LawStudio's Security Model

Protecting Your Data

LawStudio™ | *powered by Veritext*

The LawStudio **Security Model**

Introduction

Information security and privacy are built into the fabric of everything we do at Veritext. Helping to protect the confidentiality and integrity of your data is a core part of our mission. This document provides an overview of the systems controls implemented in LawStudio and all of our security practices. All Veritext facilities and systems are compliant with the highest security standards, including HIPAA and PII.

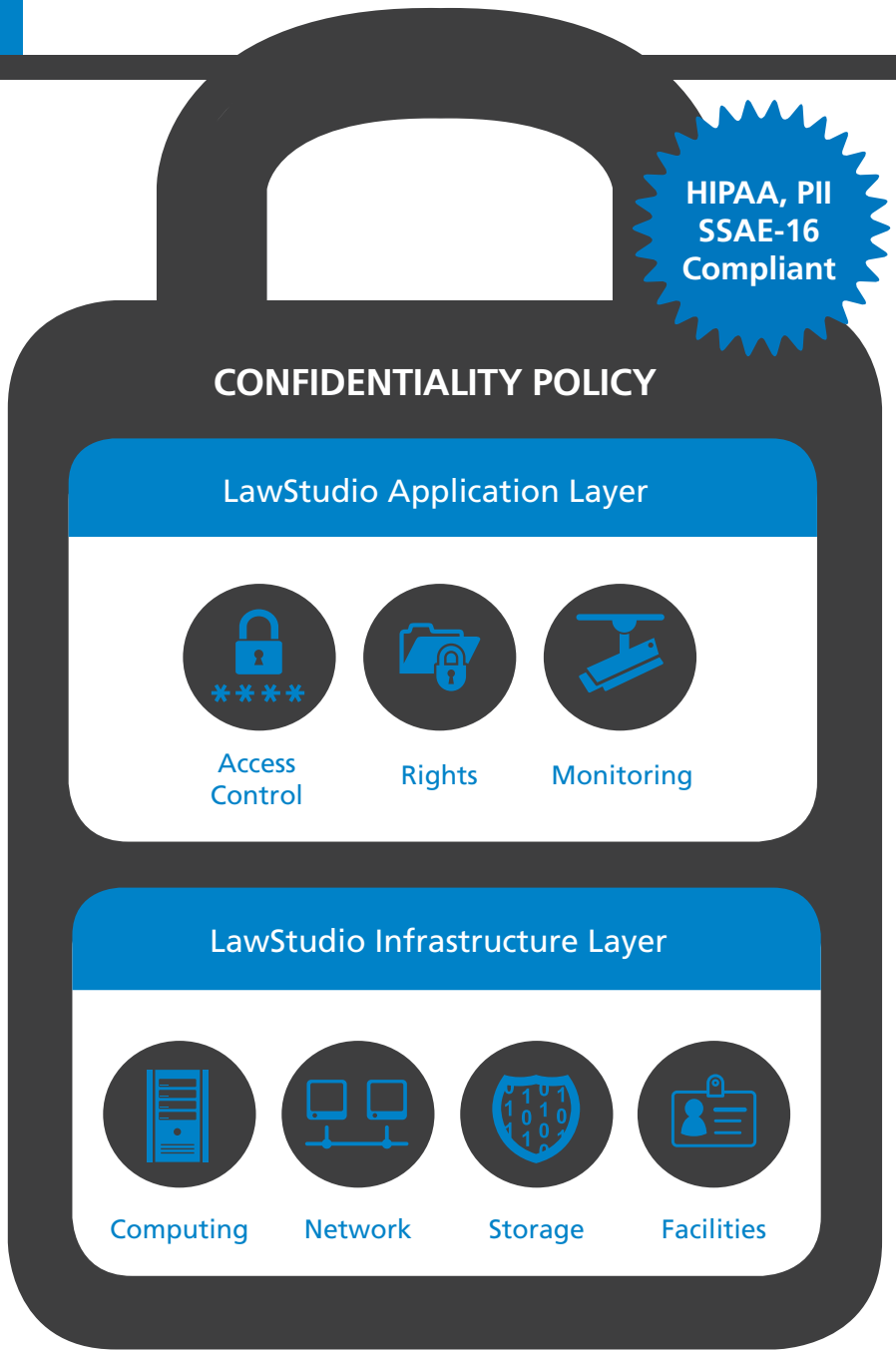
The LawStudio Security Model

Data security in LawStudio is implemented at two layers and ensured from a process perspective by Veritext's company confidentiality policy.

The first is the foundational Infrastructure Layer, wherein data is stored and moved through the computing and storage systems. Here, LawStudio utilizes strong data encryption, both at rest and in transit to protect against unauthorized access to the data without authenticated, auditable privileges.

The second layer is the Application Layer, wherein data is processed and presented to authorized individuals based on privileges determined by the client.

Both of these system implementation layers are supported by our confidentiality policy (in which all Veritext employees are trained to and held to) and prescribes practices designed to ensure protection of your data in the course of developing, maintaining and delivering our products and services. The schematic (right) illustrates this model, and the following sections provide more detail on the security layers and the policy around them.



Security Within the **Infrastructure Layer**

Security Within the Infrastructure Layer

In the Infrastructure Layer, security is built into the ways ***computing*** devices (i.e., servers) are accessed and protected, how the ***network*** allows communication between devices and how it transmits data, how ***storage systems*** protect transient and permanent data as it is stored, and how all of the physical computing, network and storage devices are protected within the ***facilities*** in which they are hosted. While LawStudio leverages Veritext's dedicated technology infrastructure as well as Amazon cloud hosting services, the following implementation of the security policy is maintained throughout the Infrastructure Layer.

Computing security is implemented via best practices for operating system configuration. All computing devices are configured for access only by authorized, auditable administration staff operating under Veritext's confidentiality policy. All servers are protected by the latest virus and malware protection and maintained at the most recent viable security patch level. Client data is not stored at the computer layer, and all data is managed in protected storage subsystems.

Network security is implemented via best practices for external and internal network controls. Within the internal computer and storage network, only identified hosts and application ports are permitted to traverse the network as configured in firewalls and virtual hosting configurations. In addition, for both the external (i.e., connecting with clients via the Internet) and internal network, data is encrypted in transit to ensure that access to data "on the wire" is protected. External client and agent access is always carried via the secure-socket layer (i.e., HTTPS) protocol.

Storage security is implemented for all client files via strong encryption, with access control implemented within the Application Layer (See "Access Control"). Data is encrypted at rest using the AES-256 bit encryption standard.

Facilities security is assured in Veritext's internal hosting environment via a controlled access dedicated cage in a CenturyLink Tier IV, SSAE-16 compliant data center. Subsystems that are hosted in the Amazon Web Services cloud environment are equally protected via Amazon's strong facilities controls. More information on Amazon's strong facilities controls can be found at http://aws.amazon.com/security.

Security Within the **Application Layer**

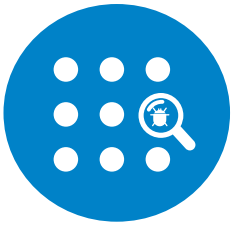
Security Within the Application Layer

In the Application Layer, security is built into the ways ***access*** to data by a client is controlled, the ways that clients can ***manage rights*** to different sets of data, and how access to the application and systems is ***monitored***.

Access Control within LawStudio is implemented both for clients accessing the system, as well as across subsystems and services that make up LawStudio. For clients using LawStudio, usernames and passwords are stored in an encrypted fashion using SHA-256 (SHA-2). User login is required in order to obtain a token for a session, which allows a user to access LawStudio resources for the duration of the session.

Once the user logs in, the session token remains active as long as there is user activity. The token is removed when the user logs out, or if their is no user activity for fifteen minutes. For subsystem communication, LawStudio implements a stateless REST API to integrate systems. A component needs to authenticate the user first with the LawStudio Service before the user can use any of the LawStudio REST services. A component authenticates a user with LawStudio by calling a REST service with the user's login name and password. After successful authentication, a token is returned. This token is passed in all the subsequent REST calls to LawStudio for any operation performed by the component on the user's behalf.

Rights Management within LawStudio is designed to allow the client control over which artifacts (i.e., documents, multimedia objects, etc.) can be accessed by users within the system. In addition, for documents with annotations, a client can specify whether those annotations are publicly available to those who have access to a published copy of the document, or are for the client's internal use only. Training material for LawStudio describes how to set up users and rights. For more information, see: http://help.lawstudio.com/knowledge_base/categories/shared-workspaces. For publishing documents to colleagues outside of LawStudio, a client can provide access to selected documents via a password protected link with time-expiration to provide secure, efficient access to the documents.



Close and rigorous ***Monitoring*** of the LawStudio system ensures that the controls and policies are truly effective and that new and emerging threats do not compromise data security and integrity. Active monitoring includes the use of systems and network tools that alert Veritext staff to unexpected conditions in systems access and utilization, as well as systems and subsystem faults that may indicate an underlying problem. In addition, access audit logging is enabled throughout the system to ensure that potential unauthorized access can be quickly assessed and resolved.

Veritext Confidentiality **Policy & Procedure**

Veritext Confidentiality Policy & Procedure

Underpinning the design, implementation and support for LawStudio is the Veritext Confidentiality Policy. The policy delineates responsibilities around information privacy and security for all employees, as well as general and security-specific management roles. While the policy itself is an internal policy document, the specific scope of the policy includes:

Protection of Data **Integrity & Availability**

Protection of Data Integrity & Availability

Veritext ensures that your data is not only secured for access only to authorized individuals, but also works hard to ensure that it is always available for your access. There are two aspects of data integrity and availability assurance: The first is ***high-availability infrastructure*** and the second is a sound ***recovery*** posture.

For high-availability infrastructure, all client data is stored on resilient, high-performance storage array within hardened Tier IV hosting centers (See "Facilities" in "Infrastructure Layer") High availability is achieved through redundant components (i.e., disk drives, controllers) to ensure that data is not lost even if specific components in the storage subsystem fail. As a safety net in assuring data availability, database backups are performed to capture all changes. This data is backed up to tape nightly and stored offsite. Data stored within Amazon's infrastructure is highly redundant and backed by a 99.99% availability SLA.

Additional Questions?

For any additional information or questions about any of Veritext's security practices, please contact us at helpdesk@veritext.com.

About Us

About LawStudio

Part legal support software, part secure Cloud storage, LawStudio is an online workspace where law firms can organize and build their case in a user-friendly collaborative environment.
www.lawstudio.com

Email: support@lawstudio.com
Tel: 844.224.0330

About Veritext Legal Solutions

Veritext provides superior court reporting and litigation services to the legal industry with a proven track record of industry excellence. Veritext is the established leader in technology-driven deposition and litigation support services for law firms and corporations.
www.veritext.com

Headquarters

290 West Mount Pleasant Avenue
Suite 3200
Livingston, NJ 07039
Tel: 800.567.8658

LawStudio™ VERITEXT LEGAL SOLUTIONS

© 2015 LawStudio, Veritext Legal Solutions