Comprehensive Cybersecurity Policy for Global Insurance Firm

1. Introduction

Cyber threats targeting insurance companies have increased dramatically in recent years. This document outlines a multi-tiered cybersecurity framework for our organization, based on the Zero Trust model and cloud-native defense systems.

2. Security Architecture

Our infrastructure uses layered defense:

- Perimeter firewalls and intrusion detection systems
- Micro-segmentation in internal networks
- Secure VPN tunnels for remote access
- Cloud-native access controls

3. Compliance

We comply with the following standards:

- ISO 27001
- SOC 2 Type II
- GDPR and regional privacy acts

4. Risk Heatmap

Risks are categorized by likelihood and business impact. Quarterly reports are generated and reviewed by the Board's Security Committee.

5. Incident Response

An Incident Response Team (IRT) is on-call 24/7. A tested playbook is in place for:

- Phishing

- Ransomware
- Insider threats
- Data exfiltration

6. Training

Employees undergo simulated attacks and quarterly mandatory training. Metrics are used to adjust future awareness campaigns.

7. Monitoring & Audits

SIEM systems continuously collect logs. Red-team audits are performed annually.

This document serves as the cybersecurity blueprint for our global operations.