Security Policy for GlasgowUni

1. GlasgowUni Cloud Security Policy

1. Policy Statement
GlasgowUni is committed to maintaining the highest level of security for our cloud-based systems and data. We recognize the importance of protecting our digital assets and the privacy of our students, staff, and stakeholders. This policy outlines our commitment to implementing robust security measures, maintaining compliance with industry standards, and fostering a culture of cybersecurity awareness within our organization.

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 risk of cyber threats also increases. This policy aims to mitigate these risks by setting clear expectations for cloud security, defining roles and responsibilities, and outlining best practices for data protection, access control, and network configurations. By adhering to this policy, we can protect our organization from potential cyber threats, ensure the integrity and availability of our data, and maintain the trust of our students, staff, and stakeholders.

3. Responsibility and Accountability
- IT Administrators: Responsible for implementing and managing cloud security controls, including access control, data protection, and secure network configurations.
- Security Teams: Responsible for conducting security assessments, responding to security incidents, and ensuring compliance with industry standards.
- Employees: Required to follow this policy and report any security concerns to the IT Administrators or Security Teams.

4. General Requirements for Cloud Security
- Access Control: Implement Role-Based Access Control (RBAC) to limit access to data and systems based on job function. Use Multi-Factor Authentication (MFA) to verify the identity of users.
- Data Protection: Encrypt data at rest and in transit to protect against unauthorized access. Conduct regular backups to ensure data can be recovered in the event of a loss.
- Secure Network Configurations: Use Virtual Private Networks (VPNs), firewalls, and Intrusion Detection Systems (IDS) to secure network traffic and detect potential threats.
- Compliance Standards: Maintain compliance with ISO 27001, NIST, and CSA CCM standards for cloud security.

5. Identified Cybersecurity Risks and Mitigation Strategies

2. Risk 1: Insider Attack

- Background Research: Insider attacks are a significant threat to cybersecurity. These attacks can come from within the organization, from individuals who have access to sensitive information and systems.
- Likelihood: High. Insider attacks are increasingly common, with 68% of organizations reporting vulnerability to such attacks.
- Consequences: Insider attacks can lead to financial losses, damage to assets and

infrastructure, loss of client trust, and disruption of systems.
- Mitigation Strategies: Implement regular audits, segregate duties, use a fraud detection system, classify and encrypt sensitive data, communicate with clients about security practices, restrict administrative privileges, and have an incident response plan in place.

3. Risk 2: CyberAttack

- Background Research: Cyberattacks pose a significant risk to organizations, with potential for significant financial and operational damage.
- Likelihood: High. Cyberattacks are increasingly common and sophisticated, with 68% of organizations reporting vulnerability to such attacks.
- Consequences: Cyberattacks can lead to financial losses, unauthorized access to assets, loss of client trust, disruption of systems, and damage to infrastructure.
- Mitigation Strategies: Conduct regular security audits and penetration testing, implement robust access control and encryption, educate clients about security threats, regularly patch and update systems, and implement physical security measures.

6. Summary

Adherence to this Cloud Security Policy is mandatory for all GlasgowUni employees. Regular reviews of this policy will be conducted to ensure its effectiveness and relevance. Non-compliance with this policy may result in disciplinary action. By adhering to this policy, we can protect our organization from potential cyber threats, ensure the integrity and availability of our data, and maintain the trust of our students, staff, and stakeholders.