INFORMATION SECURITY POLICY

Purpose
This policy establishes a framework to secure Autostop's information assets, ensuring the confidentiality, integrity, and availability of data while adhering to applicable regulatory requirements.

Scope
This policy applies to:

- All employees, contractors, and third-party service providers.
- All systems, devices, and data owned or managed by Autostop.

Commitment to Security
Autostop is committed to protecting its information assets against unauthorized access, disclosure, alteration, destruction, or disruption.

Roles and Responsibilities

- **Information Security Officer (ISO):** Leads the security strategy and oversees implementation.
- **Employees:** Follow security protocols and promptly report security incidents.
- **IT Team:** Implement and maintain technical security controls.
- **Third-Party Vendors:** Comply with Autostop’s security requirements and policies.

Key Security Principles

- **Access Control:** Data access is restricted to authorized individuals based on their roles and responsibilities.
- **Data Classification:** Information is categorized by sensitivity (e.g., Public, Internal, Confidential).
- **Incident Response:** A defined process is in place for detecting, reporting, and resolving security incidents.
- **Risk Assessment:** Risks to information assets are periodically evaluated, with an annual review.
- **Physical Security:** Measures are implemented to safeguard information systems and data.
- **Continuous Monitoring:** Systems are monitored in real-time to detect anomalous activity.
- **Threat Intelligence:** Stay updated on emerging risks using threat intelligence services

Acceptable Use of Resources

- Do not share passwords.
- Use company-provided devices strictly for authorized purposes.
- Avoid downloading unauthorized software.
- Personal devices must meet company security standards if used at ,or for work (BYOD policy).

Handling Personal Data

- Personal data must be processed in accordance with legal requirements (e.g., GDPR).
- Sensitive data must be encrypted both at rest and during transmission.
- Define retention periods for different types of data (e.g., HR, financial, customer).
- Use secure disposal methods for physical and digital data (e.g., shredding, secure wiping).

Supply Chain Security

- Implement and enforce security standards for third-party vendors and contractors.
- Require regular audits or compliance certifications from suppliers handling sensitive data.

Incident Reporting

- All incidents must be reported to the ISO within 24 hours.
- Prompt investigations will be conducted to mitigate potential damage.

Training and Awareness

- Annual mandatory security training is required for all employees.
- Regular updates will be provided on emerging security threats.
- Conduct regular simulated phishing tests to evaluate awareness.

Disaster Recovery and Business Continuity

- Ensure regular data backups and secure storage.
- Establish timelines for resuming operations after incidents.
- Conduct regular tests of disaster recovery plans.

INFORMATION SECURITY POLICY

Regular Penetration Testing

- Conduct regular penetration testing and vulnerability assessments.
- Document and address identified vulnerabilities promptly.

Compliance and Audits

- The policy complies with TISAX requirements.
- Regular security audits will be conducted to ensure adherence.

Policy Enforcement and Metrics

- Define metrics to track policy adherence (e.g., incidents reported, training completion rates).
- Review these metrics regularly to refine the policy as needed.

Policy Review and Updates

- The policy will be reviewed annually or when significant regulatory or technological changes occur.
- Relevant updates will be communicated to employees and external partners.

Consequences of Non-Compliance
Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment or legal action where applicable.

Acknowledgment
Employees and external partners are required to stay informed of any changes relevant to them and acknowledge their responsibilities under this policy.

For Detailed Version of this policy please refer to **Document DO 5.IT.000.002 Detailed Information Security Policy**

Policy reviwed and approved by:

CEO
Panayiotis Pitsikos

CFO
Lazar Stojković

CSO
Ivan Sakellariou

COO
Branko Vasić

Information Security Officer
Nikola Cvetković

Plant Manager
Igor Rajković

Quality Manager
Nenad Vulić

Approval date:
Leskovac, 30.01.2025.

PROMENA/REVIZIJA			
A/A	**Datum/Date**	**Strana/Page**	**Razlog/Reason**
A1	24.12.2024	/	Initial document

Dokument/List: **ORIGINAL** ✓ **KOPIJA/COPY** ☐

	Ime i Prezime, Pozicija / Name and Surname, Title:	**Potpis / Signature:**
Uradio / Created by:	Nikola Cvetković, ISO	
Proverio / Checked by:	Igor Rajković, Menadžer fabrike	
Odobrio / Approved by:	Panayiotis Pitsikos, CEO	