	<b>ISMS POLICY</b>		
	BGEK-02	RELEASE DATE 07.02.2022	REVISION #/ DATE 00

**The main theme of the TS EN ISO 27001:2013 Information Security Management System is "Manufacturing of outerwear out of woven, knitted and crocheted fabric (coats, coats, jackets, trousers, suits, suits, anoraks, raincoats, evening dresses, etc.). Information security used to protect customs and foreign trade transactions and all information assets of logistics, storage, accounting, finance and information processing activities related to these transactions.**


In the scope of; human, infrastructure, software, hardware, organizational information, third-party information and financial resources demonstrating the information security management is provided, securing risk management, information security management process to measure its performance and to ensure the regulation of relations with third parties on issues related to information security.

In this means, the purpose of our **ISMS Policy** is;

- Managing information assets, determining the security values, needs and risks of assets, developing and implementing controls for security risks
- Defining the framework that will create the methods for determining information assets, values, security needs, vulnerabilities, threats to assets, and frequency of threats.
- Defining a framework for assessing the confidentiality, integrity, accessibility impacts of threats on assets.
- To set out the working principles for handling risks.
- To monitor the risks continuously by reviewing the technological expectations in the context of the scope of service.
- To meet the information security requirements arising from the national or international regulations to which it is subject, fulfilling the legal and relevant legislation requirements, meeting the obligations arising from the agreements, and corporate responsibilities towards internal and external stakeholders.
- To reduce the impact of information security threats on service continuity and to contribute to the sustainability
- To have the competence to respond quickly to information security incidents that may occur and to minimize the impact of the incident.
- To maintain and improve the level of information security over time with a cost-effective control infrastructure.
- To improve the reputation of the institution, to protect it from negative effects based on information security
- To ensure the sustainability of the Information Security Management System
- Continuously improving the Information Security Management System

<b><u>PREPARED BY</u></b>	<b><u>APPROVED BY</u></b>
ISMS COORDINATOR MUSTAFA ÇEÇ	GENERAL MANAGER EMRE KIZILGÜNEŞLER

ÇOK GİZLİ     GİZLİ     HİZMETE ÖZEL     ANONİM     DAHİLİ     HARİCİ

	<b>ISMS POLICY</b>			
	BGEK-02	BGEK-02	BGEK-02	BGEK-02

**The main theme of the TS EN ISO 27001:2013 Information Security Management System is "Manufacturing of outerwear out of woven, knitted and crocheted fabric (coats, coats, jackets, trousers, suits, suits, anoraks, raincoats, evening dresses, etc.). Information security used to protect customs and foreign trade transactions and all information assets of logistics, storage, accounting, finance and information processing activities related to these transactions.**

In the scope of; human, infrastructure, software, hardware, organizational information, third-party information and financial resources demonstrating the information security management is provided, securing risk management, information security management process to measure its performance and to ensure the regulation of relations with third parties on issues related to information security.

In this means, the purpose of our **ISMS Policy** is;

- Managing information assets, determining the security values, needs and risks of assets, developing and implementing controls for security risks
- Defining the framework that will create the methods for determining information assets, values, security needs, vulnerabilities, threats to assets, and frequency of threats.
- Defining a framework for assessing the confidentiality, integrity, accessibility impacts of threats on assets.
- To set out the working principles for handling risks.
- To monitor the risks continuously by reviewing the technological expectations in the context of the scope of service.
- To meet the information security requirements arising from the national or international regulations to which it is subject, fulfilling the legal and relevant legislation requirements, meeting the obligations arising from the agreements, and corporate responsibilities towards internal and external stakeholders.
- To reduce the impact of information security threats on service continuity and to contribute to the sustainability
- To have the competence to respond quickly to information security incidents that may occur and to minimize the impact of the incident.
- To maintain and improve the level of information security over time with a cost-effective control infrastructure.
- To improve the reputation of the institution, to protect it from negative effects based on information security
- To ensure the sustainability of the Information Security Management System
- Continuously improving the Information Security Management System

<u>PREPARED BY</u>	<u>APPROVED BY</u>
ISMS COORDINATOR MUSTAFA ÇEÇ	GENERAL MANAGER CİHAN YER
<input type="checkbox"/> ÇOK GİZLİ <input type="checkbox"/> GİZLİ <input checked="" type="checkbox"/> HİZMETE ÖZEL <input type="checkbox"/> ANONİM <input checked="" type="checkbox"/> DAHİLİ <input type="checkbox"/> HARİCİ	