SM Cloud Security Policy

This Cloud Security Policy aims to provide comprehensive guidelines for securing cloud-based resources and data, ensuring their confidentiality, integrity, and availability. This policy seeks to protect sensitive information, comply with applicable regulations, and mitigate risks associated with cloud computing. By implementing these guidelines, we strive to maintain a secure cloud environment that supports our platform's operational and strategic goals.

1. Purpose

The purpose of this policy is to safeguard the confidentiality, integrity and availability of data handled through cloud computing services. It establishes a structured framework of responsibilities and measures to ensure compliance with regulatory requirements and adherence to security guidelines in the realm of cloud computing.

2. Scope

This policy pertains to systems managing the data defined in the "2.1. Information Types" section of this document and encompasses all relevant cloud services. It applies to servers, databases and devices regularly used for email, web access or work tasks, covering both new and existing installations. Every user engaging with company IT services is subject to this policy, and its security control requirements are universally applicable to all approved cloud systems.

3. Cloud Service Provider Selection

Understand the Shared Responsibility Model

It's crucial to understand the shared responsibility model between you (the cloud customer) and your cloud service provider (CSP). CSPs like AWS, Azure, and GCP are responsible for the security of the cloud infrastructure, while you are responsible for securing your data, applications, and configurations within that infrastructure.

When selecting cloud service providers (CSPs), the following criteria must be considered:

- **Security Certifications**: CSPs must possess industry-recognized security certifications such as ISO/IEC 27001, SOC 2, or FedRAMP.
- **Data Protection Measures**: Assess the CSP's data protection capabilities, including encryption, access controls, and data redundancy.
- **Compliance**: Ensure that the CSP complies with relevant laws, regulations, and industry standards such as GDPR, HIPAA, and PCI-DSS.
- **Incident Response**: Evaluate the CSP's incident response and disaster recovery procedures.
- **Service Level Agreements (SLAs)**: Review SLAs to ensure they meet our organization's availability and performance requirements.

4. Data Classification and Handling

Data Classification

Data must be classified based on its sensitivity and importance. The following classification levels shall be used:

- **Public**: Data intended for public access.
- **Internal**: Non-sensitive data used within the organization.
- **Confidential**: Sensitive data that requires restricted access.
- **Restricted**: Highly sensitive data that requires strict access controls.

5. Protection of Data in Transit and Data at Rest

A key element of security in cloud environment is the protection of data in transit between you (the end-user) and the provider. This is a two-fold responsibility for both you and the provider. You'll need network protection to prevent the interception of data and encryption to prevent an attacker from reading any data should it be intercepted.

- Enable default encryption: Data at rest is encrypted by default in GCP natively. Ensure that this is enabled across all of your storage services, including Cloud Storage, Persistent Disks, and databases. Use industry-standard encryption algorithms such as AES-256 for data at rest and TLS 1.2 or higher for data in transit.
- Use Customer-Managed Encryption Keys (CMEK): By default, CMEK allows you to manage your own encryption keys for certain GCP services, further securing and managing in-place encryption for your data.
- Cloud Key Management Service Setup: Key creation and import, as well as the management of cryptographic keys integrated into one cloud service and implementation of related cryptographic operations.
- Authenticate data in transit: All your applications should use Transport Layer Security to communicate with GCP services and among themselves. Ensure all your services and APIs are external facing to use HTTPS.
- Implement application-level encryption. More encryption at the application level may be used for highly sensitive data prior to storage in GCP services.

6. Asset Protection

When selecting a cloud service provider, you need to understand the physical location of where your data is stored, processed and managed. This is especially important following the implementation of government and industry regulations like GDPR.
To ensure your assets are protected a good provider will have advanced physical protection in their data center to defend your data from unauthorized access. They will also ensure your data assets are erased before any resources are re-provisioned or disposed of to prevent it from falling into the wrong hands.

7. Visibility and Control

A key factor in security is the ability to see and control your own data. A good service provider will offer you a solution that provides full visibility of your data and who is accessing it, regardless of where it is and where you are.
Your provider should offer activity monitoring so you can discover changes to configuration and security across your ecosystem. As well as supporting compliance with the integration of new and existing solutions.

8. Implement Strong IAM Processes

Identity and Access Management is one of the most important steps in strengthening security in a Google Cloud. IAM serves for users to manage the access to resources and control their operations. The following steps can be followed to ensure the strong IAM implementation:

- Utilize the PoLP strategy: Use the principle of least privilege for all users of the Cloud. The strategy involves granting the least number of permissions to services and people so that they can accomplish their jobs. Review and adjustment of the permissions have to be performed on a regular basis.
- Use strong authentication methods: Make all users and services implement strong passwords, as well as enable MFA for accounts that have full access to the administrative settings.
- Use service accounts: Create and implement service accounts for managing access to applications and controlled systems of the Google Cloud. The account permissions must be minimal to ensure strong security.
- IAM policy audit: Review the IAM policy on a regular basis in order to find out existing and risky permissions and eliminate outdated access.

- Use Cloud Identity for managing users and setting protocols: The Cloud Identity should be used for managing all the users in the whole GCP organization. It will also allow to configure the IAM settings either individually or collectively.

9. Secure the perimeter

Because cloud networks are based on software-defined networking (SDN), there is greater flexibility to implement multilayer security guardrails. You should start with basic segmentation of workloads between different virtual networks and only allow for required communication between them. Additionally, restrict incoming traffic to your applications using network or application layer firewalls.
Attacks such as SQL injections, data exposure, and cross-site scripting are some of the major application security concerns that a web application firewall (WAF) based on OWASP threat detection rules can help detect and protect against. A multilayer distributed denial-of-service (DDoS) defense strategy is unavoidable to protect workloads from organized DDoS attacks in the cloud. All cloud service providers offer DDoS protection tools that can be integrated with your application front end to detect and protect against such attacks.
An efficient firewall that can act as a gatekeeper against incoming threats and malicious attacks should be deployed at your network perimeter. You can deploy cloud-native firewall services or more advanced third-party tools that perform intrusion detection, packet inspection, traffic analysis, and threat detection. You can also opt for a separate intrusion detection system (IDS) or intrusion prevention system (IPS) in the architecture to fortify the perimeter security of your cloud deployments.

10. Secure Your Network

It is important to strengthen GCP's network configuration to make the resources more secure from attacks. The best practices would include:

- Use network segmentation: Use VPCs (Virtual Private Clouds) and subnets to segment the environment and reduce the potential spread of a security breach to other networks and ongoing processes
- Use incorporating firewall rules: Set and maintain strong firewall rules to control the inbound and outbound traffic and allow only those ports and protocols which are needed for the companies they belong to
- Use Google Private Access: In addition to Google Cloud Private Access, which was implemented in the previous step, there are some other services to ensure that some of the VPC networks can access the APIs of the other network residing in some remote places on the Earth.
- VPN or Cloud Interconnect: They enable private connections to be transferred, thus encrypted between on-premises networks and GCP, using Cloud VPN or Cloud Interconnect.
- Google Cloud Armor: It can help secure your applications and services from the threats posed by DDoS attacks and other web-based menaces.

11. Detailed Logging and Monitoring

Logging and monitoring are effective in detecting and responding to security incidents across your GCP environment. Implementation of the following practices:

- Set up Cloud Audit Logs: Enable Cloud Audit Logs for all projects to log administrative activities, data accesses, and system events on your GCP resources.
- Cloud Monitoring Implementation: Use Cloud Monitoring to set up dashboards, warning metrics, and signaling on monitoring resources within GCP. Monitor relevant security indicators and establish notifications for possible security issues.
- Log the Cloud: Log from all your GCP services and applications centrally into Cloud Logging. Optionally, install log sinks to export the logs to external systems for long-term storage and analysis.
- Implement log analysis: You should regularly perform a log check to monitor logs for possible security threats, unusual activities, or violations related to regulations. You might consider using a tool like Cloud Logging with its logs-based metrics to establish custom monitoring based on log events.
- Alerts Sounds: Configurable alerts for critical security events, such as IAM policy changes, changes in firewall rules, or actions such as unusual access patterns. In case the conditions for an alert are satisfied, the said alerts should be delivered to the right on-call staff with enough context to act on it.

- Incident Management
- Your ideal provider will have a pre-planned incident management process in place for common types of attacks. They will be ready to deploy this process in response to any attack.
- There will be a clear contact route to you to report any incidents, with an acceptable timescale and format in place.

12. Regular Patching and Updating of Systems

Keeping systems updated is a key to maintaining a good security posture. A good patching strategy includes:

- Enable auto-updates where feasible for GCP services and resources in such a way that it will always run with the latest and most secure versions.
- Implement patch management: Where the resource cannot be updated automatically, there must, therefore, be a patch routine. This will involve the testing of patches in the non-production environment prior to application in production systems.
- Use Container-Optimized OS: When it comes to containerized workloads, use Container-Optimized OS by Google. It is secure, up-to-date, and optimized to run containers.
- Keep libraries and dependencies up to date: Upgrade libraries, frameworks, and dependencies applied in applications regularly to fix known vulnerabilities.
- Monitor for Security Advisories: Keep abreast of Security Advisories and Vulnerabilities applicable to in-use GCP services and software applications; apply the recommended fixes or mitigations.

13. Implement Strong Backup and Disaster Recovery

GCP Security, Data Protection, and Business Continuity: Take comprehensive measures in backup and disaster recovery.

- Use Cloud Storage for backup: Keep backups of only your most important data and configurations in Cloud Storage to use its durability and availability. Configure Versioning so you can maintain multiple versions of your data.
- Enable Disaster Recovery plans: Design Disaster Recovery plans and put them to test at various times in the GCP environment. Consider leveraging multi-region deployment for critical applications to increase their resilience.
- Snapshot for VM backup: Periodically take a snapshot of your Compute Engine instances and persistent disks for recovery in case of data loss or system failure.
- Database backups: Enable and set up automated backups for managed database services and others not causing the same; implement a standard and frequently followed procedure.
- Backup recovery test: Test the process of backup and recovery regularly to check its expected suitability and familiarize the team with the recovery procedure.

14. Secure your containers

Container security involves both container and orchestration platform protection, and Kubernetes is the solution most often used in the cloud. You will need to create industry standard security baselines for containerized workloads with continuous monitoring and reporting for any deviations.
Organizations require tools that can detect malicious activities in containers — even those that happen during runtime. The necessity of security technologies that enable visibility into container-related activities — as well as the detection and decommissioning of rogue containers — cannot be overstated. With the threat landscape always changing, it's best to employ technologies that leverage advanced AI and machine learning (ML) to detect malware without relying on signatures.

15. Data Loss Prevention (DLP) Measures

Arguably one of the biggest concerns surrounding GCP is with respect to the methods by which sensitive data is safeguarded from either being lost or inadvertently exposed to the wider Internet.

- Use Cloud DLP: Offer Google Cloud's service-based Data Loss Prevention to automatically identify, classify, and protect sensitive data in your GCP environment.

- Data Classification: Develop and implement a data classification scheme that identifies and classifies sensitive information across your organization.
- Set the DLP policies, or the policies around data loss prevention, to be able to spot or redact sensitive information in rest data and data in transit. It could be personal identification data, financial data, or any other private data.
- Monitor data movement: Effective monitoring tools and alerting should be set up in order to determine unusual data access patterns and voluminous data transfers, testing for potential data exfiltration activities.
- Educate users: Train your staff along with guidelines on how to handle sensitive data and how to effectively utilize GCP services securely to ensure no user data gets accidentally exposed.

16. Security Assessments and Vulnerability Testing

Proactive identification and mitigation of security flaws are crucial in sticking to your security posture. Allow for regular security assessments of your system.

- **Do vulnerability scanning**: Regularly scan your GCP environment for vulnerabilities with tools like Cloud Security Command Center or third-party scanning tools for vulnerability.
- **Penetration testing:** Conduct regular penetration testing of your GCP environment to quickly identify potential vulnerabilities that may not be detected by automatic scans. Ensure this is according to Google Cloud's penetration testing policy.
- **Implement security benchmarks:** Use benchmarks like the CIS Google Cloud Platform Foundation Benchmark to check and improve your GCP security configuration.
- **Security setting audits**: Audit and review your security settings, including IAM policies, firewall rules, and encryption settings, at regular intervals.
- **Be responsive to findings:** Set up a procedure through which findings from security assessments and pen tests can be responded to and remediated in a timely manner.

17. Change Management

Successful infiltrations of cloud workloads are most often the result of service misconfigurations or manual configuration errors. You should incorporate cloud security posture management (CSPM) solutions into your architecture to monitor for misconfigurations that could creep into your cloud deployment.
CSPM solutions add value by evaluating your deployments against a set of best practice guidelines. These could be organization-specific standards or aligned to leading security and compliance benchmarks. CSPM solutions provide a security score that quantifies the current state of security of all your workloads in the cloud, with a healthy security score indicating a secure cloud deployment. These tools will also flag any deviations from standard practices so that customers can take the necessary corrective action.

18. Enable security posture visibility

As the cloud landscape expands, the likelihood of breaches remaining unreported increases. Having the right tools in place will help achieve much-needed visibility into your security posture and enable proactive security management.
All leading cloud platforms have an advanced/premium tier of a native CSPM solution that can provide capabilities like detection of data exfiltration, event threats, IAM account hijacks, and cryptomining, to name a few. However, note that these features are often limited to their respective cloud platforms. For hybrid or multi-cloud deployments, it is recommended to incorporate a specialized tool for enabling security posture visibility.

19. Implement a Zero Trust approach

The Zero Trust (aka assume breach) approach is the gold standard for enabling cloud security. It entails not assuming any trust between services, even if they are within the organization's security perimeter.

The main principles of a Zero Trust approach involve segmentation and only allowing for minimal communication between different services in an application. Only authorized identities should be used for this communication. Any communication that happens within an application or with outside resources should be monitored, logged, and analyzed for anomalies. This applies to admin activities as well. Here, you can adopt either native or third-party monitoring and logging tools.

20. Implement an incident response plan

When it comes to cybersecurity, organizations that have an incident response plan in the event of a breach are better equipped to remediate the situation, avoid operational disruptions, and recover any lost data.
Incident response plans are designed to ensure your security teams act in the most efficient manner in the event of an attack. Think of the plan as a remediation framework that should include strict roles and responsibilities so that each team member knows what they have to do in each scenario. Enable notifications so that your team is notified as fast as possible of the breach.

21. Keep data security posture in mind

Data is everywhere, fueling enterprises' growth and innovation. However, its dynamic and uncontrolled nature makes it a prime target for threat actors. With sensitive data flowing across cloud environments and in and out of unmanaged and shadow data stores, the risk of exposure is significant. Employing a data security posture management (DSPM) solution will help you discover, classify, and protect sensitive data — such as personally identifiable information (PII), information subject to Payment Card Industry (PCI) regulations, and protected health information (PHI) — against loss, theft, misuse, and unauthorized access.
DSPM solutions provide security teams with an approach to protecting cloud data by ensuring sensitive and regulated data have the correct security posture, regardless of where the data resides or is moved to.

22. Leverage a cloud detection and response approach

Enterprises are pivoting to use a cloud detection and response (CDR) security approach to help address common challenges pertaining to cloud environments. This approach focuses on threat detection, immediate incident response, and service integrations tailored to aid cloud scalability, innovation, and data sovereignty.

23. Implement cloud security policies

Organizations should define cloud security policies to implement organization-wide restrictions and ensure security. For example,these policies can restrict workload deployment using public IPs, contain east-west traffic flow, or implement monitoring of container workload traffic patterns.
The implementation approach differs among service providers. In Azure, customers can use Azure policies. In Google Cloud, customers can use organizational policies. The advantage of security policies is that they will auto-enforce the compliance standard across the board in cloud deployments.

24. Document and Report

In-depth documentation of security policies and settings enables an organization to track changes and lessons learned. Version control systems make information current for stakeholders, and communication of security metrics regularly promotes awareness and proactive management. Thus, it ensures that all incidences connected to security are recorded and analyzed for the betterment of future responses.

25. Policies and Procedures

Policies and procedures are the foundation of any cloud security program. Reviewing the cloud provider's policies and procedures is critical to ensure they align with the organization's security requirements and compliance regulations. Identifying gaps in policies and procedures will help the organization understand where they need to focus their security efforts.
The policies should address the following:

- Access control and authentication
- Data protection and encryption
- Incident response and disaster recovery
- Auditing and logging
- Monitoring and reporting
- Compliance with relevant regulations and standards

Uncontrolled outbound access
Users must secure access to networks. But they also need to manage data flows from cloud assets. Data Loss Prevention (DLP) tools can track files and data and block unauthorized exfiltration. But restrictions on outbound access are not always applied properly.

Resource Segregation
The first recommendation was segregate resources by projects to create isolation boundaries and ensure that projects contain the resources that are related to the project.
The benchmark automatically assumes resource segregation as stated in the Overview section: "Most of the recommendations provided with this release of the benchmark cover security considerations only at the individual project level and not at the organization level.". [1] Even though there is no recommendation in the categories, there are some for separation of duties.
The CIS Benchmark has the following recommendations related to separation, segmentation and segregation:

- *Ensure That Separation of Duties Is Enforced While Assigning Service Account Related Roles to Users*
- *Ensure That Separation of Duties Is Enforced While Assigning KMS Related Roles to Users*

Although the benchmark already assumes project level segregation, it adds some more recommendations for IAM separation which is also related to the next main area.

26. Enforcement

The IT security team, in collaboration with Human Resources, will enforce the security policy through routine assessments. Employees who fail to comply with the policy or fail testing will have their accounts suspended and they will be required to pass security training for the account to be activated again.

27. Revision History

A revision history provides transparency and accountability by documenting any changes or updates made to the policy over time. Be sure to document each policy modification and its rationale.

Version	Revision Date	Author	Description
1.0	02/01/2023	Blake Parker, Cloud Security Admin	Initial version