Security Audit – Cyber Security Policy

Updated By: Joshua Mordecai (IT Manager – STRUMIS Ltd)

Updated On: 3rd January 2024 with amendments on 18th April 2024

Contents

Introduction

At STRUMIS Ltd & Trading Subsidiaries, we recognize the critical importance of cybersecurity in safeguarding our assets, protecting our customers' data, and maintaining the trust of our stakeholders. This Cyber Security Policy outlines our commitment to maintaining a robust cybersecurity posture and provides guidelines for all employees, contractors, and stakeholders to ensure the security of our digital assets.

Scope

This policy applies to all employees, contractors, vendors, and partners of STRUMIS Ltd who have access to the organization's information systems, networks, and data, regardless of location or device used.

Management Responsibilities

Management is responsible for establishing and enforcing cybersecurity policies, procedures, and standards.

Management shall allocate appropriate resources to implement and maintain cybersecurity measures.

Management will regularly review and update the cybersecurity policy to address evolving threats and technologies.

Employee Responsibilities

All employees are responsible for adhering to cybersecurity policies, procedures, and guidelines.

Employees must report any suspected or actual security incidents or vulnerabilities to the designated STRUMIS IT team.

Employees should undergo regular cybersecurity awareness training to stay informed about current threats and best practices. This is performed on an ad hoc basis as required.

Access Control

Access to sensitive systems and data shall be granted on a need-to-know basis.

Strong authentication mechanisms, such as passwords, multi-factor authentication (MFA), and biometric verification, shall be implemented where appropriate.

Access privileges shall be regularly reviewed and updated based on job roles and responsibilities.

Data Protection

All sensitive data, including customer information, intellectual property, and financial data, shall be encrypted both in transit and at rest.

Data classification policies shall be established to identify and protect data according to its sensitivity level.

Regular data backups shall be performed to ensure data integrity and availability in the event of a cyber incident.

Network Security

Firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation shall be implemented to protect against unauthorized access and malicious activities.

Secure configurations and regular vulnerability assessments shall be conducted on all network devices and systems.

Wireless networks shall be secured using encryption and strong authentication mechanisms.

Endpoint Security

All endpoints, including desktops, laptops, mobile devices, and servers, shall be equipped with up-to-date antivirus/anti-malware software.

Endpoint encryption shall be enforced to protect data stored on devices from unauthorized access.

Remote access to corporate networks shall be secured using virtual private networks (VPNs) and encrypted communication protocols.

Incident Response

An incident response plan shall be established to effectively detect, respond to, and recover from cybersecurity incidents.

Incident response roles and responsibilities shall be clearly defined, and all employees shall be trained on incident reporting procedures.

Post-incident reviews shall be conducted to identify lessons learned and areas for improvement.

Compliance

STRUMIS Ltd & Trading Subsidiaries shall comply with all relevant laws, regulations, and industry standards pertaining to cybersecurity, privacy, and data protection.

Regular audits and assessments shall be conducted to ensure compliance with internal policies as well as external requirements.

Enforcement

Violations of this Cyber Security Policy may result in disciplinary action and legal action if warranted.

Review and Revision

This Cyber Security Policy shall be reviewed annually and updated as necessary to address emerging threats, technological advancements, and changes in business requirements.

Conclusion

By adhering to this Cyber Security Policy, we demonstrate our commitment to protecting the confidentiality, integrity, and availability of STRUMIS Ltd's information assets. Every employee and stakeholder has a role to play in maintaining a secure and resilient cybersecurity posture. Together, we can mitigate risks and safeguard our organization against cyber threats.

Please see Pentest records for up to date information on current practices and reviews within STRUMIS Ltd

Sincerely,

Joshua Thomas Mordecai

IT Manager

STRUMIS Limited