Chapter 4 Communications Consulting GmbH
Lange Gasse 65 / 16
1080 Vienna
Austria
T +43 (0)1 353 24 24
F +43 (0)1 2533 033 6860

SECURITY RISK MANAGEMENT PLAN

1. INTRODUCTION

1.1 Purpose
This document outlines the Security Risk Management framework for Chapter 4 to identify, evaluate, and mitigate security risks effectively, ensuring the protection of our assets and the integrity of our operations.

1.2 Scope
This plan encompasses all aspects of our operations, including physical security, digital infrastructure, personnel, data, and third-party interactions.

2. RISK MANAGEMENT FRAMEWORK

2.1 Objectives

- **Protect Assets**: Safeguard physical and digital assets from security threats.
- **Ensure Compliance**: Adhere to legal and regulatory requirements, including data protection laws.
- **Promote Ethical Conduct**: Uphold our commitment to ethical business practices as outlined in our Code of Business Conduct.
- **Sustainability and Environmental Stewardship**: Integrate security measures that support our Sustainability Policy and Environmental Policy.

2.2 Key Stakeholders

- **Security Officer**: Christian Sonnenberg
- **IT Manager**: Manfred Zlamala
- **Compliance Officer**: Severin Heinisch
- **All Employees**

3. RISK ASSESSMENT

3.1 Identify Assets

- **Data**: Customer information, proprietary data, personal data as per our Data Protection Declaration.

Chapter 4 Communications Consulting GmbH
Lange Gasse 65 / 16
1080 Vienna
Austria
T +43 (0)1 353 24 24
F +43 (0)1 2533 033 6860

- **Infrastructure**: IT systems, physical offices, communication networks.
- **Personnel**: Employees, contractors, partners.

3.2 Identify Threats

- **Physical Threats**: Unauthorized access, theft, natural disasters.
- **Cyber Threats**: Malware, phishing, hacking attempts.
- **Operational Threats**: Process failures, human errors.

3.3 Assess Vulnerabilities

- **Physical Security**: Access controls, surveillance systems.
- **Digital Security**: Software updates, network defenses.
- **Human Factors**: Employee training, awareness of Code of General Conduct.

3.4 Evaluate Risks

- **Likelihood**: Probability of threat occurrence.
- **Impact**: Potential damage to assets, reputation, compliance status.

4. RISK MITIGATION STRATEGIES

4.1 Physical Security Measures

- **Access Controls**: Implement secure entry systems.
- **Surveillance**: Install CCTV cameras in critical areas.
- **Environmental Controls**: Ensure compliance with our Environmental Policy.

4.2 Cybersecurity Measures

- **Firewalls and Antivirus**: Deploy and regularly update security software.
- **Data Encryption**: Protect sensitive data in transit and at rest.
- **Regular Audits**: Conduct periodic security assessments.

4.3 Personnel Training

- **Security Awareness Programs**: Educate employees on recognizing and responding to security threats.

Chapter 4 Communications Consulting GmbH
Lange Gasse 65 / 16
1080 Vienna
Austria
T +43 (0)1 353 24 24
F +43 (0)1 2533 033 6860

- **Policy Familiarization**: Ensure all staff are aware of and adhere to our Code of Business Conduct and Human Rights Policy.

4.4 Incident Response Plan

- **Preparation**: Develop and maintain an incident response plan.
- **Detection and Analysis**: Establish procedures for identifying and assessing security incidents.
- **Containment, Eradication, and Recovery**: Define steps to control, eliminate, and recover from incidents.
- **Post-Incident Review**: Analyze incidents to improve future response and update policies accordingly.

5. MONITORING AND REVIEW

5.1 Continuous Monitoring

- **Security Metrics**: Track key performance indicators related to security.
- **Regular Reviews**: Assess the effectiveness of security measures periodically.

5.2 Policy Updates

- **Annual Review**: Update this Security Risk Management Plan annually or as needed to reflect changes in the threat landscape or organizational structure.
- **Stakeholder Involvement**: Engage key stakeholders in the review process to ensure comprehensive coverage.

1st May 2024
Vienna, Austria