Security Policy for GlasgowUni

2. 1. Policy Statement

GlasgowUni is committed to protecting the confidentiality, integrity, and availability of its data and systems. As part of this commitment, we have developed this Cloud Security Policy to provide clear guidance on the use, management, and security of cloud services within our organization.

3. 2. Purpose of Policy

This policy aims to reduce the risk of cyber threats, protect our intellectual property, personal data, and ensure compliance with relevant laws and regulations. It provides a framework for securely adopting cloud services and outlines the roles, responsibilities, and procedures for managing cloud security risks.

4. 3. Responsibility and Accountability

- IT Administrators: Responsible for implementing and managing cloud security controls, including access controls, data encryption, and secure network configurations.
- Security Teams: Responsible for conducting security assessments, responding to security incidents, and ensuring compliance with this policy and relevant standards.
- Employees: Responsible for adhering to this policy, using cloud services responsibly, and reporting any security concerns or incidents.

5. 4. General Requirements for Cloud Security

- Access Control: Implement Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to limit access to cloud services based on roles and responsibilities.
- Data Protection: Encrypt all data at rest and in transit. Conduct regular backups to ensure data availability and integrity.
- Secure Network Configurations: Use Virtual Private Networks (VPNs), Firewalls, and Intrusion Detection Systems to secure network traffic.
- Compliance Standards: Comply with internationally recognized standards such as ISO 27001, NIST, and CSA CCM.

7. Risk 1: Insider Attack

- Mitigation Strategies: Regular audits, segregation of duties, fraud detection systems, data classification, encryption, strong access control measures, regular system updates, and intrusion detection systems.

8. Risk 2: CyberAttack

- Mitigation Strategies: Regular security audits, penetration testing, cybersecurity insurance, robust access control, data encryption, client education, strong privacy policies, system patching, firewalls, physical security measures, redundancy, and disaster recovery plans.

9. 6. Summary

This Cloud Security Policy outlines GlasgowUni's commitment to protecting its data and systems in the cloud. Adherence to this policy is mandatory for all employees, contractors, and other relevant stakeholders. Regular reviews will be conducted to ensure its effectiveness, and non-compliance may result in disciplinary action.