INFORMATION SECURITY POLICY

Information security is essential for VOGT in protecting its information assets, the privacy of its customers, employees, and suppliers, and the continuity of its operations. This policy establishes guidelines and measures to ensure a secure environment, in accordance with security best practices (ISO 27001).

OBJECTIVES

- ✓ Protect the confidentiality, integrity, and availability of information.
- ✓ Minimize risks associated with information security.
- ✓ Ensure business continuity in the event of potential security incidents.

This policy applies to all employees, contractors, suppliers, and third parties who have access to VOGT's information systems and assets. It extends to all company devices, applications, networks, and databases.

The key principles that will guide information security are:

CONFIDENTIALITY Ensure that information is only accessible to authorized persons.

INTEGRITY Protect the accuracy and completeness of information, preventing unauthorized modifications.

AVAILABILITY Ensure that information is accessible to authorized users when they need it.

VOGT will conduct an ongoing assessment of the risks associated with information security. Based on this assessment, appropriate controls will be implemented to mitigate the identified risks. Risk management will be reviewed regularly and adjusted to technological, operational, and regulatory changes.

INFORMATION SECURITY POLICY

ACCESS CONTROL

AUTHENTICATION AND AUTHORIZATION: Access to company systems will be controlled by robust authentication mechanisms, such as secure passwords and multi-factor authentication (MFA), depending on the feasibility of each software program.

PRINCIPLE OF LEAST PRIVILEGE: Employees will only have access to the information and systems necessary to perform their work.

PERIODIC REVIEW: Access permissions will be reviewed regularly to ensure they remain appropriate.

The company's technological resources (such as computers, networks, applications, and mobile devices) must be used solely for work purposes and within the parameters established by VOGT. Misuse, such as accessing non-work-related content, is prohibited.

GENERAL SAFETY MEASURES

1. Antivirus and protection software: All company devices will be protected with up-to-date antivirus software and threat detection tools.
2. Encryption: Sensitive data will be encrypted to protect it and prevent it from being accessed or altered by unauthorized persons, either while it is stored or while it is being transmitted over the network.
3. Backup: Regular backups of critical data will be made and stored securely in protected locations.
4. Business Continuity and Disaster Recovery Plan: The organization will establish and maintain a business continuity plan (BCP) and a disaster recovery plan (DRP) to ensure the availability of critical information and the ability to recover from potential disruptions.

INFORMATION SECURITY POLICY

SECURITY INCIDENT MANAGEMENT

In the event of a security incident, such as a data breach or cyberattack, employees must immediately report it to the information security team. A thorough investigation will be conducted and corrective measures will be implemented to prevent the incident from recurring.

TRAINING AND AWARENESS

The company will provide ongoing training to all employees on information security, with the aim of raising awareness of risks and best practices. Employees will also be periodically evaluated on their compliance with this policy.

CONTINUOUS IMPROVEMENT

Information security is an ongoing process. VOGT is committed to regularly reviewing and improving its security policies and controls, based on internal audits, incident analysis, and technological advances.

PENALTIES FOR NON-COMPLIANCE

Failure to comply with this policy may result in disciplinary measures, ranging from warnings to termination of employment, depending on the severity of the violation.

Alberto Campos V.
General Manager