LONE WOLF SOFTWARE, INC.
6097 North 57th Drive · Glendale, Arizona 85301

www.TimeWolf.com
Sales@LoneWolfSoftware.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Lone Wolf Software, Inc. Security Policy

Introduction

The purpose of this document is to define the Lone Wolf Software, Inc. Data Security Policy. Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data security is necessary in today's environment because data processing represents a concentration of valuable assets in the form of information, equipment, and personnel. Dependence on information systems creates a unique vulnerability for our organization. Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize our ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data; violate business contracts, trade secrets, and customer privacy; or reduce credibility and reputation with its customers, shareholders and partners.

The main objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all of our and all customer data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate or that are operated by our agents.

This policy defines the Lone Wolf Software, Inc. overall security and risk control objectives that we endorse. The premise for the policy can be stated as: “Other than data defined as public, which is accessible to all identified and authenticated users, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorized entities.” This embodies the principle of least privilege. This document forms part of your conditions of employment for employees, a part of the contractual agreement for vendors, suppliers, and third party processor or agents, hereafter referred to as vendors. All parties must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

Scope of the Policy

This policy applies to all Lone Wolf Software, Inc. and customer data assets that exist in any Lone Wolf Software, Inc. processing environment, on any media during any part if its life cycle. The following entities or users are covered by this policy: Full or part-time employees of Lone Wolf Software, Inc. who have access to Lone Wolf Software, Inc. or customer data, Lone Wolf Software, Inc. vendors or processors who have access to Lone Wolf Software, Inc. or customer data, and Other persons, entities, or organizations that have access to Lone Wolf Software, Inc. or customer data.

LONE WOLF SOFTWARE, INC.
6097 North 57th Drive · Glendale, Arizona 85301

www.TimeWolf.com
Sales@LoneWolfSoftware.com
Toll Free: (800) 473-9457
Fax: (623) 930-0012

Data Life Cycle

The security of data can be understood through the use of a data life cycle. The typical life cycle of data is: generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data. Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

Data Usage

All users that access Lone Wolf Software, Inc. or customer data for use must do so only in conformance to this policy. Uniquely identified, authenticated and authorized users must only access data. Each user must ensure that Lone Wolf Software, Inc. data assets under their direction or control are properly labeled and safeguarded according to their sensitivity, proprietary nature, and criticality. Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

Data Transmission

All users that access Lone Wolf Software, Inc. or customer data to enable its transmission must do so only in conformance to this policy. Where necessary, data transmitted must be secured via cryptographic mechanisms.
This may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the Lone Wolf Software, Inc. policy on the use of cryptography.

Data Storage

All users that are responsible for the secure storage of Lone Wolf Software, Inc. or customer data must do so only in conformance to this policy. Where necessary, data stored must be secured via cryptographic mechanisms. This
may include the use of confidentiality and/or integrity mechanisms. Specific cryptographic mechanisms are noted in the Lone Wolf Software, Inc. policy on the use of cryptography.

Data Disposal

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process. The Data Security organization must develop and implement procedures to ensure the proper disposal of various types of data. These procedures must be made available to all users with access to data that requires special disposal techniques.