Variscite Information Security Policy

1. Management commitment

Variscite's management regards the protection of information - in terms of integrity, availability, and confidentiality - as a supreme value.

Company management commits to:

- Establish measurable objectives in accordance with risk assessment (pursuant to section 6.1 of the ISO/IEC 27001:2022 standard).
- Continuous improvement of the Information Security Management System (ISMS) (section 10.1).
- Conduct training and raise awareness among all employees (section A.6.2).
- Implement a risk management process for identifying, controlling, minimizing, and preventing failures (section 6.1).
- Plan changes in a systematic and controlled manner as part of the ISMS (section 6.3).
- Address nonconformities through corrective and preventive actions (section 10.2).
- Allocate needed resources to meet the requirements of the ISO/IEC 27001 standard.
- Validate regulatory requirements and customer demands.

2. Organizational Responsibility

- **Chief Information Security Officer** – Responsible for the ongoing management of information security policy, controls, and processes (section A.6.1).
- **Organization employees** – Committed to maintaining confidentiality and information security, particularly technological information, intellectual property, and customer data and details (section A.6.6).

3. Main Implementation Areas

3.1. Log Security

- Permission management according to the Least Privilege principle (section A.8.2).
- Access control, log documentation, two-factor authentication (2FA).

3.2. Human Resource Security

- Onboarding processes, training, revocation of permissions upon termination of employment (sections A.6.2, A.6.3).

3.3. Procurement and Suppliers

- NDAs and periodic reviews for suppliers (section A.6.6).

3.4. Backups

- Secure cloud backup, recovery according to information sensitivity (section A.8.13).

3.5. Access Control

- Connection monitoring, automatic blocking in case of irregularities (section A.8.2).

3.6. Encryption

- Encryption of source code, technological documents, backups, communications, and APIs (section A.8.24).

3.7. Remote Work

- Use of VPN, 2FA, BYOD policy with encryption and connection management (section A.6.1.5).

3.8. Mobile Computer Security

- Assigning authorized role holders, controls to prevent information loss (section A.8.3).

4. Continuous Review and Improvement

- Internal audits and periodic reviews (sections 9.2.1, 9.2.2).
- Management reviews, including stakeholder inputs (sections 9.3.2, 9.3.3).
- Update the policy according to findings and regulatory changes.
- Annual policy review.
- Internal communication to all employees.
- Availability to relevant stakeholders.

Ohad Yaniv – CEO

Rafi Mandler – Quality Manager