



TECHLAW SOLUTIONS SECURITY PROTOCOLS

Introduction

One of the most critical aspects of any electronic discovery project is ensuring secure data handling. The aggressive deadlines typically associated with e-Discovery projects and the large volumes of data managed cannot be permitted to compromise proper chain-of-custody and data confidentiality protocols.

With more than 25 years of experience managing sophisticated and sensitive corporate and government projects, TechLaw Solutions implements stringent security measures to ensure your data remains safe and uncompromised.

There are several key areas TechLaw Solutions focuses on to ensure your data remains secure:

- ▶ Facility Management
- ▶ IT Environment: Hardware Functionality, Redundancy, and Security
- ▶ Software Functionality and Security

Facility Management

Your data physically resides at a TechLaw Solutions Data Center and is accessible to your review team 24/7 via a secure 128-bit SSL connection.

Restricted Access

First, TechLaw Solutions employees not related to a project are prevented from coming in contact with critical data. Personnel in data processing facilities, with a wealth of experience and credentials, are well accustomed to the sensitivity and attention required to properly manage both e-Discovery and paper-based projects. Additionally, as a condition of employment all TechLaw Solutions employees must sign, and are subject to, a Confidentiality Agreement.

The TechLaw Solutions Data Center includes an array of highly sophisticated servers and other security-related software and hardware to store, process, and produce electronic data. This equipment, confined in a secure area with highly restricted access, prevents unauthorized access. Active key-cards are required to gain entrance and only top-level information technology staff and senior level project managers have access to the area and equipment.

TechLaw Solutions can also provide our clients with separate processing rooms for projects requiring an additional layer of measured security (hardware, hard copy documents, document review, etc.). This configuration also features restricted card access as well as video monitoring to prevent co-mingling of data.

Data Destruction

When a project is completed and it is no longer necessary for TechLaw Solutions to maintain or store the media or relevant data, appropriate actions are taken to permanently remove and delete all data. Upon written client notification or court order, TechLaw Solutions will follow one of three processes:

1. destroy the data and provide the necessary documented assurances that the data was destroyed; or
2. contract with a bonded destruction company to perform the destruction and provide related documentation; or
3. return the data in accordance with final instructions.

IT Environment: Hardware Functionality, Redundancy & Security

TechLaw Solutions constantly evaluates, upgrades, and invests in high-performance technology to ensure the most efficient, secure review experience.

Staging and Review

Once received, data is loaded onto servers located in a staging cluster. The staging environment handles initial processing, including culling, keyword searches, indexing, and de-duping. After processing, the data is moved to a hosted review cluster designated specifically for review purposes.

Multi-processor servers, configured into highly redundant clusters, deliver maximum processing performance and up time for reviewers. Clusters are scalable, accommodating any size processing need. Within a cluster, servers are dedicated to maintaining separate functional roles- database management, hosting clustered file shares, and passive nodes for automatic application rollover.

All data in a cluster is stored on redundant, scalable storage area networks (SAN) configured for maximum data redundancy and data access speeds.

Data Presentation and Distributed Access

The hosted data review application is available through a scalable Citrix server farm. This distributed data model improves performance and adds the security of maintaining data on servers inaccessible from internet connected appliances.

Multi-processor servers are configured on a load-balanced farm for maximum redundancy. The Citrix farm is also scalable to meet any client access requirements. Citrix access gateways and the Citrix web server farm are in place to provide or restrict access to the application and your data.

All Citrix access gateways and Citrix web servers are configured in a load-balanced cluster or high availability configuration. This design assures uninterrupted connectivity.

Connectivity

TechLaw Solutions has multiple circuits in place to manage and maintain outside connectivity, maximize speed and performance, and provide broad and secure bandwidth. The primary connection is a DS3, with a T1 failover circuit in the event of an ISP failure. The configuration is scalable to accommodate as many concurrent connections as necessary. Modifications to typical configurations offer a distinct separate environment when necessary.

Routing all connection circuits through individual POP provides not only circuit failsafe but also POP or ISP failsafe. In the event of a primary circuit failure, hosting communications can be quickly rerouted through the T1.

Data Backup

For added data security, all data on SAN appliances is backed up nightly to magnetic tape. This backup data is stored for a pre-determined period as part of the service agreement.

Configurations, network components, and other relevant essential information are backed up on tape media on a monthly basis. All backup media and the procedures to restore the backup are stored securely and away from the primary physical site. Backup testing occurs on a regular schedule, ensuring restoration within an appropriately allotted period.

Software Functionality and Security

TechLaw Solutions constantly reviews potential threats to maintain the highest level of protection for your data.

Password Protection

The use of secure passwords is critical to protecting client data. TechLaw Solutions utilizes server-based protocols and policies, including 8 character passwords using alphanumeric and special characters. Additionally, passwords are changed every 60 days and are only provided to senior information technology staff. For further protection users cannot change their application access passwords, this may only be accomplished by authorized TechLaw Solutions personnel.

Connectivity

Once a reviewer establishes a secure connection to the review application, data is exchanged between the user and the data servers. Citrix access gateways are the front-end or first level of security the

client encounters. Anyone attempting to gain access must provide a user name and password established with TechLaw Solutions for the specific project. As a secondary measure, use of an optional secure token with a rotating pass code may also be implemented.

The second level of access security occurs as authentication is required at the Citrix web server. Once validated, connection to the hosted application is established via the Citrix client or ICA client. To protect the data transmission, a Secure Sockets Layer, or SSL, is also used. All inbound and outbound connections within the TechLaw Solutions hosted and review environment are established via 128 bit encrypted SSL to ensure client data safety. This design provides for maximum data security.

Firewall and Anti-Virus

TechLaw Solutions incorporates firewall applications to manage intrusion protection, spyware, and anti virus scanning on data packets. After passing through the Citrix hardware, the access request is routed through multiple firewall appliances running in a high availability configuration. The intrusion prevention services, or IPS, monitors network traffic via deep packet scanning, searching for any abnormalities. If an abnormality is detected, that traffic is blocked and an alert will immediately be sent to the appropriate TechLaw Solutions professional.

The current TechLaw Solutions architecture and specifically the anti-virus gateway and intrusion prevention services secure the network from the core to the perimeter against potential threats. These include viruses, worms, Trojans, software vulnerabilities such as buffer overflows, peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.

Integrated gateway anti-virus and intrusion prevention delivers intelligent, real-time network security protection against sophisticated application layer and content-based attacks. The addition of anti-spyware service protects the network from intrusive spyware by cutting off installations and delivery at the gateway. Standard antivirus protection is also incorporated within the TechLaw Solutions software configuration. More details on these and other components are available for detailed discussion with TechLaw Solutions technical staff.

Summary

For over 25 years, TechLaw Solutions has delivered innovative discovery solutions while maintaining data security. Rigorous data handling protocols in each facility ensure the integrity and confidentiality of your data. ●