VERITEXT
LEGAL SOLUTIONS

# INFORMATION SECURITY AT VERITEXT

*Protecting Your Data*

SOC 2 CERTIFIED

HIPAA COMPLIANT

PCI DSS CERTIFIED

CCPA COMPLIANT

PIPEDA COMPLIANT

PIPA COMPLIANT

CSAE 3416 COMPLIANT

# The Veritext **Security Model**

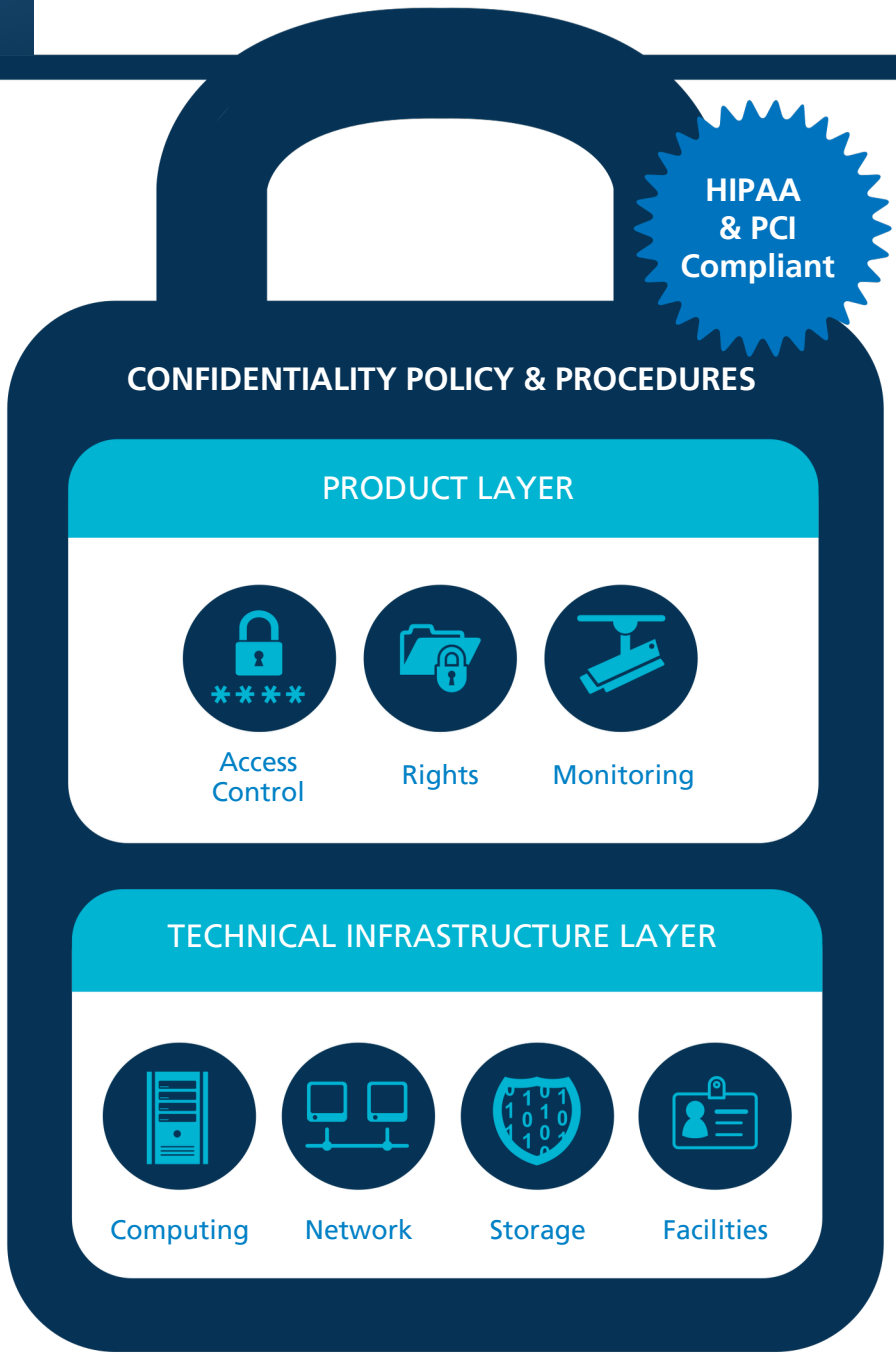
## Introduction

Information security and privacy are built into the fabric of everything we do at Veritext. Helping to protect the confidentiality and integrity of client data is a core part of our mission. Veritext has made significant investments in security-related systems, services, and processes and will continue to invest in maintaining a strong security posture as our clients' requirements continue to develop. This document provides an overview of the systems, controls, and security practices which are compliant with current HIPAA and PCI standards, as well as the latest in security best practices.

## The Veritext Security Model

On a systems level, data security at Veritext is implemented at the infrastructure layer, as well as within each of the specific products that Veritext offers. Surrounding the technical infrastructure and products are the processes and procedures that ensure that the products and services are delivered in a way that ensures information security and privacy. These processes and procedures are embedded in the company confidentiality policy and procedures. In the infrastructure layer, data is stored and moved through the computing and storage systems. Here, our systems utilize strong data encryption to protect against access to the data without authenticated, auditable privileges.

In the product layer, data is processed and presented to authorized individuals based on privileges determined by the client. Both of these system layers are supported by our confidentiality policy, which prescribes our practices designed to ensure protection of client data in the course of developing, maintaining and delivering our products and services. All Veritext employees are trained and managed on this policy. The schematic to the right below 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 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. Veritext utilizes a Amazon AWS hosting services, which maintains ISO27001, SOC, PCI and several other international standards. 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, and abiding by, the Veritext 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 compute 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. External client and agent access is always carried via the secure socket layer (i.e., HTTPS) protocol.

**Storage** security is implemented for all sensitive 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 in the Amazon Web Services (AWS) cloud environment is through Amazon's strong facility controls. Additional information about these controls is available here: **http://aws.amazon.com/security**.

# Security within the **Product Layer**

## Security within the Product 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 Veritext products and systems is implemented both for clients accessing the system, as well as across subsystems. User login is required in order to obtain access to product functions and content, and user credentials are protected from unauthorized access at all times.

**Rights Management** within Veritext products and systems ensures that access to content and resources is granted on a "least privileged" basis, meaning that access is granted only to resources required for the work function.

**Close Monitoring** of Veritext products and systems ensures that controls and policies are 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 prob- lem. In addition, access audit logging ensures that potential unautho- rized access can be quickly assessed and resolved.

# Veritext Confidentiality **Policy & Procedure**

## Veritext Confidentiality Policy & Procedure

Underpinning the design, implementation and support for MyVeritext 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 ensuresthat client data is notonly secured for access only to client-authorized individuals, but also works hard to ensure that it is always available for client 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. 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 your Veritext account or client services representative.

# About Us

**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