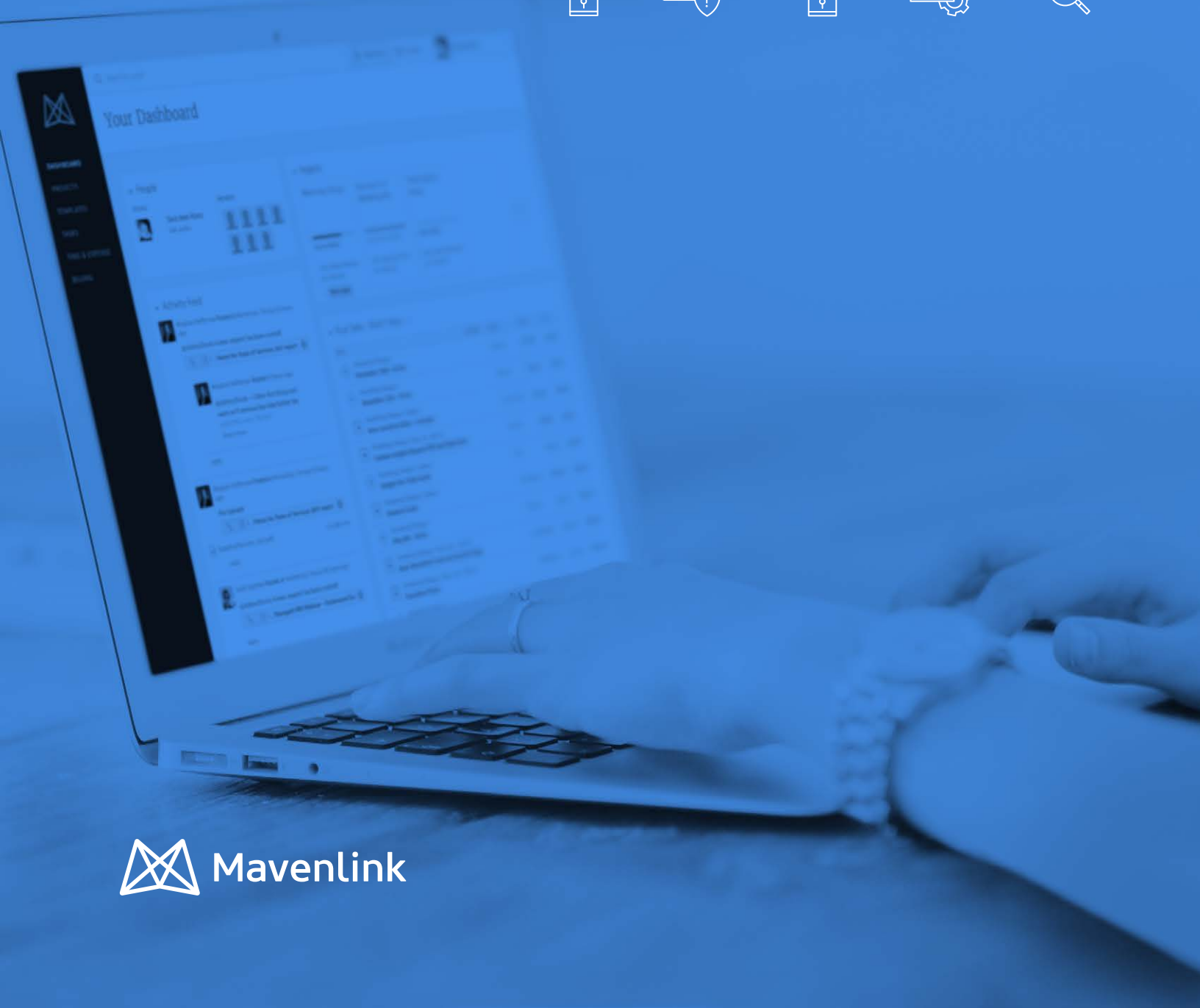
# Security and Compliance at Mavenlink




Mavenlink

# Table of Contents

# Introduction

Our mission at Mavenlink is to reinvent the way businesses work with distributed teams, subcontractors, and clients. We provide technology, expertise, and services that enable organizations to deliver projects predictably and at the desired costs or margins.

In order to fulfill our mission, Mavenlink provides Software as a Service (SaaS) to creative agencies, IT services teams, internal shared services organizations, and professional services teams. This document details the security practices and controls implemented by our executive, operations, and engineering teams to protect client business data and provide a reliable, high-performance platform for project delivery.

# Application Security

## Software Development Practices

### DEVELOPMENT PROCESS

Mavenlink maintains documented Systems Development Life Cycle (SDLC) policies and procedures that govern the design and implementation of application and infrastructure changes.

We use test-driven development (TDD), pair programming, quality assurance (QA), and code review processes to maintain standards for product quality, security and user experience.

### CHANGE MANAGEMENT

Mavenlink documents and tracks new product capabilities and enhancements via user stories, automated tests, and User Acceptance Testing (UAT).

We uses GitHub to maintain source code versions, track changes, and facilitate our mandatory code review process.

Our Continuous Integration (CI) infrastructure runs over 45,000 automated tests on every code change before being shipped to production.

### RELEASE MANAGEMENT

Mavenlink maintains a public change log, which is used to provide release notes to our customers. For customers requiring more thorough testing opportunities, Mavenlink offers a sandbox environment with a recent copy of a customer's account data that can be used to test new features and configuration changes.

# Account Security

## SIGN-IN AND AUTHENTICATION

Mavenlink client administrators can manage user provisioning on their account, and control access using an external SSO provider, or via user-configured passwords.

## SINGLE SIGN-ON (SSO)

Using Single Sign-on (SSO) authentication, Mavenlink customers can manage user system access using an external identity provider. This allows users to authenticate securely to Mavenlink using a centralized identity management tool.

Mavenlink supports both SAML v2 and OpenID technologies. As of April 2017, supported identity providers include: G Suite (OAuth2 or SAML), Yahoo, Intuit, Okta, OneLogin, Generic SAML IDP, and Active Directory Federation Services (via SAML).

## PASSWORD POLICIES & SESSIONS

Mavenlink allows administrators to specify password security criteria, including complexity, reuse, and expiration requirements. Mavenlink user passwords are hashed and salted in accordance with industry best practice, so they are never stored in plaintext on our servers.

User sessions and IP addresses are individually tracked and can be individually audited or revoked by their user. Maximum session duration can be configured by an account's administrators.

## USER PERMISSIONS AND CONTROLS

Mavenlink provides a user and account model that is built on a cascading permission set. This allows administrators to control each user's access throughout the system, while allowing privileged users (e.g. project managers) to further delineate permissions at the project level.

## ACCOUNT-LEVEL PERMISSIONS

Mavenlink's account-level user permissions are configured by account administrators (users with administrator status). Administrators can provision account-level permissions manually, as well as through departmental and/or geographical entitlements.

Account-level permissions control both the actions users may perform in the system and the types of information visible to that user.

## PROJECT-LEVEL PERMISSIONS

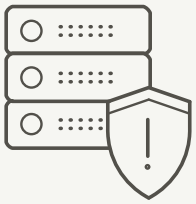
Each project created within Mavenlink follows the account-level permissions, while also enabling access control and role-based permission assignment at the project level. Project participation is limited to users invited to the project by a user with sufficient permissions, and range from full administrative privileges for that project to read-only access.

The Provider-Client dimension adds another layer of control. Every user added to a project is designated as part of the Provider (project delivery) team, or to an optional Client team. Clients in a project have limited access to certain project data, such as resource costs.

## FIELD-LEVEL PERMISSIONS

Mavenlink supports field-level permissions for user-created custom fields. By specifying field-level permissions, administrators can limit access to sensitive data associated with projects, tasks, and other records within the system.

# Infrastructure Security



Mavenlink has implemented an industry-leading software infrastructure with least-privilege role-based access, intrusion detection, and 24x7x365 monitoring.

## Physical Security

Mavenlink uses AWS for its cloud hosting services, and this creates a shared responsibility model between customers and AWS. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

Per Amazon's policy documentation: "Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors."[1] More information can be found on the AWS Compliance center at: http://aws.amazon.com/compliance.

## Corporate Segregation

Access to Mavenlink production networks and systems is strictly controlled and completely separate from corporate infrastructure, both physically and logically. Employees, whether at a Mavenlink office or on the road, must connect to our production infrastructure using a secure VPN with key-based and 2-factor authentication. Access to sensitive systems is identity-based, and restricted based on employee role using a least-privilege approach. In evaluating access levels, the security working group considers employee experience level, job responsibilities, and internal risk assessments.

[1] https://d0.awsstatic.com/whitepapers/Security/Intro_Security_Practices.pdf

# Network Security

Mavenlink hosts its application and customer data on Amazon Web Services' (AWS) core cloud servers. Amazon is the largest provider of virtualized cloud infrastructure in the world and has become the industry leader in best practices. AWS provides extensive documentation on its security and control environment, industry certifications, and third-party attestations. For more information, visit http://aws.amazon.com/security.

We operate in a strictly controlled Linux server environment that only allows validated software to be run. There is no direct access to the cloud infrastructure from the public internet, and software downloads are limited to a set of validated software packages required to operate the infrastructure.

Access to Mavenlink's secure infrastructure is strictly controlled via network security groups and identity-based authentication. Mavenlink employees requiring access must complete successful background checks and use a secure virtual private network (VPN) connection with two-factor authentication.

# Data Security

Mavenlink employs industry-leading security practices to protect customer data. All customer data is stored within AWS and isolated from Mavenlink office locations. All data is encrypted at rest, providing an added layer of security.

## Multi-tenant Architecture

Mavenlink is architected as a pure multi-tenant SaaS application, enabling the most sophisticated project collaboration experience available today. All accounts benefit from access to the latest features and code updates as they are made available,[2] and bug fixes and enhancements are released up to several times per day. Through our Agile software development methodology, we are able to deploy most improvements with zero downtime.[3]

We take the security of your data extremely seriously. All customer accounts are logically separated at the data layer, and automated testing ensures account security is maintained as features are added and changed.

## Transmission Security

Mavenlink's RESTful API is served over HTTPS and uses the OAuth 2 authorization model for secure, user-based access.

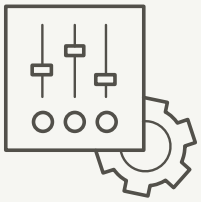
All customer data is encrypted in transit using the Transport Layer Security (TLS) protocol. Mavenlink uses industry standard AES encryption for the transmission of any customer data between our datacenter locations, as well as between our data centers and end user devices.



[2] For an additional cost, you can test upcoming changes using a recent copy of your data in Mavenlink's pre-release environment.

[3] We provide 24 hours advance notice for scheduled downtime events.

# Infrastructure Operations



## 99.9% Uptime

Most changes to the production environment require no downtime. In the case that downtime is necessary, customers are given at least 24 hours notice. Downtime is scheduled to have minimal impact on the work day in the US, and generally takes place between 7pm and 10pm Pacific Time. Mavenlink boasts 99.9% uptime[4] with an average response time of 150 milliseconds.[5]

### BUSINESS CONTINUITY

Mavenlink leverages AWS to provide a high degree of availability and fault tolerance. Our Elastic Load Balancers (ELB) route traffic to a cluster of API servers located across multiple redundant Availability Zones (AZ). Customer data is backed up multiple times per day, and shipped from our primary datacenter (AWS Oregon Region) to multiple off-site locations, including our disaster recovery site (AWS Virginia Region) that houses a live-updated standby database system.

## 24x7x365 Monitoring and Protection

Mavenlink's application performance and security is monitored 24x7x365 by a dedicated, on-site Operations team. Our monitoring systems consolidate system performance data across our infrastructure, including multiple layers of thresholds and alerts.

[4] SLA available

[5] See our live Status Page at: https://mavenlink.statuspage.io

## SECURITY

Mavenlink continuously monitors systems, conducting tests for intrusions and attacks. We implement intrusion detection system (IDS), with alarms in place to alert of suspicious activity. System and network logs are shipped off-site to aid in incident response and root cause analysis.

We monitor all Common Vulnerabilities and Exposures (CVEs) for our environment, and generally patch critical vulnerabilities within 24-hours.

To detect security vulnerabilities, Mavenlink uses a combination of automated scanning, penetration testing, and third-party security research. We also maintains a Responsible Disclosure Program through HackerOne: https://hackerone.com/mavenlink.

# Risk & Compliance

## Independent Audit

Mavenlink meets or exceeds the standards of SSAE 16 (SOC1 Type II) and AICPA SOC2 Type II, and has for the past three years with no exceptions noted. We are audited over the entire calendar year to ensure compliance at the highest possible level, and our system controls are audited for effectiveness in addition to design.[6]

## EU-US Privacy Shield

Mavenlink is committed to protecting your privacy. We have self-certified to the EU-US Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt0000000PBe4AAG&status=Active. For more information, see our Privacy Policy at: www.mavenlink.com/legal/privacy.

## Risk Management

Mavenlink conducts quarterly risk assessments of our control environment, which includes the processes, people, and technologies used to deliver Mavenlink to our customers. We also conduct third party penetration testing annually.

[6] SOC Type II reports audit the effectiveness of controls in addition to their design, whereas SOC Type I reports audit design only.

# Conclusion

Thank you for your interest in Mavenlink's security and compliance procedures. We understand that you may have specific concerns not addressed in this document, and we invite you to contact us with questions. Please note that as Mavenlink is committed to continuous improvement of our security practices, the information in this document is subject to change.

# Resources

- Security and Compliance
  https://www.mavenlink.com/trust
- System Status
  https://mavenlink.statuspage.io
- Responsible Disclosure Program
  https://hackerone.com/mavenlink
- Terms of Service (TOS)
  https://www.mavenlink.com/legal
- Privacy Policy
  https://www.mavenlink.com/legal/privacy
- API Documentation
  http://developer.mavenlink.com
- AWS Security and Compliance Quick Reference Guide
  https://d0.awsstatic.com/whitepapers/compliance/AWS_Compliance_Quick_Reference.pdf
- Amazon Web Services: Overview of Security Processes
  https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf