Autohellas

	IT POLICIES	
Autohellas	IT Security Policy	Date of first issuance: 25/09/2023

IT Security Policy

1. Purpose

The purpose of this IT security policy is to outline the security measures and practices to protect Autohellas information technology systems, data, and resources from unauthorized access, damage, disclosure, or alteration. This policy is designed to ensure the confidentiality, integrity, and availability of our IT assets.

2. Scope

This policy applies to all employees, contractors, and any other individuals who have access to Autohellas IT resources, whether on-site or remote.

3. Security Responsibilities

3.1. Management Responsibilities

The senior management team is responsible for:

- Defining and maintaining the IT security policy.
- Allocating necessary resources for implementing security measures.
- Ensuring compliance with applicable laws and regulations.

3.2. IT Department Responsibilities

The IT Department is responsible for:

- Designing, implementing, and maintaining IT security measures.
- Regularly monitoring and assessing IT security risks.
- Responding to and managing security incidents.

4. Data Access Control

Access to IT resources is granted based on job roles and responsibilities.
Users must use strong, unique passwords and should change them regularly.
Access to sensitive data and systems must be limited to authorized personnel.

5. Data Protection

5.1. Data Classification

Data should be classified based on its sensitivity and appropriate controls should be applied accordingly.

5.2. Encryption

Sensitive data in transit and at rest must be encrypted using approved encryption standards.

6. Network Security

6.1. Firewalls, Intrusion Detection and Prevention

Firewalls, intrusion detection and prevention systems should be used to protect the network from unauthorized access and malicious activity.

6.2. Updates and Patch Management

All software and hardware should be regularly updated and patched to address vulnerabilities.

7. Data Backups

- Regular data backups must be conducted and stored securely.
- Data restoration procedures should be tested periodically to ensure data recovery.

8. Incident Response

8.1. Reporting Incidents

All security incidents must be promptly reported to the IT Department.

8.2. Incident Response

Autohellas has an incident response plan in place, which includes procedures for identifying, managing and mitigating security incidents.

9. Training and Awareness

All employees should receive security awareness training to understand and recognize security threats and best practices.

10. Non-Compliance

Violations of this security policy may result in disciplinary action, including temporary or permanent suspension of IT system access.

11. Policy Review

This policy will be reviewed regularly to ensure its effectiveness and compliance with evolving threats and regulations.

Autohellas is committed to maintaining the security and integrity of its IT assets. All employees and authorized individuals are expected to adhere to this policy to protect our organization's information technology resources.