# Cloud Security and Governance Policy

1. Introduction

   Data Pilot is committed to maintaining the security, privacy, and compliance of our cloud infrastructure across multiple cloud service providers (CSPs). This Cloud Security and Governance Policy outlines the security measures, controls, and best practices for AWS, Azure, and GCP environments.

2. Cloud Service Provider Selection

   Data Pilot will carefully evaluate and select cloud service providers based on their security capabilities, compliance certifications, reliability, and scalability. AWS, Azure, and GCP have been chosen based on their industry-leading security frameworks and extensive service offerings.

3. Access Control

   3.1. Identity and Access Management (IAM)

   a. Data Pilot will implement a strong IAM strategy, following the principle of least privilege (PoLP) for all users and roles.

   b. Multifactor Authentication (MFA) will be enforced for all privileged accounts.

   c. Regular audits of IAM configurations will be performed to ensure compliance and identify any vulnerabilities.

   3.2. Privileged Access Management (PAM)

   a. Data Pilot will implement PAM solutions to manage and control privileged access to cloud resources.

   b. Privileged access will be regularly reviewed, monitored, and revoked when no longer required.

   c. Just-in-Time (JIT) access will be implemented to minimize the exposure of privileged accounts.

4. Data Security and Encryption

   4.1. Data Classification and Handling

   a. Data Pilot will classify data based on its sensitivity and define appropriate security controls.

   b. Clear data handling procedures will be established, including data retention and disposal practices.

   4.2. Data Encryption

   a. Data Pilot will encrypt data both at rest and in transit using industry-standard encryption algorithms.

   b. Key management will be implemented to ensure secure and centralized control over encryption keys.

5. Network Security

5.1. Virtual Private Cloud (VPC) Design

a. Data Pilot will design VPCs with segmented subnets to control traffic flow and minimize the risk of lateral movement.

b. Network Access Control Lists (NACLs) and Security Groups will be configured to restrict access to the necessary ports and protocols.

5.2. Traffic Monitoring and Intrusion Detection

a. Data Pilot will implement network monitoring tools and intrusion detection systems to detect and respond to any suspicious activity.

b. Network traffic logs will be regularly reviewed to identify potential security incidents.

6. Compliance and Auditing

6.1. Compliance Frameworks

a. Data Pilot will adhere to relevant industry standards and compliance frameworks, such as GDPR, HIPAA, and ISO 27001.

b. Regular assessments and audits will be conducted to ensure compliance and identify areas for improvement.

6.2. Logging and Monitoring

a. Cloud service provider's native logging and monitoring services will be utilized to collect and analyze logs from various cloud resources.

b. Security Information and Event Management (SIEM) solutions will be employed to consolidate and correlate logs for real-time monitoring.

7. Incident Response and Disaster Recovery

7.1. Incident Response Plan

a. Data Pilot will establish an incident response plan to promptly detect, respond to, and recover from security incidents.

b. Roles, responsibilities, and communication channels will be defined to ensure a coordinated response.

7.2. Disaster Recovery (DR)

a. Data Pilot will implement DR strategies, including regular backups and the replication of critical data across multiple regions for quick recovery.

8. Training and Awareness

a. Data Pilot will provide regular security awareness training to employees, contractors, and partners to ensure the adoption of best security practices.

b. Employees will be encouraged to report any security concerns or potential vulnerabilities promptly.

9. Continuous Improvement

   a. Data Pilot is committed to continuous improvement of its cloud security and governance practices.

   b. Regular security assessments, penetration testing, and vulnerability scanning will be performed to identify and mitigate risks.

10. Policy Review

    This Cloud Security and Governance Policy will be reviewed annually, or as needed, to incorporate emerging security technologies, changes in cloud service providers' offerings, and evolving compliance requirements.

By adhering to this Cloud Security and Governance Policy, Data Pilot aims to ensure the confidentiality, integrity, and availability of its cloud infrastructure while maintaining compliance with relevant industry standards and regulations.