Cyber Security Policy Statement – GKOUSKOS DIMITRIOS

Information is a critical company asset. Information is comparable with other assets in that there is a value in using it and a cost in obtaining it. Nonetheless, unlike many other assets, the value accurate and reliable information appreciates over time as opposed to depreciating. The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, Gkouskos Dimitrios has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Additionally, in this policy, the main objective followed by Gkouskos Dimitrios, is to maintain and establish effective and adequate security measures for users, in order to ensure that the integrity, operational availability of information and the confidentiality is not compromised.

Sensitive information must therefore be protected from unauthorized modification, use, disclosure, access, delay or destruction in service.

Each employee has a responsibility and duty to comply with the information protection procedures and policies described in this statement.

Purpose

The purpose of this policy is to (a) protect Gkouskos Dimitrios' infrastructure and data, (b) outline the guidelines and protocols that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

Scope

This policy applies to all of Gkouskos Dimitrios' employees (permanent and part-time employees), volunteers, contractors, interns, suppliers, and/or any individuals with access to the company's information, hardware, electronic systems, and/or software.

Confidential Data

Gkouskos Dimitrios defines "confidential data" as:

- Company's information
- Customer and supplier information
- Unreleased and classified financial information
- Legal records and company contracts
- Business processes, new technologies and/or patents in general
- Sales-related data and customer leads
- Employees' passwords, assignments, and personal information

Device Security

Company Use

To ensure the security of all company-issued devices and information, Gkouskos Dimitrios employees are required to:

- Regularly update devices with the latest security software

- Secure all relevant devices before leaving their desk
- Obtain authorization from the Office Manager and/or Inventory Manager before removing devices from company premises
- Keep all company-issued devices password-protected (minimum of 8 characters) - This includes computers, tablets, mobile devices and/or any other electronic device
- Refrain from sharing private passwords with coworkers, personal acquaintances and/or senior personnel

Personal Use

Gkouskos Dimitrios recognizes that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Always use secure and private networks
- Install full-featured antivirus software
- Regularly upgrade antivirus software
- Ensure all personal devices used to access company-related systems are password protected (minimum of 8 characters)
- Ensure all devices are protected at all times
- Lock all devices if left unattended

Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software. Therefore, Gkouskos Dimitrios requires all employees to:

- Contact the IT department regarding any suspicious emails
- Avoid opening suspicious emails, attachments, and clicking on links
- Look for any significant grammatical errors
- Avoid clickbait titles and links
- Verify the legitimacy of each email, including the email address and sender name

Transferring Data

Gkouskos Dimitrios recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Immediately alert the IT department regarding any breaches, malicious software, and/or scams
- Obtain the necessary authorization from senior management
- Verify the recipient of the information and ensure they have the appropriate security measures in place
- Refrain from transferring classified information to employees and outside parties
- Adhere to Gkouskos Dimitrios' data protection law and confidentiality agreement
- Only transfer confidential data over Gkouskos Dimitrios networks

Disciplinary Action

Violation of this policy can lead to disciplinary action, up to and including termination. Gkouskos Dimitrios' disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.