# Cybersecurity Policy and Procedure for RTO Intelligence

## 1. Introduction

- Purpose: Define the scope and objectives of the cybersecurity policy.
- Scope: Applicable to all employees, contractors, and third-party users of the company's IT resources.

## 2. Policy Framework

- Data Protection: Guidelines for protecting sensitive client data, including encryption and access controls.
- Risk Management: Regular risk assessments and mitigation strategies.
- Compliance: Adherence to relevant laws and regulations (e.g., GDPR, HIPAA, SOX).

## 3. User Access Control

- User Authentication: Use of strong, multi-factor authentication for accessing cloud resources.
- Access Privileges: Role-based access controls (RBAC) to ensure minimum necessary access.
- User Responsibility: Training and awareness programs for employees regarding safe access practices.

## 4. Network Security

- Firewalls and Intrusion Prevention: Utilizing advanced firewalls and IPS systems to protect network integrity.
- Network Monitoring: Continuous monitoring of network traffic for unusual or unauthorized activity.
- VPN Usage: Mandatory VPN use for accessing internal resources remotely.

## 5. Data Encryption

- At Rest: Ensuring all sensitive data stored in the cloud is encrypted.
- In Transit: Encryption protocols for data being transmitted over networks.

## 6. Incident Response and Reporting

- Incident Response Plan: A clear plan for responding to cybersecurity incidents.
- Reporting Mechanism: Procedures for reporting breaches or security incidents internally and to relevant authorities.
- Post-Incident Analysis: Conducting thorough analysis post-incident for improvement.

## 7. Cloud Security

- Vendor Management: Assessing and managing the security of cloud service providers.
- Cloud Security Tools: Using tools for real-time monitoring and threat detection in the cloud environment.
- Data Backup: Regular backups of critical data in separate and secure locations.

**8. Physical Security**

- Data Centres: Ensuring physical security of data centres hosting cloud services.
- Device Security: Policies for securing physical devices that access cloud services.

**9. Policy Review and Update**

- Regular Review: Annual review of the cybersecurity policy.
- Updates: Procedure for updating the policy in response to new threats, technologies, and business changes.

**10. Training and Awareness**

- Employee Training: Regular cybersecurity awareness training for all employees.
- Updates on Threats: Regular updates to staff on emerging cybersecurity threats and trends.

**11. Audit and Compliance**

- Internal Audits: Regular internal audits to ensure compliance with the cybersecurity policy.
- External Audits: Cooperation with external audits as required by clients or regulations.

**12. Implementation and Enforcement**

- Implementation: Steps for the implementation of the policy across the organization.
- Enforcement: Disciplinary measures for violations of the cybersecurity policy.

**13. Appendices**

- Glossary: Definitions of key terms used in the policy.
- Contact Information: Contact details for the cybersecurity team and external authorities.

This policy aims to provide comprehensive protection against cyber threats while maintaining the confidentiality, integrity, and availability of data handled by the cloud-based auditing company. Regular reviews and updates are essential to ensure that the policy remains effective and relevant.