Partner Access and Lifecycle Management Policy

Double Good Technologies, LP

March 2024

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.3 - User Provisioning and Deprovisioning, CC7.4 - Least Privilege, CC7.5 - Data Protection and Disposal

Table 2: Document history

Date	Comment
Mar 14 2023	Initial policy

1 Purpose and Scope

This policy establishes a standardized framework for onboarding and offboarding third-party partners (vendors, contractors, consultants) who require access to AWS and other database resources to deliver agreed-upon services. The primary purpose is to ensure:

- **Secure and Compliant Access:** Granting partners the minimum necessary access to perform their duties while adhering to the highest security standards and relevant data privacy regulations.
- **Data Protection:** Maintaining the confidentiality, integrity, and availability of company data through robust access controls and data security practices.
- **SOC 2 Compliance:** Aligning partner access management procedures with the SOC 2 trust principles for security, availability, processing integrity, confidentiality, and privacy.

This policy applies to all third-party partners requiring access to AWS and database resources to perform services for the company.

2 Background

2.1 Importance of Partner Access Management

In today's digital landscape, companies increasingly rely on third-party partners to deliver specialized services. Granting these partners access to AWS and database resources can be essential for successful project execution. However, it also introduces potential security risks and data privacy concerns.

2.2 Security and Compliance Requirements

A well-defined partner access management policy is crucial to mitigate these risks. This policy ensures that partner access is granted based on the principle of least privilege, adhering to strict security protocols. It also ensures compliance with relevant data privacy regulations and industry standards like SOC 2.

3 Onboarding Process

3.1 Pre-Approval and Qualification

Partners must submit a formal request outlining the specific AWS and database resources required to deliver their services. The request will be reviewed by a designated committee to assess the necessity and security implications of granting access, considering SOC 2 controls. Partners will be required to complete a qualification process demonstrating their understanding of security best practices, relevant data privacy regulations, and SOC 2 compliance requirements.

3.2 Access Control and Permissions

The principle of least privilege will be strictly enforced. Partners will only be granted access to the specific AWS resources and databases required for their designated tasks, aligning with TSC CC7.4 (Least Privilege) control objectives. Granular access controls (IAM roles, user permissions) will be implemented to restrict unauthorized actions. These controls will be documented and reviewed regularly. Multi-factor authentication (MFA) will be mandatory for all partner accounts accessing AWS and database resources, following SOC 2 user authentication requirements.

3.3 Security Awareness Training

Partners and their personnel requiring access will be required to complete security awareness training covering topics like data security, access controls, incident reporting, and SOC 2 compliance objectives.

3.4 Data Security and Compliance

Partners are responsible for adhering to all company data security policies, relevant data privacy regulations (e.g., GDPR, CCPA), and TSC CC7.5 (Data Protection and Disposal) controls. Data access will be logged and monitored to track activity and identify any anomalies, in accordance with SOC 2 monitoring controls. Partners are prohibited from transferring or sharing company data with any unauthorized third party, complying with SOC 2 data protection objectives.

3.5 Service Level Agreements (SLAs)

Formal SLAs will be established with partners outlining their responsibilities regarding data security, access controls, incident reporting, and adherence to SOC 2 compliance requirements.

3.6 Onboarding Documentation

The onboarding process will be documented, including access granted, roles assigned, training completed, and SOC 2 control assurances obtained from partners. Partners will be required to acknowledge acceptance of this policy.

4 Offboarding Process

4.1 Access Revocation

Upon partner termination, project completion, or change in personnel requiring access, all partner access privileges to AWS resources and databases will be promptly revoked, following SOC 2 account provisioning and de-provisioning controls.

4.2 Data Archiving or Deletion

Partner data will be archived or deleted according to the agreed-upon data retention policy, relevant regulations, and TSC CC7.5 (Data Protection and Disposal) controls.

4.3 Exit Review

An exit review will be conducted with offboarding partners to gather feedback on the access management process, including any SOC 2 compliance concerns.

5 Audit and Review

Regular audits will be conducted to ensure partners comply with this policy, maintain secure access controls, and adhere to SOC 2 requirements. These audits may involve:

Reviewing access logs and permissions to identify any anomalies or unauthorized access attempts. Verifying that partners are following data security best practices as outlined in this policy. Assessing the effectiveness of security awareness training provided to partner personnel. This policy will be reviewed and updated periodically to reflect changes in the following areas:

- AWS services and access controls.
- Database security best practices.
- Data privacy regulations.
- SOC 2 control standards.

Partners will be notified of any updates to the policy and may be required to undergo additional training or complete a requalification process to ensure continued access.

6 Review and revision for policy

This policy will be reviewed and revised periodically to ensure it remains relevant and effective.