A black and white logo

Description automatically generated

Metropolis Transit corporation

Cloud policy

Contents

[Policy Statement 1](#_Toc149997592)

[Cloud policy 1](#_Toc149997593)

[Owner of the policy 2](#_Toc149997594)

[External Resources Justifying the Policy 2](#_Toc149997595)

[Affirmative Procedure for Compliance 2](#_Toc149997596)

[Frequency of Compliance Audits 3](#_Toc149997597)

[Metric for Compliance 3](#_Toc149997598)

[Procedure for Collecting Compliance Metric 3](#_Toc149997599)

[Responsible Party(ies) for Updating the Policy 4](#_Toc149997600)

[Frequency of Policy Review 4](#_Toc149997601)

[Procedure for Updating the Policy 4](#_Toc149997602)

# **Policy Statement**

* A cloud policy, also known as a cloud computing policy or cloud governance policy, is a **set of rules and best practices created by an organization** to oversee the use of cloud computing resources. It's crucial in the digital age, ensuring efficient, secure, and goal-aligned use of cloud services by businesses and government entities.

## **Cloud policy**

* The policy name, "Cloud Security Policy," clearly identifies **the purpose and scope of the policy**. It establishes the overarching framework for securing cloud resources within the organization. This policy name is intentionally straightforward to ensure that all stakeholders understand its primary focus.
* **Policy ID: CSP-2023**
* The policy ID, **"CSP-2023,"** serves as a unique identifier for the policy. **This ID helps in easy referencing, tracking, and categorization of policies**, especially in large organizations with multiple policies in place. In this case, "CSP" stands for Cloud Security Policy, and "2023" signifies the year of its issuance or the current version.

# **Owner of the policy**

* Chief Information Security Officer (CISO)
* The **CISO holds a critical role** within the organization, being designated as the owner of the Cloud Security Policy. As **the highest-ranking security official**, the CISO is responsible for ensuring the overall security of the organization's information systems, including cloud services.
* The designation of the **CISO** as the Cloud Policy Owner signifies the critical nature of the policy and the pivotal role the **CISO** plays in safeguarding the organization's cloud resources and data. This ensures that there is a clear point of accountability for the policy's creation, enforcement, and adaptability to the changing security landscape and compliance requirements.

# **External Resources Justifying the Policy**

* The **primary reason for the existence of a Cloud Policy** is to **ensure compliance with specific industry regulations and standards**, including but not limited to the Payment **Card Industry Data** Security Standard (**PCI DSS**) and the **Health** Insurance Portability and Accountability Act (**HIPAA**). These regulations are of utmost importance for the following reasons:
* **Customer Trust:** Demonstrating compliance with these regulations fosters **customer trust**. Clients and partners are more likely **to trust an organization that can prove it is taking appropriate measures to protect their data**. Compliance helps maintain a positive reputation and enhances the organization's competitiveness.
* **Legal and Financial Implications:** Non-compliance with industry regulations can lead to severe **legal and financial consequences**. Regulatory bodies can impose fines, penalties, and legal actions against organizations that fail to meet their obligations. Additionally, data breaches resulting from non-compliance can result in costly legal settlements and damage an organization's financial standing.

# **Affirmative Procedure for Compliance**

* All employees and relevant stakeholders must be informed about the Cloud Policy through regular communication and training. This includes providing access to the policy document, **conducting training sessions**, and promoting awareness of its importance.
* All employees and **users must adhere to strict access control measures**. This includes using strong, unique passwords for cloud accounts and implementing **multi-factor authentication** (**MFA**) for enhanced security.
* All cloud resources and services must be **regularly updated and patched to address security vulnerabilities promptly**. Vulnerabilities should be identified through continuous monitoring and scanning.

# **Frequency of Compliance Audits**

* Compliance with the Cloud Policy is critical to maintaining the security of the organization's cloud resources, **safeguarding sensitive data**, and meeting **regulatory requirements.** Regular audits are essential to assess the effectiveness and adherence to the policy.
* Audits will encompass all aspects of the Cloud Policy, including but not limited to:
* Access controls and permissions for cloud services.
* Data encryption and protection measures.
* Incident response procedures.
* Security awareness and training programs.
* Patch management and updates for cloud resources.
* Compliance with industry regulations and standards.

# Metric for Compliance

* Compliance metrics are **quantitative** measures used to assess **the degree of adherence to the Cloud Policy** and associated regulatory requirements. These metrics provide a clear, objective, and quantifiable way to evaluate the **effectiveness of the organization's security controls and practices.**
* The **primary compliance metric used to measure adherence to the Cloud Policy is the "Percentage of Critical Security Controls Implemented**." This metric assesses the extent to which the organization has successfully implemented the critical security controls specified in the policy.
* The "**Percentage** of Critical Security Controls Implemented" is **calculated** as follows:
* Number of critical security controls implemented / Total number of critical security controls specified in the **policy \* 100%.**

# **Procedure for Collecting Compliance Metric**

* Metric collection procedures in the Cloud Policy detail the methods and processes by which compliance metrics, such as the "**Percentage** of Critical Security Controls Implemented," are gathered, assessed, and reported. These procedures ensure that the organization has **a systematic and consistent approach to measuring compliance.**
* Metric collection procedures specify the **data sources** from which compliance data is collected. These sources may **include**, but are not limited to:
* Security tools and software, such as vulnerability scanners, intrusion detection systems, and log analysis solutions.
* Configuration management and monitoring systems for cloud resources.
* Incident response records and incident management tools.
* Records of employee training and awareness programs.
* Access control logs and user authentication records.
* Third-party audit reports (if applicable).

# **Responsible Party(ies) for Updating the Policy**

* The Chief Information Security Officer (**CISO**) **is primarily responsible** for overseeing the security measures related to the organization's data and information systems. They possess expertise in developing and maintaining comprehensive security policies, including those pertaining to **cloud data security.**
* The Chief Information Officer (**CIO**) is responsible for the overall management and strategy of the organization's information technology **infrastructure**, including the **cloud services** utilized. They work closely with the CISO to ensure that the cloud policy aligns with the organization's IT goals and objectives.
* **Together**, these key stakeholders bring their **expertise** and insights to ensure that the cloud policy remains comprehensive, **up-to-date**, and aligned with the organization's overall security and IT strategies.

# **Frequency of Policy Review**

* The cloud policy will be subject to **regular review** to ensure its continued relevance and effectiveness in safeguarding the organization's data stored in the cloud.
* During the review process, **feedback from relevant stakeholders**, including **IT** **teams**, **data owners**, and legal and compliance departments, will be gathered and considered to enhance the policy's comprehensiveness and applicability.

# **Procedure for Updating the Policy**

* The updating process for the cloud policy will be initiated by the Chief Information Security Officer (**CISO**) in collaboration with the Chief Information Officer (**CIO**) and the Chief Security Officer (**CSO**).
* The revised policy will be communicated **to all employees** and relevant stakeholders within the organization, accompanied by **necessary training sessions** or **informational materials** to ensure a smooth transition to the updated guidelines.