REPORT AND RECOMMENDATION

REPORT;

The security audit revealed that the organization operates without enforcing the principle of least privilege, lacks a formal disaster recovery plan, has no data-backup strategy in place, maintains no documented password policy and does not use any intrusion detection system collectively creating an environment with weak access controls, no resilience against data loss, ineffective authentication practices and zero visibility into unauthorized or suspicious activities

RECOMMENDATION;

To address the identified security weaknesses, it is recommended that the organization implement a least-privilege access model by reviewing all user accounts and restricting permissions according to job responsibilities. Access should be granted only where necessary, and elevated privileges should be approved, monitored, and removed when no longer required.

It is also necessary to establish a strong password policy that enforces minimum password length, complexity, periodic updates, and protection against password reuse. Implementing multi-factor authentication (MFA), especially for administrative accounts, would provide an additional layer of protection. To improve visibility and threat detection, the organization should deploy an Intrusion Detection System or a similar monitoring tool that can analyze network traffic and alert security personnel to suspicious activity. Centralized logging and regular security reviews should accompany this system to ensure threats are identified and addressed promptly.

By implementing these recommendations, the organization will significantly reduce its exposure to cyber risks, strengthen its security posture, and improve its readiness to detect, prevent, and recover from potential incidents.