP address, device identifiers, and device attributes;
J. Other identifiers - such as signature, physical characteristics, age, sex, race, ethnicity, and gender;

K. Audio, electronic, thermal, or similar information - such as call recordings, photographs, video surveillance;
L. Employment information - such as occupation, employment history, and professional references;
M. Inferences drawn about an individual;
N. An individual's relationship to the company (e.g. customer, employee or business contact);
O. Any list, description or grouping of individuals derived using personally identifiable financial information that is not publicly available.

Outgoing Email: Emails that are sent over an open network (Internet); Emails that are being sent from a WoodmenLife network to a non-WoodmenLife email address.

Personal Electronic Devices: Any electronic device that is not owned or supplied by WoodmenLife having the capability to access, store, record, and/or transmit text messages, images/video, or audio data. Examples of such devices include, but are not limited to: laptops, workstations, cellular phones, smartphones, iPads, tablets, smart watches and printers.

Personal Workstation Peripheral Devices: Any electronic device that is not owned or supplied by WoodmenLife having the capability to connect directly or through Bluetooth to a WoodmenLife owned laptop or workstation while not having the ability to store or reproduce Data to only include keyboards, mice, headsets with or without microphones, webcams, microphones and monitors.

PINs: Personal Identification Numbers: A number or code individuals use to provide verification of identity. It is like a password except they are all numbers. PINs are commonly used for proving identity for phone systems.

Plan Workforce: Associates with access to WoodmenLife's group health plans.

Privileged Account: Any authorized user account or service account that can be used to:

A. Perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change, or remove other accounts, or make configuration changes to operating systems or applications to make them more or less secure; or
B. Affect a material change to the technical or business operations of the covered entity to include but not limited to Active Directory Administrators, Azure Active Directory Administrators, System Administrators, Security Administrators and Application Administrators.

Proprietary Information: See Nonpublic Business Information

Protected Health Information (PHI): Information of living or deceased persons which WoodmenLife receives, maintains, or creates in connection with a Health Plan that:

1. Identifies or could be used to identify an individual who is the subject of the information;
2. Relates to the past, present or future physical, mental or behavioral health or condition of an individual;
3. Relates to the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual.

A. For purposes of this policy examples of PHI include:

1. social security number;

2. telephone/fax numbers, electronic email or home addresses including street, city, county, or zip code;

3. dates directly related to a customer/insured, i.e., birth date, health care facility admission and discharge dates, dates of service, dates of claims, or date of death;

4. certificate number, claim benefit information, certificate benefits, status of a certificate, or a type of certificate;

5. medical records, numbers or clinical health information/records; and

6. premium payment or claim payment.

Public Information: Any information that is lawfully made available to the general public from: federal, state, or local government records, widely distributed media, or Disclosures to the general public that are required to be made by federal, state or local laws. Public Information includes, but is not limited to, press releases, published product marketing information, blank insurance forms, blank application and request forms, general information that is openly shared, any information displayed on a website deemed available to the public.

Push Data Updates: An application or service that opens a channel to a PC or mobile device such that the User does not have to actively ask for data updates, but the information is automatically “pushed” to the PC or mobile device.

Sanctioned Software: Software that has been tested and approved for use on WoodmenLife owned mobile devices by the Business Technology Division and Security Administration Department.

Sanitization: Is the process of deliberately, permanently, and irreversibly removing or destroying the data stored on an Asset or Media. An Asset or Media that has been sanitized has no usable residual data and even advanced forensic tools should not ever be able recover erased data.

Security Incident: any occurrence or event that results in damage, loss or destruction of Information Resources or, is a weakness, which may not necessarily immediately result in damage, but could result in security being compromised.

Split Tunnel Connection: A type network connection that allows an Asset to connect to multiple different networks simultaneously to allow different types of traffic to be sent to different destinations and possibly bypass security controls.

Strong Password: Passwords must meet the criteria established by WoodmenLife as defined in the Information Security Acceptable Use Policy.

System Account ID: A unique sequence of characters used to identify a system account used to access WoodmenLife Information Resources.

Third Party Service Provider: A person or entity that is not an affiliate of WoodmenLife, that provides services to WoodmenLife and that maintains, processes, or otherwise is permitted access to Confidential Information through its provision of services to WoodmenLife.

Use or Used: The accessing, sharing, employment, application, utilization, examination or analysis of information by any person working within WoodmenLife or by any Sales Associate.

User: An approved person accessing WoodmenLife Information Resources.

User ID: A unique sequence of characters used to identify a person and allow access to WoodmenLife Information Resources.

Virus: A software program which replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network. The symptoms of Virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

VPN: Virtual Private Network.

Vulnerability: A weakness in the system, application, infrastructure, or control or a design flaw that can be exploited to violate system integrity.

Wireless Network: A computer network where there is no physical wired connections between Assets. The network is connected by radio waves and/or microwaves to maintain communications.

WoodmenLife: Woodmen of the World Life Insurance Society and any subsidiary companies or affiliates.

Workstation: Personal Computers (PC's), Portable Computers (Laptops), Computer Terminals, Hand-Held Computers, Tablet PC's, etc.