Cyber Security Policy

1. Purpose

The purpose of this Cyber Security Policy is to protect the confidentiality, integrity, and availability of the SEA's information, systems, and data. This policy establishes the minimum security requirements for all employees, contractors, and third parties who access SEA information or systems.

2. Roles and Responsibilities

Management is responsible for:

- Providing appropriate resources for cybersecurity.
- Ensuring compliance with this policy.
- Reviewing cybersecurity risks regularly.

Employees are responsible for:

- Following this policy and associated procedures.
- Protecting SEA information.
- Reporting suspected security incidents immediately.
- Completing required security awareness training.

IT Administrator / Security Lead is responsible for:

- Implementing security controls.
- Monitoring systems and networks.
- Managing access controls.
- Responding to security incidents.

4. Access Control

- Access to SEA systems shall be granted on a "least privilege" basis.
- User accounts must be unique and must not be shared.
- Multi-factor authentication (MFA) shall be enabled for email, cloud services, VPNs, and administrative accounts.
- Access rights shall be reviewed at least annually and whenever personnel change roles.
- Accounts shall be disabled promptly when employment ends.

5. Password Requirements

Passwords must:

- Be at least 12 characters long.
- Be unique and not reused across systems.
- Not be shared with any person.
- Be stored only in approved password management software.

Default passwords must be changed before systems are deployed.

6. Device Security

- SEA devices must be protected by passwords or biometric authentication.
- Devices must automatically lock after 10 minutes of inactivity.
- Anti-malware protection must be installed and maintained.
- Operating systems and applications must be kept up to date.
- Unauthorized software installation is prohibited.

7. Email and Internet Usage

Employees must:

- Exercise caution when opening email attachments or links.
- Verify unusual requests involving payments, banking details, or sensitive information.
- Report suspected phishing emails immediately.
- Use SEA systems for legitimate business purposes only.

Access to malicious, illegal, or inappropriate websites may be restricted.

8. Data Protection

Information shall be classified according to its sensitivity:

Public

- Information approved for public release.

Internal

- Information intended for SEA use only.

Confidential

- Sensitive business, customer, financial, employee, or intellectual property information.

Confidential information must:

- Be shared only with authorized personnel.
- Be stored in approved locations.
- Be encrypted when transmitted externally.

9. Remote Working

Employees must:

- Use SEA-approved devices whenever possible.
- Connect through approved secure services.
- Avoid using public Wi-Fi without VPN protection.
- Protect SEA information from unauthorized viewing or access.

10. Backup and Recovery

- Critical business data shall be backed up regularly.
- Backups shall be protected from unauthorized access.
- Recovery procedures shall be tested periodically.
- Backup copies shall be maintained separately from production systems.

11. Third-Party Security

Third-party suppliers with access to SEA information or systems must:

- Meet appropriate security requirements.
- Protect SEA data according to contractual obligations.
- Notify the SEA of any security incidents affecting SEA information.

12. Security Incident Reporting

Employees must immediately report:

- Suspected phishing attempts.
- Malware infections.
- Lost or stolen devices.
- Unauthorized access attempts.
- Data breaches or suspected data breaches.

Reports should be made to the IT Administrator or designated Security Lead without delay.

13. Security Awareness Training

All employees shall:

- Complete cybersecurity awareness training upon joining.
- Participate in annual refresher training.
- Complete additional training when required.

14. Monitoring and Compliance

SEA reserves the right to monitor its systems, networks, and information assets to:

- Detect security threats.
- Investigate incidents.
- Ensure compliance with this policy.

Any violation of this policy may result in disciplinary action up to and including termination of employment.

15. Policy Review

This policy shall be reviewed annually or whenever significant changes occur in cyber security technology, legislation, or SEA operations.

Frantisek Plachy
Managing Director
SEA Enterprises a.s.

5 July 2026

0626-01