# Risk Management Plan for TechSecure Inc.

**Executive Summary**This document outlines the risk management plan for TechSecure Inc., a medium-sized technology solutions company. The primary goal of this plan is to identify potential risks, assess their impact and likelihood, and develop mitigation strategies to ensure the security and continuity of business operations.  
  
**Introduction**  
TechSecure Inc. is a medium-sized company specializing in technology solutions, including web application hosting, data processing, and client services. The company’s critical assets include customer data, IT infrastructure, and intellectual property. This risk management plan follows the NIST SP 800-30 framework and aims to minimize vulnerabilities and mitigate potential threats.  
  
**Risk Assessment Methodology**  
The risk assessment process follows these key steps:  
1. Asset Identification: Listing critical assets that require protection.  
2. Threat Identification: Identifying external, internal, and environmental threats.  
3. Vulnerability Assessment: Evaluating the vulnerabilities that may expose assets to threats.  
4. Risk Analysis: Calculating the risk level by assessing the likelihood and impact.  
5. Risk Treatment: Developing strategies to mitigate, transfer, avoid, or accept the risks.  
6. Monitoring and Review: Continuously reviewing and updating the risk management plan.  
  
**Asset Identification**

|  |  |  |
| --- | --- | --- |
| Asset Type | Asset Description | Value/Criticality |
| Data | Customer data, employee records | Critical |
| Hardware | Servers, routers, workstations | High |
| Network | LAN, WAN, VPN | High |
| People | IT staff, managers, users | Medium |
| Software | CRM systems, ERP solutions | High |

**Threat Identification and Vulnerability Assessment**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Threat Type | Description | Likelihood | Impact | Risk Level |
| Phishing Attack | Unauthorized access via deceptive emails | 4 | 5 | High |
| Malware Infection | Data corruption from malicious software | 3 | 4 | Medium |
| Insider Threat | Data theft or misuse by employees | 2 | 5 | Medium |
| Power Outage | Disruption of business operations | 3 | 3 | Medium |

**Risk Treatment Plan**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Risk Description | Mitigation Strategy | Responsible Person | Status |
| R1 | Phishing Attack | Implement multi-factor authentication (MFA) | IT Security Manager | Ongoing |
| R2 | Malware Infection | Use updated antivirus software and regular scans | IT Admin | Completed |
| R3 | Insider Threat | Conduct regular employee awareness training | HR Manager | Ongoing |
| R4 | Power Outage | Install uninterruptible power supplies (UPS) | Facility Manager | Planned |

**Monitoring and Review**  
The risk management plan will be reviewed semi-annually to update risks and mitigation measures as needed. Any new threats will be assessed and added to the plan.  
  
**Conclusion**  
This risk management plan provides a structured approach to identifying, analyzing, and mitigating risks that could affect TechSecure Inc. By implementing the recommended controls and continuously monitoring for emerging threats, the organization can enhance its resilience and maintain operational continuity.