Risk Assessment and Prioritization Report

1. Executive Summary

This report presents the findings of a risk assessment conducted for the organization. It identifies critical risks to operations and assets, evaluates their impact and likelihood, and proposes prioritization for mitigation.

2. Methodology

1. Asset identification
2. Threat and vulnerability analysis
3. Risk evaluation (Likelihood & Impact matrix)
4. Risk prioritization
5. Recommendations for mitigation

3. Risk Assessment Summary

Risk ID	Description	Likelihood	Impact	Risk Level	Priority
R1	Phishing attack leading to data breach	High	Severe	Critical	1
R2	Unpatched software vulnerabilities	Medium	High	High	2
R3	Physical theft of devices	Low	Medium	Moderate	3
R4	Natural disaster (e.g., fire, flood)	Low	Severe	High	4

4. Recommendations

- Enhance employee training on phishing awareness (R1)
- Implement regular software updates and patch management (R2)
- Introduce device encryption and secure storage policies (R3)
- Develop and test disaster recovery plans (R4)

5. Conclusion

Addressing the highest-ranked risks will significantly reduce the organization's exposure to security breaches and operational disruptions. Continuous monitoring and periodic reassessment are recommended.

Important Notes

- This assessment reflects risks as of the report date; risks may evolve over time.
- The prioritization is based on current organizational context and available information.
- Mitigation strategies should be reviewed and updated regularly.
- Stakeholder involvement is crucial for effective risk management.