This policy,

It defines our rules and approaches necessary to ensure the business continuity of SARBAK METAL A.Ş.'s information assets, to manage the risks to these information assets and to use the information assets in accordance with business purposes.

Establishment and management of the Information Security Management System (ISMS) to fulfill the requirements of the ISO 27001 standard in a way to protect the confidentiality, security and integrity of our information assets in the studies to be carried out regarding the collection, creation, processing, transfer and archiving of information while performing our company activities and it is intended to be constantly favored.

This policy covers all units of our Company, our employees and our customers. Our employees (User) are obliged to comply with the rules, processes and instructions specified in the annex to this policy and by reading this policy , they undertake to comply with the rules defined in this Policy. In order to increase the awareness of information security, trainings will be carried out to our employees in order to improve their technical and behavioral competencies.

ISMS will be continuously and systematically evaluated and improved. **IT Personnel** are responsible for managing the ISMS. Information **Security Management System Manager** is responsible for the installation, continuous development and control of the system.

All legal regulations and contracts related to information security will be complied with. The information security risks of our company are defined according to the "Risk Management Process"; This policy will be systematically reviewed.

The Information Security Policy will be implemented in the most effective way; That the Information Security Management System will be continuously developed and controlled by managing it in an integrated manner with our other management systems ; we undertake that the necessary sanctions will be applied in case of security violations.

SARBAK METAL A.Ş.

1. GENERAL RULES

Employees are required by SARBAK METAL's Information Security Management System (ISMS) ISO 27001 Standard to comply with this Information Security Policy, SARBAK METAL Personnel Regulation, Disciplinary Regulation, all the information security policy referred to or mentioned in the Information Security Policy undertake to comply with procedures, instructions, legislation and the terms of this undertaking, and to protect the confidentiality of information and documents related to their duties. Every SARBAK METAL employee is committed to protecting the confidentiality of information and signs the "**Personnel Information Form**".

Company employees are responsible for the storage/preservation and physical security of all kinds of information, files and / or programs they create as a result of their work. These studies will be carried out in accordance with the "Company **Physical and Environmental** Security Instruction" and the "**Server Security Instruction**" determined for the files and documents to be shared on the Company's network.

Electronic Information:

- Company employees are responsible for securely backing up theirvaluable and critical information on their computers on the Common Use Server. Therefore, valuable and critical information about the work by employees will be stored in "Shared" and "Private" work files reserved for the employee within the Common Use Server, instead of being stored on personal computers.
- No documents, information or software will be exchanged on personal computers and Common Use Server allocated by the Company without the permission and authorization of the user.
- Unauthorized employees are prohibited fromseeing or obtaining confidential and sensitive information of the Company. Therefore, when problems occur on personal computers, unauthorized persons will not intervene and the problems encountered will be reported to authorized persons.
- Will take up unnecessary space in your Common Areas and are not related to work music and picture files, games, movies and similar programs (mpg, mpeg, avi, exe, com, gif, jpg extensions) are prohibited.

Information on Paper Medium :

- Whether sensitive or not, the confidentiality of the information and documents related to the duties of the employees will be protected and the documents in paper media in the form of information and documents will be recorded according to the **"Back Up Usage Instruction"**.
- Company employees will not leave any documents on their desks, whether sensitive or not, on their desks outside of working hours and during leave periods.
- Paper and electronic storage media containing sensitive information will be protected in a locked and/or safe deposit box when not in use.

Information and Communication Systems and Equipment:

- They are managed in accordance with **the Company Asset Management Process**, including the Internet, common use servers, email, telephone, pagers, fax, computers, mobile devices and mobile phones.
- When using company telecommunication devices, the relevant laws and regulations are complied with.
- All equipment purchased for or on behalf of the Company, developed for the Company by the Company's employees or related persons for the Company , is the property of the Company . All hardware will be used in accordance with the applicable license, warning, agreement and agreements.
- The Company's information and communication systems and equipment are primarily used for the performance of the Company's business. Personal use of telecommunication devices is permitted as long as they do not conflict with the interests of the Company and the amounts of their use are used within limits that will not cause material damage to the Company. However, it may not interfere with the normal operations and business activities of the Company. In cases where excessive personal use is detected, the Company reserves the right to restrict and cancel the use of the telecommunication device .
- Users are responsible for all communication they make with telecommunication devices.
- The company may not use telecommunication devices illegally in any way. The Company may not use telecommunications devicesto delete, access, download and transmit inappropriate content . Users are prohibited from providing others with the credentials necessary to use telecommunications devices. In addition, information cannot be transferred to the Company network without being scanned for malware.
- Any use of these systems that is unlawful, offensive, contrary to the Company's other policies, standards and guidelines, or that is detrimental to the Company is a violation of this policy.

2. PASSWORD USAGE AND REMOTE SYSTEM OPERATING RULES

It is ensured that the employees of the Company access the Company's computer network through the desktop computers and/or mobile devices given to them for their work . Access to information resources will be carried out in accordance with the "Password Instruction" and **"Remote Access Instruction"**.

- Remote access is provided by "User Accounts" given to employees.
- A user name and password are provided for each "User Account" for the purpose of providing access control, including on servers and network devices, and preventing unauthorized access.

- Any user password is the employee's responsibility.
- Employees will comply with the "Password Use and Management Instruction" announced to them when using the user name and password given to them.
- Computer resources will not be shared unless necessary, and if the resources are shared, they will definitely act according to the rules of "Password Use and Management Instruction" .
- Employees cannot be connected with remote access without the knowledge of the IT department, it provides information when connecting and disconnecting, it cannot enter files that are not related to its job while working. All remote access will be recorded.
- HR's knowledge of software, database and files related to Human Resources and cannot be accessed without permission. In HR-related software and database, the ADMIN user is the HR Manager. Logs are open to the Information Processing Department.
- Users, information that they have been granted access to, and information outside the domains and that they will not attempt to access the areas. Therefore, it is forbidden to access unauthorized servers and to take actions that disrupt internal and external network security or network traffic.
- Any kind of company belonging to the company , customers, other third parties served disclosure, reproduction, alteration, distortion, destruction, loss, misuse , theft or unauthorized access of information is prohibited.

3. INTERNET USAGE RULES

- When using the company's internet resources, the relevant laws and regulations are complied with.
- The Company's internet resources are primarily used for the performance of the Company's business. personal use of internet resources is permitted in a way that does not conflict with the interests of the Company, does not harm the Company or discredits the Company.
- From the reliability of any information to be obtained from the Internet and used for business there should be suspicion and it should be known that the information received is likely to be outdated and inaccurate.
- Users can use their own users via their personal computers and/or mobile devices accounts are responsible for all transactions carried out on the internet. Therefore, users properly store their user accounts and passwords and may not share them with others; and changes it in accordance with the "**Password Instruction**".
- Piracy from the Internet isnot allowed to contain any of the inappropriate, written and graphic material. It is strictly forbidden to make purchases with credit card numbers that do not belong to him , password that does not belong to him. In addition, downloading and/or installing all kinds of files and programs such as anti-virus programs, cracked programs, screen savers, patches, desktop pictures, helper, repair programs is prohibited because they damage Computer Operating Systems.

- Considered to be the property of the Company, prepared for the internal use of the Company , with the Company's customers

  all kinds of information, documents, files, announcements and/or software (business potentials, unit costs, prices, investments, tender information, etc.) that will affect the Company's relationship or the image of the Company , that have not been approved by the Company, use and distribution outside of the assigned duties, selling, explaining, renting over the internet and /or transmitting to third parties outside the Company for any reason by any other method strictly prohibited. When it is determined that important information belonging to the Company is given or disclosed to unauthorized persons or if there is a doubt about it, **the Human Resources Regulation** and **Disciplinary Process** are applied.

  Company resources may not be used to store, link , bookmark , access and post inappropriate content.

4. SOFTWARE USE AND INTELLECTUAL PROPERTY RIGHTS COMPLIANCE RULES

Software installed on company computers is managed in accordance with the **"Company Asset Management Process"**.

- The relevant laws and regulations will be complied with when using the Company's software.
- The Software will be used in accordance with the applicable licenses, warnings, contracts and agreements.
- All software developed for the Company or for the Company, whose right to use for or on behalf of the Company has been obtained, is registered in the Company's asset inventory and is the property of the Company .
- In order to prevent the violation of usage rights, the software will be provided by the Company from reliable sources and in accordance with the Purchasing Processes.
- The company's internet resources and communication infrastructure cannot be used for any unapproved, free commercial software. No commercial software may be copied, sent, received or reproduced without the Company's permission.
- For Software and other products, the use of only licensed versions within the number of licenses will be checked by the Company.
- Unless otherwise stipulated in the license oragreements, copying of the software in any way, except for backup and archiving, is an offense according to the relevant Legislation. In addition to being prohibited by Kanunlarca, copying unauthorized software is a violation of this Policy.

5. ANTİ-VİRÜS POLİTİKASI

- Licensed anti-virus software is installed on company computers and their permanent operation is ensured.

- Computers that do not have anti-virus software installed are prohibited from being made available and connecting to the Company network. When computers without anti-virus software installed are detected, the relevant unit of the Company will be notified.
- No user can remove anti-virus software from the system they are using and no other anti-virus software can be installed on their system.
- Malicious virus programs (for example; viruses, worms, trojan horses, email bombs, etc.) It is forbidden to create and distribute within the Company.
- In the absence of anti-virus software, wireless access (Infrared, Bluetooth, etc.) features should not be activated and, if possible, anti-virus programs and new generation viruses should be protected.

6. ELECTRONIC MAIL USAGE RULES

- **When using** company **e-mail resources**, **the relevant laws and regulations are complied with.**
- **Company e-mail resources will be used primarily for the performance of official and approved Company business.**

1. Company employees in the performance of their defined duties they will send/receive e-mails using the company resources to be provided to them.
2. Company employees are responsible for all e-mail transactions performed with their own user accounts.
3. Company employees are responsible for preventing unauthorized persons from viewing and reading corporate e-mails in their jurisdiction.
4. Passwords are used in e-mail systems. Personal passwords may not be displayed or shared with others, including authorized officers of the Company. Otherwise, the person who shares the password is deemed to have accepted the responsibility of the person who learns the password on behalf of himself. Personal passwords are revoked by the Admin Authorized Officer in case of termination of the employee's employment contract and in case of emergency.
5. Hardware/software systems used for electronic mail access are protected against unauthorized access .

- **Company employees should check their e-mails regularly.**

1. Emails will be replied to or forwarded to the contact person as soon as possible.
2. Documents whose e-mail attachments are critical and valuable will be archived in accordance with the **"Server Security Instruction"**.
3. Even if "Announcement" is not written in the "Subject" section, the **Human Resources Department is authorized** to **send announcement e-mails** containing many users in the "To" section. The e-mails to be sent for the purpose of announcement are announced to the relevant persons by the Human Resources Manager after the control of the Human Resources Manager.
4. All out-of-company emails will contain the following warning message:

"*This e-mail message and attachments are private to the person or institution to which it is sent and are confidential. It can also be legally hidden. It cannot be disclosed or*

published to third parties in any way. If you are not the recipient from whom the message was sent, you are strictly prohibited from disclosing, copying, directing and using the contents of this e-mail and you must delete it and its attachments immediately. SARBAK METAL does not give any guarantee that the information contained in this message is accurate or incomplete. Therefore, it is not responsible for the content, transmission, receipt, storage and use of this information in any form. The opinions in this message belong to the sender and may not reflect the views of SARBAK METAL.

This e-mail and its attachments are private and confidential and intended for the exclusive use of the individual or entity to whom it is addressed . It may also be legally confidential. Any disclosure, distribution or other dissemination of this message to any third party is strictly prohibited. If you are not the intended recipient you are hereby notified that any dissemination, forwarding, copying or use of any of the information is strictly prohibited, and the e-mail should immediately be deleted. SARBAK METAL makes no warranty as to the accuracy or completeness of any information contained in this message and hereby excludes

any liability of any kind for the information contained therein or for the transmission, reception, storage or use of such information in any way whatsoever. The opinions expressed in this message are those of the sender and may not necessarily reflect the opinions of SARBAK METAL. "

- **Company employees are obliged to act in accordance with the moral rules and the legislation in force in the use of electronic mail.**
  1. Personal use of e-mail resources is permitted as long as it does not conflict with the interests of the company and is careful not to be large enough to occupy the system unnecessarily .
  2. Employees can use inappropriate content (pornography, racism, political propaganda, material containing intellectual property, etc.) by e-mail. they can't.
  3. In case of being a member of the lists on the Internet for personal use , the Company's electronic mail addresses are not used.
  4. The Company's electronic mail system may not be used in any way to send messages containing items intended to harass, abuse or in any way harm the rights of the recipient.
  5. The e-mail system of the Company cannot be used for the receipt of any free or commercial software, sending or storing it without the knowledge of the IT department.
  6. Users are required to share information using electronic mail forwarding, file servers, and other mechanisms established by authorizable Information Security.
  7. No electronic mailboxes are created on the system except for company employees.

- **Usersare obliged to delete unnecessary electronic mail.**

  1. Electronic mails can contain malicious code such as viruses, electronic mail bombs, and Trojan horses.

  2. Electronic mails of unknown origin and attached files; chain messages and electronic mails containing any executable files attached to the messages; e-mails asking to enter the user code/password will be informed to the IT Department without any action; it will certainly be open up, the response will not be written and will be deleted immediately, and will certainly not be forwarded to others.

- **E-Mail Software**
  1. Users may only use e-mail software and configurations approved by the Company's authorized bodies .
  2. It is forbidden to change the current security settings of the e-mail software..
  3. Users are prohibited from using features in the email software that will hide the identity of the sender.

- **The purchase and use of electronic mail accounts for company users is managed by the Information Processing Officer with the approval of the Information Security Manager with the notification of the Human Resources department, deprecation , and the Human Resources department.**
- **All electronic mail** systems and **the creations and maintained on these systems and/or stored messages, information and files (including backed-up copies) are all considered Company information assets.**
- **From computers whose security is not sure (for example, common computers such as internet cafes**) **computers in the use area) web e-mail system cannot be used.**

7. MONITORING AND AUDITING RIGHTS

The Company reserves the following rights; and employees have been informed and accepted by reading this Policy about the Company's monitoring and supervision rights.

- Information security management systems and the activities carried out with these systems monitoring, recording and periodically auditing,
- Monitoring all transactions made using internet systems,
- The Company shall monitor all transactions made using e-mail systems,
- Removing the detected software that does not comply with the license agreements without informing the user ,
- The right to share information about the user's activities with the software with third parties, law enforcement or the judiciary without the user's consent,
- Sharing information about theuser's activities on the internet, e-mail system, common use servers and mobile vehicles and equipment of immovable or mobile companies with third parties, law enforcement or the judiciary without the permission of the user

8. ENFORCEMENT AND PUNISHMENT

Disciplinary Proceedings will be initiated against those who do not comply with the Information Security Policy and other policies, processes and instructions specified herein; As a result of the investigation, one or more of the ways of warning, reprimand, fine, contract termination will be applied. If deemed necessary, legal action will be initiated.