2026-02-18

CYBER SECURITY POLICY

Purpose:

This policy defines the principles and measures implemented by Nova Åkeri AB to protect company information, IT systems, and personal data from unauthorized access, loss, or misuse.

Scope:

This policy applies to all employees, subcontractors, and any individuals with access to company systems or data.

1. Information Security Principles

- Company information must be handled securely and only accessed by authorized personnel.
- Personal data must be processed in accordance with GDPR and company policies.
- Confidential information must not be shared with unauthorized persons.

2. Access and Password Management

- Employees must use strong passwords and keep them confidential.
- Access to systems is granted based on job responsibilities.
- Accounts must not be shared between employees.

3. Use of IT Equipment

- Company devices must be used for business purposes only.
- Software must not be installed without authorization.
- Employees must avoid accessing suspicious links or downloading unknown files.

4. Data Protection and Storage

- Documents containing personal or sensitive data must be stored securely.
- Data must not be transferred to unauthorized external devices or platforms.
- Backup procedures must be followed where applicable.

5. Incident and Breach Reporting

- Any suspected cyber security incident (e.g. phishing, hacking attempt, data loss) must be reported immediately to management.
- Examples include:
- Suspicious emails or links
- Unauthorized system access
- Lost or stolen devices
- Accidental sharing of sensitive information

6. Breach Handling Procedure

- Management will assess the incident and take immediate action to limit damage.
- Access may be restricted or systems temporarily shut down if necessary.
- Affected data and systems will be secured and investigated.
- If personal data is affected, the incident will be handled in accordance with GDPR requirements, including notification to authorities where required.

7. Responsibility

- All employees are responsible for following this policy.
- The Managing Director is responsible for overseeing cyber security and incident response.