**Cybersecurity Self-Audit Report**

**FE/24/6475710187**

Objective: This report details an audit of my personal cybersecurity practices, identifying strengths, weaknesses, and an improvement plan to enhance my digital security posture.

Findings

1. Passwords and Authentication
   * Some passwords are reused across multiple accounts and are not regularly updated.
   * Multi-factor authentication (MFA) is enabled for critical accounts, but a password manager is not in use.
   * Risk Level: High (Increased risk of credential compromise.)
2. Device Security
   * Antivirus software and firewalls are active, but regular security checks are not consistently performed.
   * Updates for the operating system and software are installed, but sometimes delayed.
   * Risk Level: Medium (Potential exposure to malware and security vulnerabilities.)
3. Social Media Privacy
   * Privacy settings are configured on some accounts, but not all are reviewed regularly.
   * Some personal information is publicly visible, creating potential risks.
   * Risk Level: Medium (Increased exposure to social engineering and identity theft.)
4. Email Practices
   * Awareness of phishing threats exists, but sophisticated attacks still pose a challenge.
   * Suspicious emails and links are generally avoided, but verification practices need improvement.
   * Risk Level: Low to Medium (Possible vulnerability to phishing and email scams.)
5. Data Backup and Encryption
   * Backups are performed manually but could be automated.
   * Data is not encrypted, creating a security risk if devices are compromised.
   * Risk Level: High (Potential data loss or exposure in case of a breach.)

Improvement Plan

1. Password Security
   * Implement a password manager to generate and store unique passwords.
   * Enforce regular password updates across all critical accounts.
2. Device Protection
   * Automate security scans and updates to ensure system protection.
   * Regularly check and optimize firewall settings.
3. Privacy Enhancements
   * Conduct a thorough review of social media privacy settings and update them monthly.
   * Reduce the amount of publicly shared personal information.
4. Email Security Awareness
   * Take additional training on phishing detection and email verification methods.
   * Enable advanced spam filtering and security tools for email accounts.
5. Data Protection
   * Encrypt sensitive data and files to prevent unauthorized access.
   * Automate data backups to a secure, encrypted cloud or external storage.

Monitoring and Review

* Implement a cybersecurity self-audit every six months to assess progress.
* Set up security alerts and periodic training to stay informed about emerging threats.
* Track improvements using security tools and updated best practices.

Conclusion By implementing the outlined security improvements, I aim to enhance my digital safety and reduce potential vulnerabilities. Regular audits and proactive measures will ensure long-term cybersecurity resilience.