Prismatic iPaaS

Data Privacy and Security Information

Introduction

This document serves as a lite version of our standard security questionnaire to give prospects an idea of our security and privacy practices at Prismatic. More information on Security and Privacy at our company can be found in the below links. This document, in its entirety, is protected by NDA.

Legal Center: https://prismatic.io/legal/terms/

Privacy Policy: https://prismatic.io/legal/privacy/

Security: https://prismatic.io/legal/security/

Table of Contents

Compliance

C-1: Does Prismatic comply with industry regulations and standards applicable to its customers' sectors?

Yes, Prismatic complies with relevant industry standards, including SOC 2, HIPAA, GDPR, CJIS, and is currently working on FedRamp compliance. Prismatic is committed to adhering to sector-specific regulations as required by our customers.

C-2: Has Prismatic undergone any third-party audits or security certifications?

Yes, Prismatic undergoes annual third-party audits for SOC2 Type II by an AICPA accredited firm. Prismatic also undergoes an annual pen test by a third-party and has an open bug-bounty program where anyone can audit our platform security. Our SOC2 audit is a type 2, which includes all 365 days a year the controls have to be maintained. Further, many companies pick and choose the controls they want to be audited on in their SOC2 audits. At Prismatic, we hold ourselves accountable to audit all Security controls in the Security Trust Services portion of the SOC2 Trust Services framework.

Data Governance

DG-1: How does Prismatic classify and manage the data it processes?

Prismatic classifies data based on sensitivity and applies corresponding access and handling controls. Our customer data is only accessible to a small number of backend engineers who undergo background checks, fingerprinting, and have been authorized through various means and certifications to handle such data. Moreover, it is our policy that we never view customer data unless the customer requests us to in helping them out with programming steps.

DG-2: What policies are in place for data retention and deletion?

Data retention policies are customizable by customers to either be 14 days by default or zero retention by configuration, with secure deletion practices in place for data that is no longer needed.

Facility Security

FS-1: What physical security measures does Prismatic implement at its data centers?

Prismatic uses AWS as a sub-processor. AWS implements comprehensive physical security measures including 24/7 surveillance, biometric access controls, and environmental protections at all data center locations. AWS data centers are secure by design and our controls make that possible. “Before we build a data center, we spend countless hours considering potential threats and designing, implementing, and testing controls to ensure the systems, technology, and people we deploy counteract risk.” AWS considers site selection, redundancy, availability, and capacity planning in its secure design strategy. Further, AWS has full business continuity and disaster recovery plans and a pandemic response plan. Their physical access to their data centers is highly controlled. In addition, AWS performs monitoring and logging, surveillance and detection, device management, infrastructure maintenance, governance and risk compliance, and maintains operational support systems for climate and disaster contingencies.

Human Resources

HR-1: Are employees trained on privacy and security best practices?

All employees undergo regular training on privacy and security generally and best practices specifically for each standard with which we are compliant, including data handling and incident response protocols.

HR-2: How does Prismatic manage access controls for its employees?

Access controls are strictly enforced through role-based access permissions. Authorization is granted after review of the employee’s background check and is only granted for certain data types with specific certifications for those data types that need to be accessed. Prismatic has strict procedures on authorization and termination of access which are certified in our SOC2 report. All access is reviewed and updated quarterly.

Information Security

IS-1: What encryption methods are used to protect data in transit and at rest?

Data in transit is protected using TLS 1.2 or higher, while data at rest is encrypted using AES-256 encryption standards. Prismatic's iPaaS is a data connection and integration platform.

- *A note on TLS 1.2 or higher: If the customer's browser supports TLS 1.3, that will be used. If not, it drops down automatically to TLS 1.2. TLS 1.2 has several secure ciphers and a few that are weak but because of the way the internet and browser compatibility work, someone could potentially be running a very out of date browser which would need an older weaker cipher from the options in TLS 1.2. Prismatic must support TLS 1.2 due to the compatibility issues with TLS 1.3 and older browsers.

IS-2: How does Prismatic handle security incidents?

Prismatic has a dedicated incident response team that follows a structured protocol for handling security incidents, including notification processes for affected customers and governmental agencies overseeing the standards Prismatic adheres to.

Legal

L-1: How does Prismatic ensure compliance with global data protection laws (e.g., GDPR, CCPA)?

Prismatic ensures compliance with global and US data protection laws by implementing comprehensive data protection measures, regular internal audits, and data processing agreements. Further, each employee undergoes privacy training separated into role function on what sensitive data is and how to protect it.

Operations Management

OM-1: How does Prismatic monitor its infrastructure for security threats?

Continuous monitoring of our infrastructure is conducted to identify and mitigate security threats. We look for vulnerabilities and security flaws in the functioning of our platform with internal penetration tests, external penetration tests, and a bug bounty program. Our platform code is meticulously checked with various tools to identify code vulnerabilities which are all corrected within our standard internal vulnerability SLAs

OM-2: What is the process for applying security patches?

Security patches to Prismatic owned infrastructure are applied within 7 days of release. Code vulnerability patches are reviewed, tested, and released with strict adherence to our internal SLAs which are audited and certified in our SOC2 report.

Risk Management

RM-1: How does Prismatic assess and manage risks related to third-party vendors?

Prismatic maintains a meticulous third-party vendor risk assessment program. Third-party vendors are assessed annually for compliance with Prismatic's security requirements. Prismatic uses a combination of vendor incident history and SOC2 Type II reports along with security questionnaires, as needed, to assess vendor risk to Prismatic operations.

Release Management

REL-1: What processes are in place for the secure development and deployment of new features?

Prismatic maintains a secure development policy which is made up of system change control procedures, software version control, technical review of applications after operating platform changes, restrictions on changes to software packages, secure system, engineering principles, secure development environment, system security testing, system acceptance testing, open-source components, code review, integration with CI/CD, and specifications on acquisition of third-party systems and software.

Resilience

RES-1: Does Prismatic have a disaster recovery plan? How frequently is it tested?

Prismatic maintains a comprehensive business continuity and disaster recovery plan, tested annually, to ensure business continuity under nearly all circumstances. Prismatic maintains an RPO of 1 hour and an RTO of 4 hours for platform availability. These recovery goals are further bolstered by SLAs defined with each customer in the final MSA. Additional Disaster Recovery details can be found in Appendix B: Disaster Recovery Details.

Security Architecture

SA-1: How is the iPaaS platform architected for security?

The iPaaS platform is designed with a multi-layered security approach, including network segmentation via VPC and region, firewalls, strict access controls to safeguard customer data, and API secrets used to access all portions of the platform's data manipulation functions. There is no co-mingling of data and each process has it's own clean process runner within the platform.

Data Privacy and Security within the Architecture

Organizational Content, as defined in our Master Service Agreement (MSA), is stored in a protected and encrypted storage within the system. Step results, execution payloads, logs, and telemetry are stored for a maximum of 14 days in a separate part of the system that is also encrypted and can only be accessed with limited authenticated accounts which are tightly controlled. Step results and execution payloads

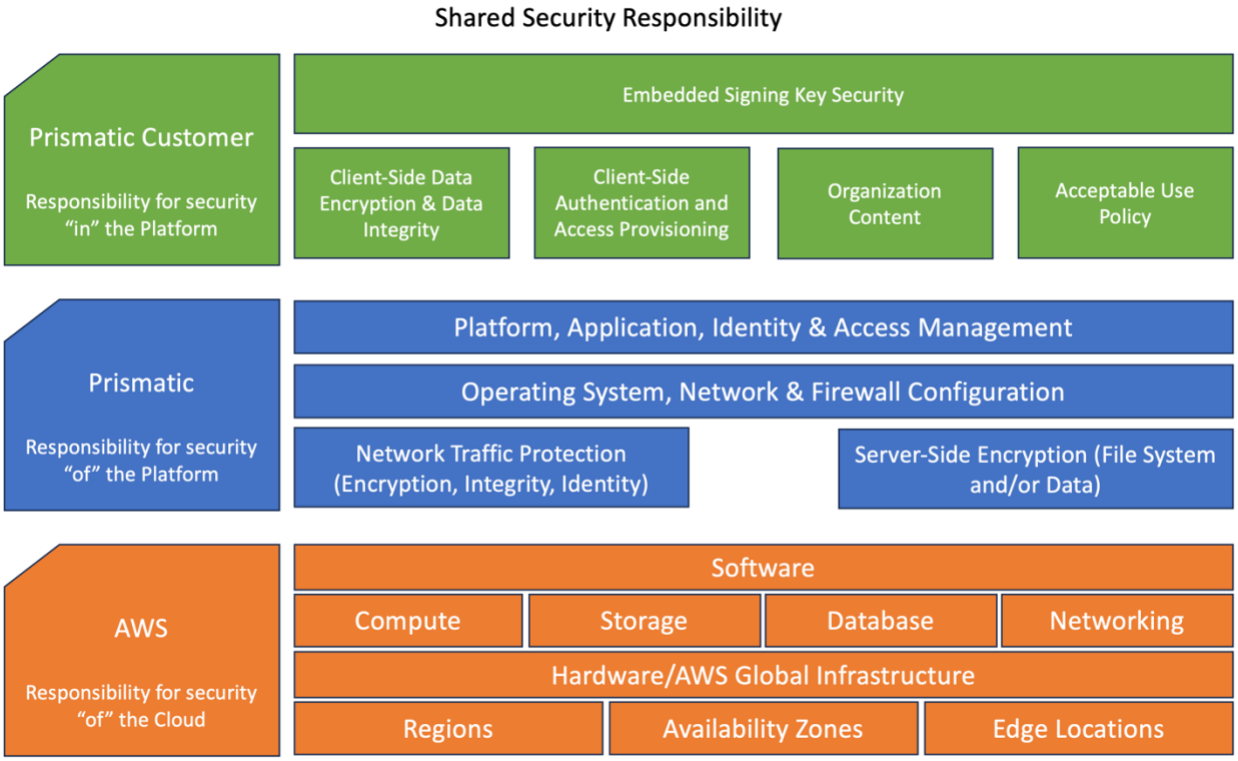
could possibly contain customer data depending on what and how you've integrated data points. It is possible to turn off step results for customers once you have the integrations running correctly and how you expect.

More details about the architecture and design can be found in Appendix A: Architecture.

Platform Shared Security Model

We split security responsibility up into three segments:

1. Our sub-processor AWS's responsibility for security **of the cloud**.
2. Prismatic's responsibility for security **of the platform**.
3. Customer's responsibility for security **in the platform**.



prismatic

Appendix B: Disaster Recovery Details

Prismatic's AWS DR Processes

- We test our BC/DR with tabletop tests and functional tests.
- We use Terraform in AWS. It allows us to rebuild or remake the environment at will - restore the production state.
- All our code is offsite in GitHub and GitLab and is highly controlled with MFA only access.
- All our API secrets are offsite in Doppler also with MFA only access. Access to API secrets is strictly controlled even amongst the engineering team with only a small subset of our engineers with access.
- BCP with BIA allows us to restore any part of our company at any time within a very short timeframe (due to cloud nature).
- For the database, we have it snapshotted continuously and that data is replicated across many AZs just by the nature of how RDS works.
- We do a full database backup, nightly, and those backups are stored in RDS/S3 which is highly available via AWS.
- For S3, we have replicated our most important data to another bucket in the system across to another region.
- All this data is versioned and is backed up across many AZs, again by nature of how S3 works.
- For Redis, we have a standby node ready if the master fails. This data is temporal though and is not backed up.