1. PURPOSE

The purpose of this instruction is to define the approach and solutions used to ensure the security of systems belonging to Kerevitaş Gıda San. ve Tic. A.Ş. against cyber threats.

2. SCOPE

Bu prosedür Kerevitaş Gıda San. ve Tic. A.Ş.'ye ait tüm sistemleri kapsar.

3. DUTIES, AUTHORITIES, AND RESPONSIBILITIES

R (Responsible)	The person responsible is the one who performs the task; there should be only one 'R' in each row	**C (Consulted)**	The person consulted.
A (Accountable)	The person who approves the completion of the task; there should be one 'A' in each row. This is the first person to be asked about the completion of the task.	**I (Informed)**	The person informed.

Roles and Responsibilities	**Information Security Director**	**Application/System Owner Administrator**	**Help Desk**	**Cyber Security Director**	**Information Security Board**
Conducting a Risk Analysis	R			C	A
Selecting Solutions Based on Risk Analysis Results	I	R		AR	I
Approval for Solution Implementation			I	AR	RI
Establishing Usage Policies for the Solution	AR			C	I
Deployment and Operation of the Solution	I	R	I	A	I

4. APPLICATION

Kerevitaş Gıda San. ve Tic. A.Ş, evaluates cybersecurity in the following areas. It adopts a layered security approach. The solutions used in the relevant areas are listed below.

1. Endpoint Security
2. Data Security
3. Vulnerability Management
4. Application Security
5. Secure Remote Access
6. Monitoring

4.1. Endpoint Security

Endpoint security is a solution used to protect computers, laptops, tablets, and mobile devices connected to the company network from cyber threats. Endpoint security provides defense against physical loss or theft of devices, malware accessing the network, or unauthorized individuals. Endpoint security is an important part of network security and helps reduce the risks of data theft, ransomware, phishing, and other cyber attacks.

1. Symantec EndPoint Security and Microsoft Defender Provides protection against malware on user computers and servers.
2. Forcepoint URL Filter Ensures secure internet access for users.
3. Windows Defender Firewall Prevents attacks on user computers at the network level.
4. Windows Defender ATP - EDR Used to detect advanced malware.
5. Phishing – Training Used to increase and measure employee awareness against phishing attacks.
6. Email Security MS O365 advanced security package is used for email security.
7. Identity Security MS O365 advanced security package is used for identity security.

4.2. Data Security

Data security is the protection of any kind of data stored or transmitted in computer systems, networks, databases, and other digital environments from unauthorized access, use, alteration, disclosure, loss, or destruction. Data security includes technological, organizational, and legal measures to ensure the integrity, confidentiality, and availability of data. It aims to protect data against various threats such as cyber-attacks, natural disasters, human error, or intentional acts.

1. Symantec DLP:Monitors data leakage according to the rules set by the Information Security Board.
2. Disk Encryption: Ensures the protection of data on a computer in case of loss or theft.
3. RMS - Rights Management System: Protects office files and PDF documents.
4. SecureFileTransfer: Used for secure file receiving and sending from outside the organization.
5. AIP - Data Classification: Used for classifying and labeling documents according to the classification levels set by the Information Security Board.

6. Local CA: Provides transparent authentication for users connecting to the corporate wireless network and ensures the security of non-public web applications.

4.3. Vulnerability Management

Vulnerability management is the process of identifying, evaluating, and addressing security vulnerabilities in information systems. The goal of vulnerability management is to prevent attackers from infiltrating systems, causing data breaches, or leading to service disruptions. It includes steps such as regular scanning, risk analysis, patching, and reporting.

1. Vulnerability Scanner – Qualys: Used to find and fix vulnerabilities on servers before attackers can exploit them.
2. InsightVM - Web Vulnerability Scanning: Used to find and fix vulnerabilities in web applications before attackers can exploit them.
3. Fortify Static Source Code Analysis: Used to find and fix vulnerabilities in applications before they go live.
4. Penetration Testing Service: Professional firms test systems for vulnerabilities from an attacker's perspective. Identified vulnerabilities are then fixed.
5. Hardening – Sechard: Ensures the security levels of servers are improved according to international CIS (Center for Internet Security) standards.

4.4. Application Security

Application security is a process that ensures the protection of web applications and their data from cyber attacks. Application security includes tools and methods to prevent and detect security vulnerabilities during the design, development, usage, and testing phases of applications. It applies fundamental security principles such as confidentiality, integrity, and availability to applications.

1. F5 - WAF, LOAD BALANCER: Prevents attacks on web applications and distributes load in systems with multiple application servers.
2. SSL Certificate: Ensures secure access to web applications.
3. Microsoft Cloud Apps Security: Monitors user activities in cloud services and identifies anomalies.
4. Microsoft Defender for O365: Ensures security in the Microsoft cloud (Office 365) environment.

4.5. Secure Remote Access

Secure remote access is a technology that allows employees or consultants to connect to the company's network resources from outside. This technology enables users to access the company's systems and perform their work from home, while traveling, or from another location. Secure remote access typically involves security measures such as VPN (Virtual Private Network) and user authentication to grant access.

1. Pulse Secure – VPN: Ensures secure access for users and consultants to the company's network systems from outside.

2. PAM – CyberArk: Records the activities of consultants on the systems and protects important accounts.
3. Local CA: Provides transparent authentication for users connecting to the corporate wireless network and ensures the security of non-public web applications.
4. MFA (Multi-Factor Authentication): Provides strong authentication for system access.

4.6. Monitoring

The monitoring process in security involves continuously observing systems and networks, detecting suspicious or abnormal activities, and intervening when necessary. Tools such as log collection, SIEM, IDS/IPS are used to detect and analyze security events early. The monitoring process in security helps reduce the organization's security risks, protect against cyber-attacks, and minimize the impact of any breaches.

1. SIEM - IBM Qradar, Log Collection: Collects security logs from critical systems.
2. Security Operation Center: Monitors and analyzes system logs 24/7 and reports significant ones for action.
3. ThreatMon: Monitors the organization's assets in the cyber world.
4. File Audit – DI: Monitors file servers, tracking the creation, deletion, and modification of files.
5. Azure ATP: Ensures the security of Active Directory servers and prevents identity theft.