Cybersecurity Diagnostic Report

Overall Score:

300/500 (60.0%)

Category Breakdown:

Access Control: 65/80 (81.25%)

Data Protection: 50/70 (71.43%)

Employee Awareness and Training: 40/70 (57.14%)

Governance and Policies: 25/70 (35.71%)

Incident Response and Recovery: 50/70 (71.43%)

Network Security: 50/90 (55.56%)

Third-Party Risk Management: 20/50 (40.0%)

Recommendations:

Focus on strengthening key areas: Governance and Policies, Third-Party Risk Management.

Suggested Tools for Improvement:

Governance and Policies: NIST Cybersecurity Framework, CIS Controls

Third-Party Risk Management: OneTrust, Prevalent

Answers Summary:

Q1: Yes

Q2: Yes, but informal

Q3: Occasionally

Q4: No

Q5: No

Q6: Yes

Q7: Not Sure

Q8: No

Q9: Yes, monthly or more frequently

Q10: No

Q11: Yes

Q12: Yes, for all systems

Q13: Yes, but delayed

Q14: Partially

Q15: Yes, real-time monitoring

Q16: Yes, but weak encryption

Q17: Yes, always

Q18: Yes, but not tested

Q19: Yes, with offsite storage

Q20: No

Q21: No

Q22: Yes, enforced through contracts

Q23: No

Q24: Yes, but less frequently

Q25: Yes, with mandatory updates

Q26: Yes, strictly enforced

Q27: Yes, enforced rigorously

Q28: Yes, with MFA enabled

Q29: Partially enforced

Q30: Yes, but rarely audited

Q31: Yes, with cybersecurity measures included

Q32: Yes, within the first month

Q33: Yes, but less frequently

Q34: Yes, with mandatory reporting

Q35: Yes, but infrequently

Q36: Yes, fully automated

Q37: Yes, but without detailed analysis

Q38: No, but considered

Q39: No

Q40: No

Q41: Yes, strictly enforced

Q42: Partially implemented

Q43: Yes, with real-time updates

Q44: Yes, quarterly or more frequently

Q45: Yes, at least annually

Q46: Yes, but infrequently

Q47: Yes, but without compliance checks

Q48: No

Q49: No

Q50: Yes, but not integrated