# Risk Treatment Plan

This guide outlines the steps for implementing the risk treatment plan within the organization.

## Introduction

Following the evaluation, the appropriate risk treatment strategies are developed based on ISO 27001 standards. Treatment options include:

* **Mitigation**: Implementing additional security controls, such as stronger encryption, stricter access controls, and improved incident response procedures.
* **Avoidance**: Altering business processes to remove the risk entirely, such as discontinuing the use of systems with known vulnerabilities.
* **Transfer**: Outsourcing certain functions to third-party vendors or obtaining cybersecurity insurance to transfer the risk.
* **Acceptance**: In cases where the cost of mitigation outweighs the potential impact, the organization may decide to accept the risk but continue monitoring.

# 2. Risk Treatment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Risk Description** | **Risk Treatment Options** | **Risk Treatment Actions** | **Responsible Parties** | **Timeline** |
| 001 | Unauthorized access to sensitive customer and financial data | Mitigate | Implement biometric access controls  Enhance audit logging  Regular security awareness training | IT Security Manager, HR for Training |  |
| 002 | Data breach from external cyberattacks | Mitigate | Strengthen firewall configurations  Upgrade Intrusion Detection Systems (IDS)  Perform regular penetration testing | IT Security Manager, Network Admin |  |
| 003 | Malware infections | Mitigate | Deploy endpoint detection and response (EDR) solutions  Update antivirus software  Implement controls on software installations | IT Security Manager, Endpoint Security Team |  |
| 004 | Insider threats | Mitigate | Implement user activity monitoring  Conduct regular background checks  Provide insider threat awareness training | IT Security Manager, HR Department |  |
| 005 | Physical theft of devices | Mitigate | Enhance physical security controls  Ensure all devices are encrypted  Enable remote wipe capabilities | Physical Security Manager, IT Security Team |  |
| 006 | Non-compliance with data protection regulations |  | Regularly review and update compliance policies  Use automated tools for monitoring compliance  Conduct staff training | Compliance Officer, HR for Training |  |
| 007 | Denial-of-Service (DoS) attacks | Mitigate | Implement Distributed Denial-of-Service (DDoS) protection  Monitor network traffic for anomalies | Network Security Team |  |

This risk treatment plan gives comprehensive idea on addressing identified risks in structured and timely manner ensuring accountability and efficient risk management.