Security Policy for GlasgowUni

2. 1. Policy Statement

GlasgowUni is committed to maintaining the security and privacy of all data and information stored in the cloud. We understand the risks associated with cloud storage and are dedicated to implementing comprehensive security measures to mitigate these risks. We strive to comply with all legal and ethical standards in our cloud security practices.

3. 2. Purpose of Policy

The purpose of this policy is to establish guidelines and procedures for securing GlasgowUni's cloud-based data and services. This policy aims to protect the university's information assets from all threats, whether internal or external, deliberate or accidental.

4. 3. Responsibility and Accountability

Responsibility and accountability for enforcing this policy are as follows:
- IT Administrators: Responsible for implementing and managing cloud security controls.
- Security Teams: Responsible for conducting security assessments and responding to security incidents.
- Employees: Required to follow security policies and report any security concerns.

5. 4. General Requirements for Cloud Security

GlasgowUni adheres to the following security practices:
- Access Control: We implement Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) to ensure only authorized individuals have access to our data.
- Data Protection: We encrypt all data at rest and in transit and perform regular backups to prevent data loss.
- Secure Network Configurations: We use VPNs, Firewalls, and Intrusion Detection Systems to secure our network.
- Compliance Standards: We comply with ISO 27001, NIST, and CSA CCM standards.

8. Background Research

: Insider attacks can be highly damaging as they come from individuals with inside knowledge of our systems.

9. Likelihood

: High, as 68% of organizations feel vulnerable to insider attacks.

10. Consequences

: Financial losses, asset damage, client mistrust, system disruption, and infrastructure damage.

11. Mitigation Strategies

: Regular audits, segregation of duties, fraud detection systems, data classification, data encryption, client communication, access control, system updates, and incident response plans.

13. Background Research

: Cyberattacks can lead to unauthorized access to sensitive data and system disruption.

14. Likelihood

: High, as cyberattacks have become increasingly common.

15. Consequences

: Financial losses, asset theft, client mistrust, system disruption, and infrastructure damage.

16. Mitigation Strategies

: Regular security audits, cybersecurity insurance, access control, data encryption, client education, system updates, firewalls, intrusion detection systems, physical security measures, and disaster recovery plans.

17. 6. Summary

This policy outlines GlasgowUni's commitment to cloud security and our strategies for mitigating cybersecurity risks. Adherence to this policy is mandatory for all employees. We will conduct regular reviews to ensure its effectiveness. Non-compliance may result in disciplinary action. We encourage all employees to familiarize themselves with this policy and to report any security concerns to the IT Administrators or Security Teams.