pireks
BAKIR ALAŞIMLARI SANAYİ VE TİCARET A.Ş.

# Information Security
# Policy

# Information Security Policy

## 1- Purpose

This instruction is prepared to highlight the importance of information security to the workplace employees, establish the rules that must be followed, ensure that information is used correctly and to contribute to the company's operations, and prevent misuse of information.

## 2- General Principles

While the confidentiality of employees' personal information is important, this confidentiality does not apply to the use of software, hardware, and other facilities provided for work-related activities. Our company has the right to control the information used in the workplace.

Employees are obligated to comply with intellectual property rights and the applicable laws in this regard. All equipment, software, and documents supplied by the company are provided in compliance with the relevant laws, and all company-provided resources are intended for carrying out company operations. Employees are not allowed to install any software, add, remove, or modify hardware, or connect additional devices to the network without permission.

All data, information, documents, drawings, programs, and other resources produced during employment are the property of our company. The sharing of information produced by employees or processed by them using our company's resources, as well as the alteration, deletion, or preventing access to this information, without permission, is prohibited.

Employees are responsible for the integrity, proper use, confidentiality, prevention of unauthorized access, and accessibility of all assets under their responsibility, conducting regular risk analysis to prevent harm to the company, and ensuring business continuity.

Employees may not attempt to access other people's information or systems, stop, block, or interfere with the systems' operation. They cannot delete or alter the company's information.

Our company reserves the right to audit compliance with information security principles, assess whether any practices are inconsistent with these principles, and take necessary measures to correct any violations.

## 3- Internet Usage

Employees of the company are members of two communities when using the internet: one is the community within their own PC network, and the other is the internet, which connects all networks and users worldwide. Being a member of these communities also imposes certain duties and responsibilities on the individual.

While our company adheres to the principles of free will, this freedom cannot be used without limits. Any flow of information that could harm the company cannot be considered under the framework of free expression. All user activities are continuously monitored, and if systems are used improperly, necessary actions will be taken.

The internet access and email services provided to employees by our company should be used to access information that affects productivity in their duties and to communicate with colleagues or other individuals regarding their work.

Employees, as members of the computer network, are responsible for using the internet and email system appropriately.

In general, internet services may not be used:

- In violation of applicable laws (Laws, Regulations, etc.),
- In a way that disrupts the rules and regulations of any service server, database, website, or network accessed,
- Fraudulently, inappropriately, rudely, aggressively, or misleadingly,
- To threaten, annoy, insult, intimidate, or coerce other users,
- In a way that harms the company's reputation and name,
- To break the security of any computer network or access an account that does not belong to the user,
- In a way that prevents other users from using or benefiting from the provided services,
- For playing games or trading game programs,
- To distribute viruses or other malicious software,
- To make obscene files accessible to the public,
- To organize charity campaigns,
- For personal gain, following up on business matters, requesting money using company resources, or looking for work outside the company.

Employees who violate these prohibitions may be subject to disciplinary actions, including termination of employment.

**4- Email Usage:**

Our company has provided the email system to enhance the efficiency of your work. It is mandatory to use the system exclusively for company-related business. The email account allows sending and receiving emails. If the email service is misused, the company reserves the right to take disciplinary actions, including termination of employment.

- The email account may not be used in a way that violates intellectual property laws. Copyrighted materials, such as articles, software, etc., may not be distributed inappropriately via email.
- The sending, receiving, printing, or any other form of distribution of our company’s confidential information, trade secrets, or other sensitive data in violation of company policies is prohibited.
- Using language or expressions that discriminate against individuals based on their race, nationality, gender, age, disability status, or religious or political beliefs, or any other form of offensive or harassing language, is prohibited.
- Sending or requesting sexually explicit messages or images is prohibited.
- Emails cannot be sent for personal or non-work-related purposes, such as jokes, cartoons, or political messages.
- The email account cannot be used to send bulk or commercial messages (spam). This includes advertisements, informational announcements, charity requests, petitions, and political or religious messages, but is not limited to these types of messages. These messages may only be sent to those who have requested them.
- The email account may not be used to collect responses to bulk or commercial messages sent by other service providers.
- Falsifying, altering, or deleting email headers is prohibited.
- Sending large quantities of identical or similar messages, large files, or messages that disrupt the functioning of another account or server (mail-bombing) is prohibited.
- The email service may not be used in a way that annoys, intimidates, or threatens other users. This includes using language, message frequency, or message size to achieve this effect. Even a single

unwanted message will be considered in this context. If a user indicates they do not wish to receive further messages, no additional messages may be sent to them.
- Chain emails, whether they involve money requests or not, cannot be forwarded or reproduced.
- Email accounts may not be used to collect responses to messages sent by other service providers if those responses violate our or other service providers' internet and email usage policies.

The company reserves the right to access and review any messages sent through the email system if deemed necessary, regardless of their content. As the company management may access your personal messages without prior notice, personal messages that are intended to remain private should not be sent using this email system.

**5- Virus Protection:**

Any data received from the internet or other computers on the local or wide area network must be scanned for viruses before use. Antivirus software has been installed on all computers, and these programs update automatically every day. Users are responsible for ensuring that the antivirus software on their computers is active and up to date.

**6- Security:**

Even if inappropriate activity is carried out by a friend, family member, guest, or another employee, the responsibility for any misuse of an account lies with the employee. Therefore, employees are responsible for taking measures to prevent unauthorized access to their accounts. Employees are prohibited from using their accounts to break into other accounts or gain unauthorized access to another network or server. Employees must:

- Implement adequate security measures to prevent unauthorized use of their accounts.
- Not use other users' passwords without authorization to access their electronic messages or accounts.
- Not attempt to bypass security measures or user authentication on any server, network, or account. "Cracking" or using accounts or servers that are not explicitly authorized to access or investigate other network security is prohibited. The use and distribution of tools designed to compromise security are prohibited. This includes, but is not limited to, password guessers, password crackers, or network probing tools.
- Not attempt to interfere with any user, server, or network service (denial of service attacks). This includes flooding networks, attempting to overload a service, or crashing a server, but is not limited to these actions.
- Users who compromise the security of systems or networks may be subject to legal prosecution. Our company will cooperate in any security investigations related to other systems and networks, including cooperation with legal authorities in the case of criminal investigations.

**7- Company's Monitoring and Review Rights:**

Our company has the right to monitor all data in the information system, though it is not obligated to do so. This includes monitoring the websites users access, examining files they send or receive, and reviewing electronic messages sent and received. Users are responsible for all data they create, save, send, or receive on their computers or the internet, and they give their prior consent for such data to be monitored and reviewed by the company.

**8- Management's Right to Access Information:**

Local network access, internet access, and the email system have been established by our company to facilitate work-related communication and information sharing. Although employees use personal passwords to access these systems, the systems are the property of the company, and company management has the right to access any relevant documents on users' computers, data related to the internet, and the content of electronic messages for any company-related matter. The systems may be audited by company management without prior notice. All system passwords are accessible to management, and personal passwords are available to the network administrator.

**COMMITMENT**

I have read the entire instruction. The content of the instruction has been fully explained to me, and I understand all aspects of it. I hereby accept, declare, and commit that I will exercise the utmost care regarding all matters explained to me in the Information Security Directive, comply with the rules, avoid prohibited actions, and acknowledge that if it is determined that I do not adhere to this commitment, my employment contract will be terminated for just cause.

... / ... / .....

Name Surname

Signature