Cybersecurity Diagnostic Report

Overall Score:

235/500 (47.0%)

Category Breakdown:

Access Control: 25/80 (31.25%)

Data Protection: 50/70 (71.43%)

Employee Awareness and Training: 30/70 (42.86%)

Governance and Policies: 25/70 (35.71%)

Incident Response and Recovery: 35/70 (50.0%)

Network Security: 40/90 (44.44%)

Third-Party Risk Management: 30/50 (60.0%)

Recommendations:

Focus on strengthening key areas: Governance and Policies, Network Security, Access Control, Employee Awareness and Training.

Suggested Tools for Improvement:

Access Control: Okta, Microsoft Entra ID (Azure AD)

Employee Awareness and Training: KnowBe4, Infosec IQ

Governance and Policies: NIST Cybersecurity Framework, CIS Controls

Network Security: Snort, Wireshark

Answers Summary:

Q1: No

Q2: Yes, but informal

Q3: No

Q4: Yes, ongoing and mandatory

Q5: No

Q6: No

Q7: Not Sure

Q8: Yes, continuously

Q9: Yes, but less frequently

Q10: No

Q11: No, shared accounts are used

Q12: No

Q13: Yes, within 24 hours

Q14: Partially

Q15: No

Q16: No

Q17: Yes, always

Q18: Yes, tested regularly

Q19: No

Q20: Yes, annually or more frequently

Q21: Yes, annually

Q22: Partially

Q23: Yes, but superficially

Q24: Yes, but less frequently

Q25: Yes, with mandatory updates

Q26: Yes, strictly enforced

Q27: Partially enforced

Q28: Yes, but without MFA

Q29: Partially enforced

Q30: No

Q31: No

Q32: No

Q33: Yes, but less frequently

Q34: Yes, but voluntary

Q35: Yes, but infrequently

Q36: Yes, partially automated

Q37: Yes, but without detailed analysis

Q38: No

Q39: Yes, but loosely followed

Q40: No

Q41: Yes, strictly enforced

Q42: Yes, with encryption and access controls

Q43: No

Q44: Yes, annually

Q45: No

Q46: Yes, annually or more frequently

Q47: Yes, with regular compliance checks

Q48: No

Q49: Yes, before adoption and periodically

Q50: Yes, integrated with response tools