Security and Compliance

Overview

The AutoSync Cloud Service adheres to the highest standards of security and compliance to ensure the confidentiality, integrity, and availability of data. This page outlines the security measures, regulatory compliance standards, and best practices implemented within the system.

---

1. Security Architecture

1.1 Authentication and Authorization

- **OAuth 2.0 & SSO**: The AutoSync Cloud Service uses **Keycloak** for Single Sign-On (SSO) and OAuth 2.0-based authentication. OAuth tokens are used to authenticate API requests, ensuring that only authorized users and systems can access resources.
- **JWT (JSON Web Token)**: All interactions with the AutoSync API require JWT tokens. These tokens are generated during the login process and must be included in the `Authorization` header of each request.
  - **Access Tokens**: Short-lived (e.g., 1 hour) and required for accessing protected resources.
  - **Refresh Tokens**: Long-lived tokens used to obtain a new access token when expired.
- **Role-Based Access Control (RBAC)**: Permissions are granted based on roles such as "Admin", "User", and "Viewer", with each role having specific access levels to resources.

1.2 Encryption

- **Data in Transit**: All communications between clients, services, and databases are encrypted using **TLS 1.2+** to protect data from eavesdropping and tampering during transmission.
- **Data at Rest**: All sensitive data, including user information, files, and metadata, is encrypted at rest using **AES-256** encryption. This ensures that data remains protected even if unauthorized access to storage occurs.
- **Key Management**: Encryption keys are managed and rotated periodically using **AWS KMS (Key Management Service)** or **HashiCorp Vault** for secure storage.

---

2. Compliance and Regulatory Standards

The AutoSync Cloud Service meets various industry standards and regulations to ensure that data handling and processing comply with best practices and legal requirements.

2.1 General Data Protection Regulation (GDPR)

- **Data Processing Agreement (DPA)**: The service is fully GDPR-compliant, and a **Data Processing Agreement (DPA)** is provided to customers ensuring that personal data is handled lawfully and transparently.
- **Data Minimization**: Only the minimum required personal data is collected and stored, in line with the principle of data minimization under GDPR.
- **Right to Access and Deletion**: Users can request access to their personal data or request its deletion at any time through the service portal or by contacting support.
- **Data Anonymization**: Where possible, personally identifiable information (PII) is anonymized or pseudonymized to reduce privacy risks.

2.2 Health Insurance Portability and Accountability Act (HIPAA)

- **Protected Health Information (PHI)**: AutoSync Cloud Service ensures that health-related data is handled in accordance with **HIPAA** regulations. All PHI is encrypted both in transit and at rest, and access is controlled and logged to meet HIPAA security standards.

- **Business Associate Agreement (BAA)**: A BAA is available for customers who wish to use the service to process PHI, outlining the responsibilities of both parties in securing health information.

2.3 Payment Card Industry Data Security Standard (PCI-DSS)

- **PCI-DSS Compliance**: AutoSync Cloud Service adheres to **PCI-DSS** standards for handling payment card information. We ensure that cardholder data is encrypted and that all payment processing activities are conducted using secure and compliant systems.
- **Tokenization**: Payment data is tokenized to avoid storing sensitive card details in the system.

2.4 California Consumer Privacy Act (CCPA)

- **CCPA Rights**: In compliance with the **CCPA**, users have the right to:
  - Know what personal data is collected.
  - Request deletion of their personal data.
  - Opt out of the sale of their personal data (if applicable).
- **Consumer Data Requests**: Users can submit requests for data access or deletion via the **AutoSync user portal** or by contacting support.

2.5 Federal Risk and Authorization Management Program (FedRAMP)

- **FedRAMP Authorization**: The AutoSync Cloud Service complies with the **FedRAMP** program for federal agencies, ensuring that security controls are in place for cloud services used by U.S. government agencies. This includes continuous monitoring, vulnerability scanning, and regular audits.
- **Security Assessment**: Regular assessments and audits are performed to ensure that security measures remain aligned with FedRAMP requirements.

---

3. Security Measures

3.1 Network Security

- **Firewall Protection**: All services are deployed behind **AWS Security Groups** and **GCP VPC Firewalls**, which enforce strict access control rules and prevent unauthorized access.
- **DDoS Protection**: **AWS Shield** and **Cloudflare** are used to protect the service from Distributed Denial of Service (DDoS) attacks.
- **Intrusion Detection Systems (IDS)**: **AWS GuardDuty** and **Google Cloud Security Command Center** monitor for suspicious activity and potential security breaches.

3.2 Secure Development Lifecycle (SDLC)

- **Code Reviews and Static Analysis**: All code changes are subject to peer reviews and static code analysis using tools like **SonarQube** to identify vulnerabilities early in the development process.
- **Security Testing**: Regular **penetration tests** are conducted, and vulnerabilities are addressed using an agile patching process.
- **CI/CD Pipeline Security**: The CI/CD pipeline is protected using **GitHub Actions** with secrets management, and deployment is only allowed after automated security checks are passed.

3.3 Logging and Monitoring

- **Audit Logging**: All critical system actions (e.g., user login, file uploads/downloads, data modification) are logged to **AWS CloudTrail** and **Google Cloud Audit Logs**. These logs are retained for at least 1 year to comply with regulatory requirements.
- **Real-Time Monitoring**: **Prometheus** collects system metrics, which are visualized on **Grafana** dashboards. Alerts are triggered for any anomalies or potential security incidents.
- **ELK Stack**: **Elasticsearch**, **Logstash**, and **Kibana (ELK)** are used for centralized logging and monitoring, providing real-time insights into system activity.

---

4. Incident Response

4.1 Incident Detection

- **Anomaly Detection**: Machine learning models are used to identify unusual patterns of activity (e.g., unusual API usage, spikes in traffic) that could indicate a security breach.
- **Real-Time Alerts**: Any security event or breach attempt triggers alerts to the security team via **PagerDuty** or **Slack** for rapid response.

4.2 Incident Management

- **Incident Response Plan**: A comprehensive incident response plan is in place to handle data breaches, service outages, and other security incidents. The plan includes detailed steps for detection, containment, investigation, and reporting.
- **Breach Notification**: In the event of a data breach, customers are notified within 72 hours as required by **GDPR** and other relevant regulations.

---

5. Security Best Practices

- **Zero Trust Architecture**: A **Zero Trust** model is implemented for all internal and external network communications. All users and services are authenticated and authorized before accessing any resource.
- **Patch Management**: All system components are regularly updated to address security vulnerabilities, with a focus on critical patches that may impact system security.
- **User Education and Training**: Employees undergo regular security awareness training to mitigate human risks, including phishing attacks and insider threats.

---

6. Data Backup and Disaster Recovery

6.1 Backup Strategy

- **Daily Backups**: Full database and file storage backups are taken daily and encrypted. Backups are stored in **AWS S3** with cross-region replication to ensure data availability in case of disaster.
- **Snapshotting**: Kubernetes nodes and persistent volumes are snapshot periodically to provide quick recovery from hardware failures.

6.2 Disaster Recovery

- **RTO (Recovery Time Objective)**: The target recovery time is 2 hours for mission-critical systems.
- **RPO (Recovery Point Objective)**: The target recovery point is 1 hour, ensuring minimal data loss in case of a disaster.

---

7. Compliance Audits and Certification

- **Internal Audits**: Regular internal security audits are conducted to ensure compliance with security policies and industry standards.
- **Third-Party Audits**: The AutoSync Cloud Service undergoes annual third-party security audits, including penetration testing and vulnerability assessments, to ensure external validation of our security posture.
- **Certifications**: We are certified for **ISO/IEC 27001** (Information Security Management) and **SOC 2 Type II** (System and Organization Controls).

Conclusion

The AutoSync Cloud Service prioritizes security and compliance, ensuring that all customer data is handled with the highest level of protection. By adhering to industry standards such as **GDPR**, **HIPAA**, and **PCI-DSS**, and implementing comprehensive security measures, we ensure that our platform is secure, reliable, and compliant with regulatory requirements.