SmartRoom™

SECURITY OVERVIEW

SECURITY OVERVIEW

Here at SmartRoom, we take a security-first approach to everything we do. We combine a number of safeguards that make up the most advance dimensional security solution of any virtual data room on the market. Ensure your data is protected at all times and have complete peace-of-mind it never falls into the wrong hands.

Security standards are divided into the following categories: administrative, physical and technical safeguards.

ADMINISTRATIVE SAFEGUARDS

Documented, formal practices to manage the selection and implementation of security measures that protect information and guide the conduct of personnel in relation to the protection of information.

PHYSICAL SAFEGUARDS

Practices to manage the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion.

TECHNICAL SAFEGUARDS

Processes that are put in place to protect and to control information access and data that is stored, transmitted and shared over the network.

ADMINISTRATIVE SAFEGUARDS

Security Management Process

Risk Management Analysis

Penetration testing, vulnerability scanning, and patching updates are conducted regularly by top-level security firms. We have a dedicated 24/7 infrastructure monitoring team to watch for any unusual activity and to handle any potential issues.

Information Access Management

Access Authorization

Customized Security Profiles
Administrators have full control over all data and can restrict access to any document, file, or folder. Custom security profiles can be created for individuals or groups to restrict view, print, save and modify rights.

Remote Document Detonation
SmartRoom gives administrators the ability to remotely detonate documents even after they have been downloaded by end users. This gives administrators full control of data even if it’s been taken out of the platform.

ADMINISTRATIVE SAFEGUARDS

Data Backup Plan

Our cloud hosted servers are on a robust platform that provides us stability and emergency access to backup processes by Microsoft Azure, the industry's leading hosting provider. Our high-performance back-up systems capture data at multiple intervals throughout the day. Database replication provides redundancy-stored at dispersed geographical locations.

Disaster Recovery Plan

Our systems are built on the principals of high availability and disaster recovery. We have a documented Disaster Recovery Plan that has been tested in real time. Our DR plan is reviewed and updated annually. Our recovery time objective is 24 hours. Our recovery point objective is 15 minutes.

PHYSICAL SAFEGUARDS

Facility Security Plan

All data is stored in multiple locations across the globe on servers maintained by Microsoft Azure. An account's data is generally stored at the server location that is geographically nearest to the administrator. All data centers containing SmartRoom servers are SSAE 16 certified, proving that they meet high standards for security. Physical access is tightly controlled and double verification is required to proceed to any areas housing data.

Access Controls & Validation Procedures

Data Center access controls follow AICPA AT-801 I standards and procedures as well as industry practices. Every user accessing our servers by our hosting provider, Microsoft Azure, is logged in and monitored.

TECHNICAL SAFEGUARDS

Access Control

Unique User Identification

SmartRoom provides custom multi-factor authentication and secure password requirements to ensure only provisioned users have access to the room.

Logical Security

SmartRoom is enhanced by network segmentation, firewall security, and proactive intrusion detection systems. The application itself is built using multiple layers of logical security to ensure the integrity of our user rights systems.

In addition to our internal application firewalls, SmartRoom utilizes data hosting provider Microsoft Azure's web application firewall (WAF) in Azure Application Gateway that helps protect from common web-based attacks like SQL injection, cross-site scripting attacks, and session hijacking. It comes preconfigured with protection from threats identified by the Open Web Application Security Project (OWASP) as the top 10 common vulnerabilities

Alert Logic Intrusion Detection System

SmartRoom utilizes the intrusion detection services of Alert Logic, the industry leader in cloud workload security. Alert Logic provides Security-as-a-Service solutions that combine cloud-based software and innovative analytics with expert services to assess, detect and block threats to SmartRoom. The protection extends to all layers the platform and infrastructure stack to defend against a broad range of server-side threats including hard-to-detect web application attacks such as SQL injection, path traversal and cross-site scripting as well as advanced malware, command to control, brute force and many others.

TECHNICAL SAFEGUARDS

Audit Control

Notification and Archiving

Full audit logs and real-time reporting of any and all user activity are readily available to SmartRoom administrators.

Data Integrity

Mechanism to Authenticate Data

Enable customizable electronic watermarks on documents to protect from improper distribution, alterations, or destruction of data.

Restrict print screen or third-party screen capture applications to prevent unauthorized use or alteration of data.

Transmission Security

Encryption and Decryption

SmartRoom uses TLS 1.2 AES 256-bit encryption; all data is encrypted in transit and at-rest. In addition, SmartRoom uses dual encryption, using a separate encryption key for each file AND a separate key for each site. Files are double-encrypted by taking each unique file key and encrypting it with the site key.

ABOUT SMARTROOM

SmartRoom, is a next-generation virtual data room. Built from the ground up, it was designed to deliver greater efficiency and bank-grade security for file sharing and collaboration. Appeasing both end-users and IT departments, SmartRoom facilitates success for the entire organization and all parties involved.

CONTACT US TO GET STARTED

sales@smartroom.com
www.smartroom.com I 877.332.5739

Sara Patterson
Lead IT Technician
John Miloa
Lead Technician

SmartRoom™