Security Policy for Gumsa

1. Gumsa Cloud Security Policy

1. Policy Statement
Gumsa is committed to maintaining the highest level of cloud security to protect our data, systems, and operations. We recognize the importance of robust cybersecurity measures in today's digital landscape. This policy outlines our commitment to implementing best practices in cloud security, mitigating potential risks, and ensuring the integrity and confidentiality of our data.

2. Purpose of Policy
The purpose of this policy is to establish guidelines and procedures for securing our cloud-based systems and data. As we increasingly rely on cloud services for our operations, the need for a comprehensive cloud security policy becomes paramount. This policy aims to protect our organization from potential cybersecurity threats, ensure the integrity and confidentiality of our data, and maintain compliance with relevant regulations and standards.

3. Responsibility and Accountability
- IT Administrators: Responsible for implementing and managing cloud security controls.
- Security Teams: Responsible for conducting security assessments and responding to incidents.
- Employees: Required to follow security policies and report any security concerns.

4. General Requirements for Cloud Security
- Access Control: We will implement Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to ensure only authorized individuals have access to our systems and data.
- Data Protection: We will encrypt all data at rest and in transit and conduct regular backups to prevent data loss.
- Secure Network Configurations: We will use VPNs, Firewalls, and Intrusion Detection Systems to secure our network.
- Compliance Standards: We will maintain compliance with ISO 27001, NIST, and CSA CCM standards.

5. Identified Cybersecurity Risks and Mitigation Strategies

2. Risk 1: Phishing

- Background Research: Phishing is a common cybersecurity threat that involves tricking individuals into revealing sensitive information. It often involves the use of deceptive emails or messages that appear to be from trusted sources.
- Likelihood: High. Phishing is a common method used in cyber-attacks and data breaches.
- Consequences: Phishing attacks can lead to significant financial losses, theft of sensitive information, damage to our reputation, and potential legal implications.
- Mitigation Strategies: We will implement strong data encryption, secure data handling processes, regular system audits, phishing awareness training for employees, and robust access control measures.

3. Risk 2: DDoS Attack

- Background Research: A Distributed Denial of Service (DDoS) attack is an attempt to disrupt the normal functioning of a network, service, or server by overwhelming it with a flood of internet traffic.
- Likelihood: High. DDoS attacks are becoming increasingly common and can affect any organization with an online presence.
- Consequences: DDoS attacks can cause significant financial damage, disrupt our services, damage our reputation, and potentially lead to additional cyber-attacks.
- Mitigation Strategies: We will implement a DDoS response plan, invest in DDoS protection services, regularly update and patch our systems, employ network segmentation, maintain transparency with our clients, and implement load balancing and rate limiting.

6. Summary

Adherence to this policy is mandatory for all employees and contractors. We will conduct regular reviews of this policy to ensure its effectiveness and compliance with evolving cybersecurity standards. Non-compliance with this policy may result in disciplinary action. We are committed to maintaining the highest level of cloud security to protect our data, systems, and operations.