

Security Best Practices

Introduction

We appreciate the amount of trust you place in AuditBoard to protect your data while we provide quality audit, risk, and compliance services to your organization.

This guide describes how protection is provided and informs AuditBoard Core Users, System Admins, IT and InfoSec teams and any others responsible for ensuring their organization's use of AuditBoard is secure and conforms with best practices.

The recommendations contained in this guide will help you take advantage of AuditBoard's available security features, and optimize your organization's use of the service for information security.

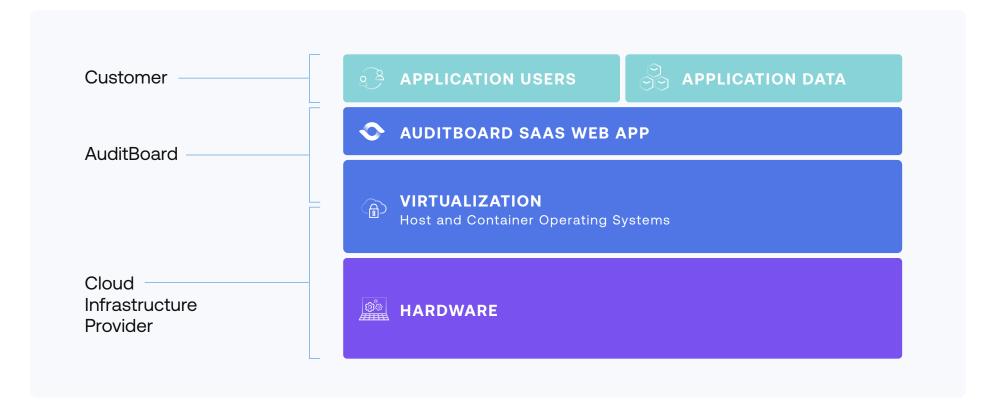
Table of Contents

Shared Responsibility Model	3
Security of the Platform (AuditBoard's Part)	4
Security and Compliance Programs	
AuditBoard Application Software Security	
Secure Cloud Hosting	
Infrastructure Security	
Data Protection	
Security on the Platform (Your Part)	6
User Management	
Authentiation Best Practices	
User Management Best Practices	
Data Management Best Practices	

Shared Responsibility Model

Ensuring your usage of AuditBoard is secure starts with understanding the division of responsibility for security between AuditBoard and your organization. Most simply put, AuditBoard is responsible for the security *of* the platform. You are responsible for your security *on* the platform.

This shared responsibility model is intended to ensure accountability and clearly outline each party's security obligations. AuditBoard handles the operation and management of its platform, including the cloud infrastructure, operating system, and web application security. You are responsible for user access management and any data you upload to AuditBoard. Based on the rules and regulations that apply to your organization, your responsibilities may vary.



Security of the Platform

How AuditBoard Does Our Part



Security and Compliance Programs

In order to protect our customers and their data, AuditBoard has adopted a formal information security management program that governs software development, infrastructure operation, administration, and delivery of the AuditBoard product application.

These security programs, along with an extensive control environment, are regularly assessed against industry standard frameworks, including: NIST 800-53, ISO 27001, SOC 2, Cloud Security Alliance STAR, and HIPAA. For a copy of our compliance reports, please reach out to AuditBoard Support or your Sales Representative.







AuditBoard Application Software Security

Continuous Software Updates - Product upgrades that contain new security enhancements as well as the latest software updates are automatically applied on a bi-weekly basis. These updates are automatic and require no downtime or customer action to be applied.

Extensively Tested - All product updates undergo strict quality and security assurance testing before being made available for release, including manual code review by developers trained in secure coding, software composition analysis, static code analysis, and web application security scanning.

Third-Party Verified - AuditBoard is regularly assessed during formal third-party penetration tests and continuously by the security researcher community in our bug bounty program. Penetration test summary reports are available for each major quarterly release of the product application. For a copy, reach out to AuditBoard Support or your Sales representative.



Secure Cloud Hosting

Browser-Based Web Application - As a fully managed software as a service (SaaS), all functionality is accessible from a web browser and any modern browser is compatible.

Trust - The AuditBoard Platform is hosted on Amazon Web Services (AWS) cloud infrastructure. It's the gold standard for thousands of companies worldwide, who rely on their extensive, integrated native security controls.

Redundancy - Services are replicated and load-balanced across data centers and regions.

Physical Security - AWS data centers are protected by industry leading physical security controls including biometric entry authentication and 24/7 monitoring.



Infrastructure Security

Configuration Management - All network and systems infrastructure is configured to conform with industry standards such as the CIS Benchmarks for AWS and Kubernetes.

Immutable Infrastructure - All production infrastructure is deployed by automation, so staff do not interact with production systems

Single Tenant Architecture - Dedicated application instances, databases and storage resources are deployed for each customer and use unique kubernetes namespaces and (lam) identities that provide segmentation and process, network and filesystem levels.

Strictly Monitored - All platform components are closely monitored to ensure performance, availability, and security.



Data protection

Transport Encryption - Strong end-to-end TLS 1.2 encryption protects customer data wherever it is transferred.

Storage Encryption - All customer files, databases, and backups are AES-256-bit encrypted before being written to permanent disk storage.

Encryption Key Management - AuditBoard leverages a native key management solution (AWS KMS) to generate, store, use and rotate encryption keys used to protect customer data.

Data Integrity - Your data is protected from loss, manipulation, or corruption by cryptographic hashing controls that enforce versioning and provide secure transactional capabilities.

Data Backup - Continuous, real-time backups allow for data recovery at 1-second granularity.

Daily Backups - Encrypted full database backups are made daily and stored in encrypted, redundant, and versioned S3 storage.

Secure Deletion - NIST-compliant data sanitization procedures are employed to securely delete data that has reached the end of its useful life.

Security on the Platform

How You Can Do Your Part (Secure Usage Best Practices)

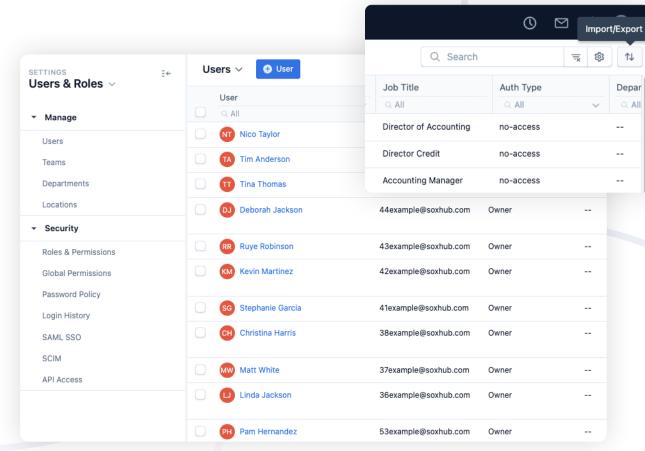




User Management

Ensure that only authorized users have access to the platform.

Periodically audit the list of authorized users in application settings to ensure all users on the platform still require access, and any unauthorized users can be removed. The list of users can be downloaded in CSV format for easier offline analysis.



Users & Roles Settings



Authentication Best Practices

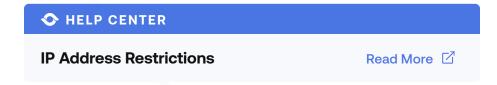
1. Use Single Sign-On (SSO)

AuditBoard supports the SAML 2.0 and SCIM protocols, making it compatible with common enterprise single sign-on solutions like Okta, OneLogin, PingOne, etc. Use this capability to sync authorized users to your corporate directory and automate the removal of terminated employees.

• HELP CENTER	
Single Sign-On User Guide	Read More 🗹
SCIM User Guide	Read More 🗹

2. Control Network Access

Limit access to your AuditBoard application by allowlisting trusted network space only, such as your VPN and corporate network IP addresses.



3. Enforce Multi-Factor Authentication

Require users to authenticate with multiple factors to reduce the risk of unauthorized access.





User Management Best Practices

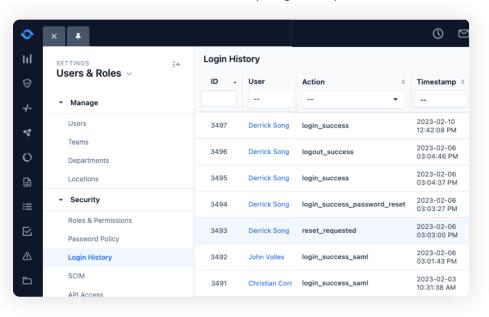
1. Follow the Principle of Least Privilege

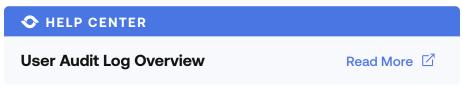
Use AuditBoard's prebuilt roles to ensure users have the minimum permissions needed to perform their function. Custom roles can be created if needed.



2. Audit Your Access Logs

AuditBoard gives you the ability to inspect and/or export Login History and Audit Logs through the platform. Regularly inspect AuditBoard logs for signs of unauthorized access or credentials requiring cleanup.





3. Ensure Appropriate Password Policies are Set

Utilize the AuditBoard password policy features to enforce requirements on passwords and make sure session lengths are set accurately.



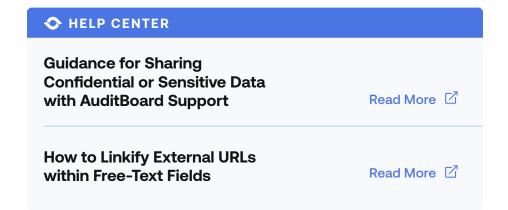
Data Management Best Practices

1. Limit Sensitive Data Exposure

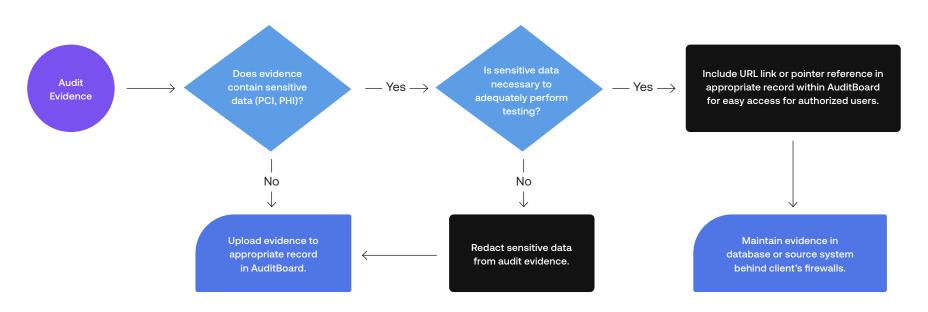
It's not uncommon for audit teams to have access to sensitive data, such as PCI, PII, or PHI. This sensitive data is generally not required to perform and document testing. Auditing Best Practices include establishing policies which prohibit including sensitive data in audit records to limit data leak exposure.

2. Reference External Links

In many cases, you can avoid any issues with sensitive data exposure by storing external links to documents instead of uploading the document artifacts themselves. These links could point to secure intranet resources or locations protected by a variety of separate security controls that could be controlled by you and your team.

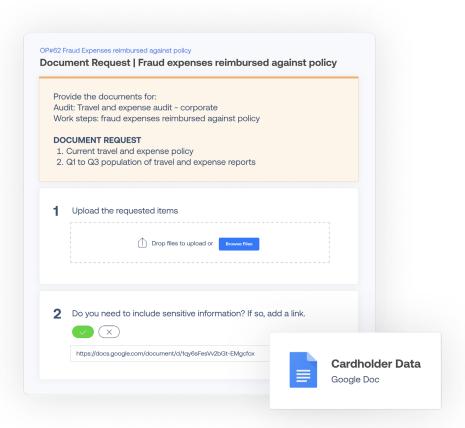


SAMPLE WORKFLOW FOR MANAGING SENSITIVE DATA



3. Implement an Acceptable Use Policy Acknowledgment

Use AuditBoard Workflows to customize requirement of an Acceptable Use Disclaimer to address potential compliance requirements



About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.

Copyright © AuditBoard 2023