HYUNDAI MOBIS **MOBİS OTOMOTİV VE MODÜL SAN. VE TİC. A. Ş.**	# GÜVENLİK YÖNETMELİĞİ (SECURITY REGULATIONS)	**KAYIT NO :** (REGD.NO) **REV.NO :** 4 (REV.NO) **REV. TARİHİ: 02.05.2025** (REV.DATE)

İÇERİK
(CONTENTS)

ONAY (APPROVAL)

BAŞLIK (ITEM)	**HAZIRLAYAN** (PREPARED BY)		**HEAD OF DEPARTMENT** (DEPARTMAN BŞK)		**ONAY CEO** (APPROVED BY CEO)
BÖLÜM (DEPARTMENT)	**GA**	**IT**	**GA**	**IT**	
ADI (NAME)	**YUSUF SARAÇ**	**MINSOO KIM**	**NECDET ÖZTÜRKÇÜ**	**MUSTAFA KURUKAFA**	**SOOMIN HWANG**
İMZA (SIGN)					
TARİH (DATE)					

HAZIRLAYAN BÖLÜM (PREP DEPT)	**KAYIT** (REGISTRATION)
GENERAL AFFAIRS	**KG BÖLÜMÜ** (QA DEPT) **/ /**

MŞT İMZA (CO-SIGN)

DAĞITIM LİSTESİ (DISTRIBUTION LIST)

DAĞITIM (DISTRIBUTION)	**İMZA** (SIGN)
PRODUCTION	
QUALITY	
PURCH.&PARTS DEVLP	
SALES	
INF.TECHNOLOGY (IT)	
ACC & FINANCE	
PRODUCTION CONTROL	

REVİZYON KAYDI (REVISION RECORDS)

REV. NO	**REV. DATE** (START DATE)	**REVİZYONUN ANA İÇERİĞİ** (MAIN CONTENTS OF REVISION)
1	**27.06.2019**	Updating responsible person of each department
2	**23.11.2021**	Clarify rule of physical security and information and network security
3	**20.07.2021**	Updating of responsible and authorized persons
4	**02.05.2025**	Updating physical security measures under ISO 27001

ALT DAĞITIM (SUB DISTRIBUTION)

DAĞITIM (DISTRIBUTION)	**İMZA** (SIGN)

MOBİS OTOMOTİV VE MODÜL SAN. VE TİC. A. Ş.	**GÜVENLİK YÖNETMELİĞİ** (SECURITY REGULATIONS)	**KAYIT NO :** (REGD.NO) **REV.NO :** 4 (REV.NO) **REV. TARİHİ** 02.05.2025 (REV.DATE)

İçindekiler

Table of Contents

Genel Hükümler

1.Bilgi Güvenliğine Genel Bakış

1.1 Amaç

Bu yönetmeliğin amacı HYUNDAI MOBIS (bundan sonraki kısımda "Şirket" ya da "Biz" olarak anılacaktır) bilgilerini korumak adına temel yapıyı düzenlemek, işlenen, saklanan ve bilgi sistemleri kanalıyla iletilen verileri virüs, bilgisayar korsanlığı vb. tehditlere karşı koruma altına alarak kendi çalışanlarımızı ve tesislerimizi izinsiz bir kişinin kötü niyetli hareketinden güvenli bir şekilde korumak ve hasar görebilirliklerini bertaraf etmektir.

1.2 Uygulamanın Kapsamı

Bu yönetmelik çalışanlarımız, sözleşmeyle yasal ilişki tesis edilmiş kişiler, ziyaretçiler ve bilgi varlıklarının kayıt altına alındığı, saklandığı ve değerlendirildiği medya ve bilgi sayım araç gereçleri için olduğu kadar ilgili tesislerimiz için de uygulanacaktır.

1.3 Tanımlar

1.3.1 İdari Güvenlik

"İdari güvenlik" terimi güvenlik organizasyonu, güvenlik politikası ve prosedür yönetimi, güvenlik eğitimi, güvenlik sınavı, güvenlik olay incelemesi vb. düzenlenmesi ve operasyonu gibi bir güvenlik faaliyeti anlamına gelmektedir.

1.3.1.1. Güvenlik Başkanı (CSO)

"Güvenlik Başkanı (CSO)" terimi bilginin korunmasıyla ilgili olarak kendisine İcra Kurulu Başkanı (CEO) tarafından yetki verilmiş olan ve güvenlik politikasının kurulması, eğitimi, denetimi vb. güvenlik uygulamaları ve teftişi konularında bir temsilci haline gelmiş yönetici anlamına gelmektedir.

1.3.1.2. Bilgi Varlıkları

"Bilgi varlığı" terimi fikri mülkiyet hakları, patent, ticari sır vb. şirketin işlediği tüm teknik ve yönetimsel bilgiler ve dokümanlar, bilgisayar sistemi, yazılım, görüntü ortamı, tesisler ve aynı zamanda bahsi geçen teknik ve yönetimsel bilgileri içeren diğer maddi ve manevi mülkler anlamına gelmektedir.

General Provisions

1.Overview of Information Security

1.1 Purpose

The purposes of these regulations are to organize basic structure for information protection of HYUNDAI MOBIS. (hereinafter referred to as the "Company" or "We"), to safely protect our personnel and facilities from misconduct of an unauthorized person and to further secure the information of the Company by protecting the data that are processed, stored and communicated through the information system from threats, such as virus, hacking, etc., and removing its vulnerability.

1.2 Scope of Application

These regulations apply to our employees, a person in privity of contract. A visitor and all information properties including media and computation equipment in which information assets are recorded, stored and utilized as well as related facilities.

1.3 Definitions

1.3.1 Administrative Security

The term "administrative security" means a security activity such as composition and operation of security organization, security policy and procedure administration, security education, security examination, security incident investigation, etc.

1.3.1.1. Chief Security Officer (CSO)

The term "chief security officer (CSO)" means an officer that is delegated with an authority over information protection from the CEO of the Company and becomes an agent for security execution and supervision, such as establishment, education, inspection, etc. of the security policy.

1.3.1.2. Information Assets

The term "information asset" means technical or managerial information that the Company possesses, such as intellectual property rights, patent, trade secret, etc. and document, computer system, software, image media, facility, as well as other tangible and intangible properties that include the said technical or managerial information.

1.3.1.3. Ticari Sır

"Ticari sır" terimi gizliliğini sağlamak için çabaya konu olan diğer iş faaliyetleri için faydalı olan üretim yöntemi ve satış yöntemi, teknik ya da işletmeyle ilgili bilgiler anlamına gelmektedir. Ticari sır Şirketin kendi kullanımı için sözleşmesel bir yol ile uyarladığı diğer bir başka şirketin ticari sırlarını da içermektedir.

1.3.2 Fiziki Güvenlik

"Fiziki güvenlik" terimi Şirketin tesisleri ve çalışanlarını erişim denetimi, bilgi varlıklarını getirme ve bilgi varlıklarından alma konularında kontrol sahibi olma, durum görüntüleme vb. konularda yetkisiz bir kişiden korumak için olan bir güvenlik faaliyeti anlamına gelmektedir.

1.3.2.1. Durum Görüntüleme

"Durum görüntüleme" terimi emniyet, olay ve güvenliğin güvenlik personeli veya bir iş lokasyonunda kurulu olan bir CCTV sistemi kanalıyla gerçek zamanlı olarak doğrulanmasıyla ilgili bir faaliyet anlamına gelmektedir.

1.3.3 Teknik Güvenlik

"Teknik güvenlik" terimi bilgi sistemlerini korumak ve bilgi sistemleri kanalıyla olabilecek sızıntıları önlemek amacıyla idari kontrol, bilgi sistemleri erişim kontrolü, gelişim ve bakım, izinsiz giriş olayı yönetimi, vb. güvenlik faaliyetleri anlamına gelmektedir.

1.3.3.1. Bilgi Sistemi

"Bilgi sistemi" kullanıcıya pürüzsüz bir hizmet sunmak adına donanım, çevresel aygıtlar ve işletim sistemini içeren çeşitli sistem yazılımları ve veri tabanı yönetim sistemleri anlamına gelmektedir.

1.3.3.2. Ağ

"Ağ" terimi Şirketin iş faaliyetleri için ilgili kuruluşlar arasında veya iş yerleri arasında çeşitli bilgileri iletmek için çeşitli sistemlerin birbiriyle bağlantı kurmasını sağlayan kablolu ya da kablosuz ağlar anlamına gelmektedir.

1.3.1.3. Trade Secret

The term "trade secret" means production method, and sales method, technical or business information useful for other business activity that is a subject of effort to maintain its secrecy. The trade secret includes trade secret of other company that the Company adopts through the privity of contract for its use.

1.3.2 Physical Security

The term "physical security" means a security activity to protect the facilities and personnel of the Company from an unauthorized person, such as access control, control over bringing and taking out of information assets, status monitoring, etc.

1.3.2.1. Status Monitoring

The term "status monitoring" means an activity related to real-time verification of safety, incident and security through management of security personnel or CCTV installed in a business location

1.3.3 Technical Security

The term "technical security" means a security activity such as administrative control, information system access control, development and maintenance, intrusion incident management, etc. in order to protect information system and prevent leakage through the information system.

1.3.3.1. Information System

The term "information system" means various system software and DBMS including hardware, peripheral devices and operating system to provide a user with smooth service.

1.3.3.2. Network

The term "network" means wired or wireless network that connects various systems to transmit various information among related organizations or among places of business for business operation of the Company.

1.3.3.3 Yedekleme

"Yedekleme" terimi, bilgi hizmetleri veya bilgi varlıklarına umulmadık ve istenmeyen bir olaydan dolayı gelecek zararları en aza indirgemek adına kopyalamak ve söz konusu bilgi hizmetleri ya da bilgi varlıklarını eski konumuna getirmek anlamına gelmektedir.

1.3.3.4. Onarma

"Onarma" terimi yedek kopyayı kullanarak önceki haline getiren kurtarma işlemi ve basit bir şekilde yedek veriyi yeniden yükleyen yenileme işlemi anlamına gelmektedir. Yedekleme, onarımın bir ön koşuludur.

1.3.3.5. Terminal

"Terminal" terimi LAN veya WAN kanalıyla bağlı olan kişisel bilgisayar ve yazıcıyla sınırlı kalmamak kaydıyla, konsol, tarayıcı gibi aletleri de içerisine alan bir giriş/çıkış aygıtı anlamına gelmektedir.

1.3.3.6. Kişisel Bilgisayar

"Kişisel Bilgisayar" terimi masaüstü ya da dizüstü bilgisayar anlamına gelmektedir.

1.3.3.7. Taşınabilir Cihaz

"Taşınabilir cihaz" terimi bir cep telefonu, akıllı telefon, kişisel dijital yardımcı (PDA), tablet, kişisel bilgisayar vb. anlamına gelmektedir.

1.3.3.8. Bilgi Güvenliği Olayı (İzinsiz Giriş Olayı)

"Bilgi güvenliği olayı" terimi koruma ve yönetimin konusu olan bilgi ve bilgi sisteminin izinsiz bir şekilde yok edilmesi veya bilgi güvenliği yönetimi sisteminde bir sorunun oluşması durumları anlamına gelmektedir.

1.3.3.9. Web posta

"Web posta" terimi giriş ve çıkış süreçleri kanalıyla bir web tarayıcı üzerinden e-postaların gönderilebildiği bir posta servisi anlamına gelmektedir.

1.3.3.10. VPN (Sanal Özel Ağ)

"VPN (Sanal Özel Ağ)" terimi Internet gibi bir genel ağı kullanarak özel bir ağ kurulmasını sağlayan bir teknoloji ya da bir ağ anlamına gelmektedir.

1.3.3.3. Backup

The term "backup" means to make a copy to minimize damages to information service or information assets, which may be caused by an unexpected and undesirable incident and to restore the said information service or information assets.

1.3.3.4. Repair

The term "repair" refers to recovery that reverts to former state using a backup copy and restoration that simply reinstall the backup data. The backup is a precondition to the repair.

1.3.3.5. Terminal

The term "terminal" means an input/output device and includes but not limited to a personal PC and printer connected through LAN or WAN, console, scanner.

1.3.3.6. PC

The term "PC" means a desktop and a laptop.

1.3.3.7. Mobile Device

The term "mobile device" means a cellular phone, smart phone, PDA, tablet PC, etc.

1.3.3.8. Information Security Incident (Intrusion Incident)

The term "information security incident" means cases in which the information and the information system that are objects of protection and management are destroyed without permission or in which a problem occurs in an information security management system.

1.3.3.9. Web mail

The term "web mail" means a mail service in which a mail may be sent using a web browser through login and logout process.

1.3.3.10. VPN (Virtual Private Network)

The term "VPN (Virtual Private Network)" means a technology or a network that enable to construct a private network using a public network such as Internet.

1.3.3.11. P2P (Eşler Arası)

"P2P (Eşler Arası)" terimi Internet üzerinden kişiler arasında bir dosyanın paylaşımını sağlama teknolojisi ve faaliyeti anlamına gelmektedir.

1.3.3.12. Web disk alanı / Web klasörü

"Web hard / Web folder" terimi her türlü bilginin Internet üzerinden saklanabileceği / hareket edebileceği / paylaşılabileceği veya bir dosyanın saklanabileceği / yüklenebileceği ve indirilebileceği bir bilgi saklama servisi anlamına gelmektedir.

1.3.3.13. DMZ (Demilitarized Zone)

"DMZ (Demilitarized Zone)" terimi bir güvenlik duvarı kurmak için dışarıya maruz kalan bir sunucu, kişisel bilgisayar vb. için bir ağ yönetim bölgesi anlamına gelmektedir.

1.3.3.14. FTP (Dosya Aktarım Protokolü)

"FTP (Dosya Aktarım Protokolü)" terimi Internet kanalıyla bir dosyanın bir bilgisayardan başka bir bilgiyara iletimini destekleyen bir protokol anlamına gelmektedir.

1.3.3.15. LAN (Yerel İletişim Ağı)

"LAN (Yerel İletişim Ağı)" terimi belli bir bölgedeki bir takım bilgisayarları, açık erişim cihazlarını vb. yüksek hızdaki iletişim hatlarıyla birbirine bağlayarak cihazlar arasındaki iletişimi sağlayan bir yerel iletişim ağı anlamına gelmektedir.

1.3.3.16. IP (Internet Protokolü) Adresi

"IP (Internet Protokolü) Adresi" terimi Internet geçici kullanımı için bir terminale atanan özgün bir adres anlamına gelmektedir.

1.3.3.17. Genel Ağ

"Genel ağ" terimi iletişim şirketlerinin belirsiz kişilere hizmet vermek üzere geliştirdikleri genel bir Internet ağı anlamına gelmektedir.

1.3.3.18. Özel Ağ

"Özel ağ" terimi bir işletme, okul vb. belli bir kurum için kullanılmak üzere geliştirilen bir iletişim ağı anlamına gelmektedir. Özel bir ağa erişime VPN vb. belli bir yöntem dışında izin verilmez.

1.3.3.11. P2P (Peer to Peer)

The term "P2P (Peer to Peer)" means technology and activity to share a file among individuals over the Internet.

1.3.3.12. Web hard / Web folder

The term "Web hard / Web folder" means an information storage service in which all types of information may be stored / moved / shared through the Internet or a file may be stored / uploaded and downloaded.

1.3.3.13.DMZ (Demilitarized Zone)

The term "DMZ (Demilitarized Zone)" means a network domain for a server, PC, etc. which shall be exposed to outside to configure a firewall.

1.3.3.14.FTP (File Transfer Protocol)

The term "FTP (File Transfer Protocol)" means a protocol to support the transmission of a file from a computer to another computer through the Internet.

1.3.3.15.LAN (Local Area Network)

The term "LAN (Local Area Network)" means a local area network that enables the communication among devices by connecting a number of computers, OA equipments, etc., in a certain area with high speed communication lines.

1.3.3.16.IP (Internet Protocol) Address

The term "IP (Internet Protocol) Address" means a unique address assigned to a terminal for use of the Internet.

1.3.3.17.Public Network

The term "public network" means a generally used Internet network that communication companies develop in order to serve unspecified individuals.

1.3.3.18. Private Network

The term "private network" means a communication network that is developed to be used for a specific institution, such as business, school, etc. An access to a private network is not permitted without a specific method, such as VPN, etc.

1.3.3.19. WAN (Geniş Alan Ağı)

"WAN (Geniş Alan Ağı)" coğrafi olarak birbirinden uzak olan geniş alanları birbirine bağlamak için olan bir iletişim ağı anlamına gelmektedir.

1.4 Görev ve Sorumluluk

1.4.1 Sözleşmesel ilişkisi olan bir çalışan ve bir kişi

A. Sözleşmesel ilişkisi olan bir çalışan ve bir kişi işbu yönetmelik ve ilgili yönergelerde yazan güvenlik politikalarını inceler.

B. Sözleşmesel ilişkisi olan bir çalışan ve bir kişi güvenlik eğitimine katılır ve Şirket'in iç denetim gibi güvenlik faaliyetleriyle aktif bir şekilde işbirliği içerisinde davranırlar.

C. Sözleşmesel ilişkisi olan bir çalışan ve bir kişi bir güvenlik olayına sebebiyet verebilecek aşırı kazanım, veri saklama veya ticari sırrı işyeri sınırları dışına izinsiz şekilde çıkarma gibi bir harekette bulunmaz.

D. Sözleşmesel ilişkisi olan bir çalışan ve bir kişi Şirket'in bigli varlıklarını dışarı çıkarmak için standart prosedürlere uyar ve izinsiz bir şekilde bu bilgi varlıklarını almaz.

E. Sözleşmesel ilişkisi olan bir çalışan ve bir kişi bir geçiş veya bir iş sistemi hesabını başkalarıyla paylaşmaz.

F. Sözleşmesel ilişkisi olan bir çalışan ve bir kişinin bir güvenlik olayı tespit etmesi halinde, ekiple (departman) beraber söz konusu olayı bir güvenlik müdürüne veya bir güvenlik kuruluşuna gecikmeden bildirir.

G. Aşağıdaki kişiler Şirket'in güvenlik yönetmeliği ihlalleri için sorumluluk kabul ederler:

G-a) Bir çalışan tarafından güvenlik yönetmeliğinin ihlali: İhlali gerçekleştiren kişi ve ekip lideri (veya departman yöneticisi)

G-b) Bir ziyaretçi tarafından güvenlik yönetmeliğinin ihlali: Giriş iznini talep eden çalışan.

1.3.3.19.WAN(Wide Area Network)

The term "WAN(Wide Area Network)" means a communication network to connect wide areas that are geographically far away.

1.4 Role and Responsibility

1.4.1 An employee and a person in privity of contract

A.An employee and a person in privity of contract shall observe security policies that these regulations and related guidelines prescribe.

B.An employee and a person in privity of contract shall participate in security education and actively cooperate with Company's security activities, such as internal inspection.

C.An employee and a person in privity of contract shall not engage in an act such as excessive acquisition, storage or taking trade secret out of the business location without permission, which is likely to cause a security incident.

D.An employee and a person in privity of contract shall follow the standard procedures for taking Company's information assets out and shall not take the said information assets without permission.

E.An employee and a person in privity of contract shall not share a pass or a business system account with others.

F.In case where an employee and a person in privity of contract finds out a security incident, he or she shall notify such facts to a security manager by team (department) or a security organization without delay.

G.The following persons shall assume responsibility for the violation of Company's security regulations:

G-a)Violation of security regulations by an employee: A person who violates and the team leader (or department manager)

G-b)Violation of security regulations by a visitor: An employee who requests an access permission.

1.4.2 Ziyaretçi

A. Bir ziyaretçi kendi çalışanı ya da başkalarına aldığı izni kiralamaz ya da bu iznin bilgilerini bu kişilerle paylaşmaz.

B. Bir ziyaretçi izin almadan kamera veya cep telefonu kamerası gibi bir video kayıt cihazı kullanarak resim ya da video çekmez.

C. Bir ziyaretçi Şirket'in resmi olarak sağladığı dışındaki herhangi bir veriyi edinmez ya da kullanmaz.

D. Bir ziyareti Şirket'in yönetmeliği ve ilgili kanun maddelerine göre Şirket'in talep ettiği güvenlik önlemlerinin ihlaliyle ilgili tüm sorumluluğu taşır.

D-a) Bir ziyaretçinin, izni burada şart koşulan durumlar dışındaki amaçlar için kiralaması ya da kullanması durumunda olduğu gibi bir izni suistimal etmesi veya kötüye kullanması durumunda, izni alınır ve giriş izni yasaklanır ve kendisinin CEO'su bunun tekrar etmemesi için gerekli önlemleri alır.

D-b) Bir ziyaretçi bir koruma alanındaki Şirket denetimini takip eder. Aksi takdirde, kendisi koruma alanı dışına alınabilir.

D-c) Bir ziyaretçinin izinsiz bir şekilde Şirket verilerini edinmeye, bu verilerden yararlanmaya ya da bu verileri sızdırmaya teşebbüs etmesi durumunda, söz konusu ziyaretçi ilgili kanunlara göre hukuki ve cezai sorumluluğu taşır.

İdari Güvenlik

2. Güvenlik Kuruluşu

2.1 Güvenlik Organizasyonu Yapısı ve Yöneten Kuruluş

A. İnsan kaynakları ekibi (departmanı) girişim güvenlik organizasyonu yapısı ve yönetimini gözeterek denetler.

B. İnsan kaynakları ekibi (departmanı) güvenlikle ilgli olarak çalışanların görev ve sorumluluklarını belirler ve bunlarla ilgili mevcut koşulları sağlar.

C. "2.4 Güvenlik Kuruluşu Görevlerinin Dağılımı" bölümünde aksi belirtilmediği sürece, Güvenlik Kurulu müzakere ile belirler.

1.4.2 Visitor

A.A visitor shall not rent or share a pass with his or her employee or others.

B.A visitor shall not take a picture or film without permission using a camera or a video tape recorder, such as a camera phone.

C.A visitor shall not acquire or use any data other than what the Company officially provides.

D.A visitor shall bear all the responsibility for violation of security measures that the Company demands in accordance with the Company's regulations and related laws.

D-a)In case where a visitor misuses or abuses a pass, such as to rent or use the pass for purposes other than what is stipulated herein, his or her pass shall be collected and he or she shall be forbidden to enter and his or her CEO shall submit measures to prevent recurrence thereof.

D-b)A visitor shall follow the Company's control within a protection area. Otherwise, he or she may be ordered out of the protection area.

D-c)In case a visitor attempts to acquire, utilize or leak the data of the Company without permission: A visitor shall bear civil and criminal responsibility in accordance with related laws.

Administrative Security

2.Security Organization

2.1Structure and Managing Entity of Security Organization

A.The human resources team (department) shall supervise structure and management of enterprise security organization.

B.The human resources team (department) shall define roles and responsibilities of employees with respect to security and maintain present condition thereof.

C.Unless otherwise prescribed in **"2.4 Division of Duties of Security Organization,"** the Security Council shall define through a deliberation.

2.2 Güvenlik Kurulu Faaliyeti

Güvenlik Kurulu CSO (Güvenlik Başkanı), güvenlik müdürü ve güvenlikten sorumlu bir kişiden oluşur ve güvenlik politikalarına karar vermek, bunları iletmek ve uygulamak üzere en az yılda iki kere toplanır.

2.3 Güvenlik Organizasyonu Şeması

İdari güvenlik çalışanları bir güvenlik müdürüne hazırlık yapar ve rapor eder ve ekibi, isimleri ve kendilerinin iletişim bilgilerini içeren bir güvenlik organizasyonu şeması (bkz: Ek-1) hazırlarlar.

2.4 Güvenlik Kuruluşu Görevlerinin Dağılımı (görev ve sorumluluklar) (1. Görev dağılımı standartlarına atıfla)

2.4.1 Güvenlik Başkanı (CSO) (Güvenlikten Sorumlu Yönetici)

A. CSO, CEO ya da CEO yetkileriyle donatılmış yönetici olur.

B. CSO, genel güvenlik müdürü olarak, tüm güvenlikle alakalı politikalara karar verir.

C. CSO, Kurumsal Güvenlik Müdürü ve Kurumsal Güvenlik Personelini atar.

D. CSO güvenlik planlaması ve uygulaması için bir güvenlik müdürüne talimat verir ve kendisini denetler.

2.4.2 Güvenlik Müdürü

A. CSO tarafından ataması yapılmış olan bir güvenlik müdürü CSO'ya rapor eder ve tüm güvenlik faaliyetlerini yerine getirir.

B. Bir güvenlik müdürü Şirket'in güvenlik yönetmeliğini tesis eder ve söz konusu yönetmeliği eğitim, bildiri vb. yollarla uygular.

C. Bir güvenlik müdürü güvenlikle ilgili kanun değişiklikleri ve ilgili şirketin güvenlik politikalarındaki değişiklikler gibi dış çevrelerdeki değişikliklere bağlı olarak güvenlik yönetmeliğini yeniden gözden geçirir. Gerekirse, güvenlik müdürü söz konusu değişiklikleri Şirket'in güvenlik yönetmeliğine yansıtır veya güvenlik eğitimi, güvenlik denetimi vb. önlemler alır.

D. Bir güvenlik müdürü her ayın belli bir gününü "güvenlik günü" olarak belirler ve güvenlik farkındalığını arttırmak adına içerideki güvenliği denetler.

E. Bir güvenlik müdürü güvenlik eğitimi ve tanıtımı yapar.

2.2 Operation of Security Council

The Security Council shall be composed of CSO (Chief Security Officer), security manager and a person in charge of security and operated at least semi annually in order to decide, deliver and implement security policies.

2.3 Security Organization Chart

Administrative security staff shall prepare, report to a security manager, and administer a security organization chart (see Attachment-1) that includes the team, name and contact of himself or herself.

2.4 Division of Duties of Security Organization (roles and responsibilities) (1. refer to the standards for division of duties)

2.4.1 Chief Security Officer (CSO) (Executive in Charge of Security)

A.The CSO shall be CEO or an executive that is entrusted with authorities of CEO.

B.The CSO, as a general security manage, shall decide all security-related policies.

C.The CSO shall appoint the Corporate Security Manager and the Corporate Security Staff.

D.The CSO shall direct and supervise a security manager to plan and implement security.

2.4.2 Security Manager

A.A security manager that is appointed by the CSO shall report to the CSO and implement all security operations.

B.A security manager shall establish the security regulations of the Company and apply the said regulations through education, announcement, etc.

C.A security manager shall re-examine the security regulations of the Company based on the changes in external environments, such as changes in laws related to security and security policies of a related company. If necessary, the security manager shall reflect the said changes in the security regulations of the Company or enforce measures such as security education, security inspections, etc.

D.A security manager shall designate a specific date every month "a security day" and inspect the security internally in order to raise security consciousness.

E.A security manager shall implement security education and promotion.

F. Bir güvenlik olayının meydana gelmesi halinde, güvenlik müdürü söz konusu olayla dışarıdan atanacak bir araştırma bilirkişiyle hizalı bir şekilde ilgilenir. Güvenlik müdürü söz konusu olay ele alındıktan sonra bu olayın tekrar etmemesi adına gereken önlemleri alır. Gerekirse, güvenlik müdürü insan kaynakları departmanına disiplin işlemi talep eder.

G. Bir güvenlik müdürü bilgi varlıklarının düzenli denetimi vasıtasıyla hasar görebilirlik araştırması ve karşı önlemleri kullanarak bir güvenlik olayı meydana gelmesinin önüne geçer.

I. Bir güvenlik müdürü CSO'ya bilgi koruma durumunu üç ayda bir rapor eder.

J. Bir güvenlik müdürü bilgi koruma faaliyetleri için bir plan ve bütçe onaylar ve devreye alır.

K. Bir güvenlik müdürü güvenlik ekibinin içerisinde olan kişilerle altı ayda bir birden fazla kere toplantı düzenleyerek güvenlik politikalarının daha aşağıdaki kişilere yayılımı için çabalar.

2.4.3 Kurumsal Güvenlik Personeli

Kurumsal Güvenlik Personeli görevleri idari güvenlik personelininkiler, fiziki güvenlik personelininkiler ve Teknik güvenlik personelininkiler olarak ayrılır. Güvenlikten sorumlu olan kişi yönetmelikte şart koşulan güvenlik faaliyetlerini hayata geçirir.

A. İdari Güvenlik Personeli

A-a) İdari güvenlik personeli bir eğitim planı belirler ve uygular ve bir güvenlik olayını çeşitli güvenlik etkinlikleri, izleme, düzenli bilgi varlığı denetimleri vb. yollarla engellemeye çalışır.

A-b) Bir güvenlik olayının meydana gelmesi durumunda, idari güvenlik personeli bu olayın araştırmasını yapar ve karşı önlemler alır.

B. Fiziki Güvenlik Personeli

B-a) Fiziki güvenlikten sorumlu olan kişi her ekibin (departmanın) talep ettiği güvenlik alanının tesis edilmesini gözden geçirir ve onaylar. Fiziki güvenlikten sorumlu olan kişi bunun sonuçlarını ilgili ekibe (departmana) bildirir ve durumu yönetir.

F.In case where a security incident occurs, the security manager shall deal with the said incident in line with an external investigative authority. The security manager shall establish measures to prevent recurrence of an incident posterior to completion of incident handling. If necessary, the security manager shall request disciplinary action to a human resources department.

G.A security manager shall prevent a security incident by vulnerability investigation and countermeasures through regular inspection of information assets.

I.A security manager shall report information protection state to CSO quarterly.

J.A security manager shall approve and operate a plan and budget for information protection activities.

K.A security manager shall endeavor to spread the security policies to lower organizations by holding a meeting of persons in charge of team security more than once semiannually.

2.4.3 Corporate Security Staff

The roles of the Corporate Security Staff shall be divided into those of administrative security staff, physical security staff and technical security staff. The person in charge of security shall implement security operations stipulated in regulations.

A.Administrative Security Staff

A-a)Administrative security staff shall establish and implement an education plan and prevent a security incident through various security events, monitoring, regular inspections of information assets, etc.

A-b)In case a security incident occurs, administrative security staff shall investigate the said incident and take countermeasures.

B.Physical Security Staff

B-a)A person in charge of physical security shall review and approve establishment of security area that each team (department) requests. The person in charge of physical security shall reply the results thereof to the said team (department) and manages its state.

B-b) Fiziki güvenlikten sorumlu olan kişi fiziki bir güvenlik sistemi işletir, ilgili prosedürleri belirler ve bunların faaliyetlerinin mevcut durumlarını yönetir. Fiziki güvenlikten sorumlu olan kişi, gerekirse, bir güvenlik müdürüne rapor eder ve önlem alır.

C. Teknik Güvenlik Personeli

C-a) Teknik güvenlik personeli bilgi teknolojisiyle ilgili tüm güvenlik faaliyetlerini tesis eder ve uygular.

C-b) Teknik güvenlik personeli bilgi teknolojisi güvenliği faaliyeti için bir plan belirler ve uygular.

C-c) Teknik güvenlik personeli bilgi teknolojisi güvenliği için ayrı bir detaylı yönerge hazırlar ve uygular.

C-d) Teknik güvenlik personeli bilgi teknolojisi güvenlik sistemini yönetir ve buradaki sonuçları inceler.

C-e) Teknik güvenlik personeli bilgisayım mülkyeti için istikarlı faaliyet ve güvenlik önlemlerini düzenler ve uygular.

C-f) Teknik güvenlik personeli, bilgi teknolojisi görevlerini yerine getiren kişi olarak, bir güvenlik müdürü tarafından görevlendirilir.

C-g) Teknik güvenlik personeli “Bölüm 4 Teknik Güvenlik”te yazılı olan içerikleri planlar ve uygular.

C-h) Bilgisayım mülkiyetinin hasar görebilirliğinin tespit edilmesi halinde, teknik güvenlik personeli bunun gelişmelerini bilgisayımla görevli olan kişiden talep eder ve bir yama uygular.

C-I) Teknik güvenlik personeli iç ve dış bilgisayım cihazları için güvenlik incelemesi yapar.

C-j) Teknik güvenlik personeli güvenlik yönetmeliğinde belirtilen güvenlik faaliyetlerini yerine getirmek için konuları uygular ve yerine getirir.

C-k) Bir güvenlik olayının meydana gelmesi durumunda teknik güvenlik personeli teknik araştırma, önlemler vb. için destek verir.

C-m) Teknik güvenlik personeli yukarıda belirtilen her maddenin sonucunu CSO’ya veya bir güvenlik müdürüne rapor eder.

B-b)A person in charge of physical security shall operate a physical security system, establish related procedures and manage current state of its operation. If necessary, the person in charge of physical security shall report to a security manager and take measures.

C.Technical Security Staff

C-a)Technical security staff shall establish and implement all security operations related to information technology.

C-b)Technical security staff shall establish and implement a plan to operate information technology security.

C-c)Technical security staff shall prepare and implement separate detailed guidelines for information technology security.

C-d)Technical security staff shall manage the information technology security system and analyze the results thereof.

C-e)Technical security staff shall arrange and implement stable operation and security measures for computation property.

C-f)Technical security staff, as a person who performs information technology tasks, shall be appointed by a security manager.

C-g)Technical security staff shall plan and implement the contents prescribed in "Chapter 4 Technical Security" herein.

C-h)In case where a vulnerability of computational property is found, technical security staff shall request its improvement to a person in charge of computation and implement a patch.

C-I)Technical security staff shall examine security for internal and external computing devices.

C-j)Technical security staff shall apply and implement matters to perform security operations specified in security regulations.

C-k)In case where a security incident occurs, technical security staff shall support for technical investigation, measures, etc.

C-m)Technical security staff shall report results of each subparagraph stated above to CSO or a security manager.

2.4.4 Ekip (Departman) Güvenlik Yöneticisi

Her ekibin (departmanın) güvenlik yöneticisi, takım lideri olarak (departmanın başı olarak), söz konusu ekibin (departmanın) güvenlik faaliyetlerini yerine getirmesinden, düzenlemesinden ve denetiminden sorumludur.

A. Bir ekibin (departmanın) güvenlik yöneticisi bir ekibin (departmanın) içerisindeki çeşitli ticari sırların güvenliğini inceler ve bir güvenlik dokümanına karar verir.

B. Bir ekibin (departmanın) güvenlik yöneticisi bir ekibin (departmanın) iç güvenlik denetiminin normal bir şekilde yerine getirilip getirilmediğini teyit eder ve bunun gözetimini yapar.

C. Bir ekibin (departmanın) güvenlik yöneticisi eki (departman) içerisindeki bir kilitleme aygıtı ve diğerlerinin düzgün bir şekilde kullanılıp kullanılmadığını ve yönetilip yönetilmediğini teyit eder ve bunun gözetimini yapar.

D. Bir ekibin (departmanın) güvenlik yöneticisi ekip (departman) içerisindeki kişilerin güvenlik eğitimini alıp almadıklarının gözetimini yapar.

E. Bir ekibin (departmanın) güvenlik yöneticisi ekip (departman) güvenliğinden sorumlu olacak bir kişiyi atar.

F. Bir güvenlik olayının meydana gelmesi halinde veya bir güvenlik olayının meydana gelebileceğinin anlaşılması halinde, ekibin (departmanın) güvenlik yöneticisi durumu Kurumsal Güvenlik Müdürüne iletir.

G. Bir ekibin (departmanın) faaliyetiyle ilgili olarak bir yere erişimin kısıtlanması halinde, bir ekibin (departmanın) güvenlik yöneticisi fiziki güvenlik personelinden bir koruma alanı tesisi talep eder.

H. Bir ekibin (departmanın) güvenlik yöneticisi Şirket'in güvenlik politikalarının etkili bir şekilde yerine getirilmesi için aktif bir şekilde destek verir.

2.4.4 Security Manager by Team (Department)

A security manager of each team (department), as a team leader (head of department), shall implement, coordinate and supervise safety operations of the said team (department).

A.A security manager of a team (department) shall review security of various trade secrets within a team (department) and decide a security document.

B.A security manager of a team (department) shall verify and supervise whether an internal security inspection of a team (department) is implemented normally.

C.A security manager of a team (department) shall verify and supervise whether a locking device and others within a team (department) are used and managed appropriately.

D.A security manager of a team (department) shall supervise the implementation of security education for members of a team (department).

E.A security manager of a team (department) shall appoint a person in charge of team (department) security.

F.In case a security incident occurs or it is apprehended that a security incident may occur, a security manager of a team (department) shall notify such facts to Corporate Security Manager.

G.In case it is necessary to restrict access to a place related to an operation of a team (department), a security manager of a team (department) shall request institution of a protection area to physical security staff.

H.A security manager of a team (department) shall actively support to effectively implement security policies of the Company.

2.4.5 Ekibin (Departmanın) Güvenlik Personeli

A. Ekibin (departmanın) güvenlik personeli, ekibin (departmanın) güvenlik müdürü tarafından görevlendirilmiş bir kişi olarak, söz konusu müdürün yönettiği şekilde hareket ederek ve aynı zamanda güvenlik denetimleri, güvenlik eğitimi vb. ekip (departman) ile ilgili güvenlik faaliyetlerini yerine getirerek, ekip (departman) içerisindeki mevcut güvenlik durumunu yönetir.

B. Ekibin (departmanın) güvenlik personeli her ay bir güvenlik günü belirler, mevcut güvenlik durumunu, sorunları vb. ekibin (departmanın) güvenlik müdürüne rapor eder ve söz konusu müdürün talimatları doğrultusunda güvenliğin gelişimini sağlar.

C. Ekibin (departmanın) güvenlik personeli Kurumsal Güvenlik Personelinin çağırdığı, güvenlik politikalarının kararıyla hizalı bir şekilde olan, ekibin (departmanın) güvenlik personeli toplantısına katılım sağlar ve söz konusu güvenlik politikalarının ekip (departman) içerisinde yayılımını sağlar.

3.Güvenlik Taahhütnamesi

3.1 Sorumlu Birim

A. Ticari sırları yasal olarak koruma altına almak ve çalışanların güvenlikle alakalı olarak farkındalıklarını sağlamak adına bir bilgi koruma teminatı beyanı hazırlanır ve sunulur.

B. İdari güvenlik personeli taahhütnamelerin konusu ve mevcut durumunu bir tablo ile göstermekle sorumludur ve herhangi bir ihmal olup olmadığını kontrol eder. Bir ihmal olması durumunda, sebeplerini anlar ve bu durumları CSO'ya rapor eder ve uygun olan önlemleri alır.

C. Bir çalışan ya da üçüncü bir taraf olduğuna bakmaksızın sadece bilgi koruma teminatı beyanı veren bir kişi iş lokasyonlarımıza erişi ve bilgi varlıklarını kullanır.

D. Bilgi koruma teminatı beyanını vermeyen bir kişi iş lokasyonlarımıza erişim yetkisi alamaz ya da sistemi kullanamaz. İdari güvenlik personeli bunun yönetiminden sorumlu olan kişidir.

2.4.5 Security Staff of Team (Department)

A.Security staff of team (department), as a person that a security manager of a team (department) appoints, shall manage the current security state within the team (department) by acting for the said manager manage as well as perform security activities related to the team (department), such as security inspections, security education, etc.

B.Security staff of team (department) shall implement a security day every month, report current security state, problems, etc. to a security manager of a team (department), and improve the security based on the instruction of the said manager.

C.Security staff of team (department) shall participate in the meeting of security staff of team (department) that Corporate Security Staff convenes, involving those in line with the decision of security policies, and spread the said security policies within the team (department).

3. Security Covenant

3.1 Managing Entity

A.An information protection pledge statement shall be prepared and submitted in order to legally protect trade secret and raise the security awareness of employees.

B.Administrative security staff shall maintain the objects and the current state of covenants with the tables and check for any omission therein. If there is any omission, he or she shall comprehend the causes thereof, report such facts to CSO and take appropriate measures.

C.Only a person irrespective of an employee or a third party, who submits the information protection pledge statement may access our business location and use the information assets.

D.A person who does not submit the information protection pledge statement will not be permitted to enter the business location or to use the system. Administrative security staff shall bear the management responsibility thereof.

3.2 Çalışan

A. Çalışanlar bilgi güvenliği konusunda çok iyi bir şekilde bilgilendirilir, bilgi koruma teminatı beyanını hazırlar ve taahhütnameyi Şirkete girişleri sırasında işe alım sorumlusuna iletirler. Bilgi koruma teminatı beyanı ilgili yasalar ve bilgi gizliliği konusunda uyulacak hususları açıkça belirtir.

B. İdari güvenlik personeli hizmeti devam eden çalışanlarda düzenli bir şekilde bilgi güvenliği teminatı beyanını talep eder.

C. Şirketten ayrılan bir çalışan koruması gereken ticari sırları, sözleşme süresini, yasaların gözetimi ve haksız rekabetin önüne geçmek adına yasal sorumlulukları vs. içeren "Emekli Olanlar İçin Ticari Sır Koruma Teminatı Beyanı"nı hazırlar ve verir.

D. Daimi personelin istifa etmesi veya işten çıkarılması durumunda, söz konusu personelin kimlik kartı alınarak/ biyometrik tarama sistemlerine sınırlama konularak tesislere girişi engellenir.

E. Daimi personelin istifa etmesi veya işten çıkarılması durumunda, söz konusu personelin şifrelerine bloke konulması ile bilgi sistemlerine erişimi engellenir.

F. Geçici personelin ayrılması veya çalışmasının sonlandırılması durumunda, söz konusu personelin kimlik kartı alınarak/biyometrik tarama sistemlerine sınırlama konularak tesislere girişi engellenir.

G. Geçici personelin ayrılması veya çalışmasının sonlandırılması durumunda, söz konusu personelin şifrelerine bloke konulması ile tesislere ve bilgi sistemlerine erişimi engellenir.

H. İstifa dilekçesi veya işten çıkarma bildirim tarihi ile personelin ilişik kesmesi arasında ilgili personel firmanızda çalışmaya devam ediyorsa, bu personelin yaptığı işlemler izlenir.

I. İşten ayrılacağı bilinen veya tahmin edilen personelin yerini alabilecek yedek personel görevlendirilir.

3.2 Employee

A.An employee shall be well-informed of importance of information security, prepare the information protection pledge statement, and submit the covenant to a recruiter in joining the Company. The information protection pledge statement shall specify matters to be complied with respect to related laws and confidentiality of information.

B.Administrative security staff shall regularly request the information protection pledge statement from employees in service.

C.An employee who is leaving the Company shall prepare and submit the "Retiree Trade Secret Protection Pledge Statement" which includes the contents of trade secrets that he or she shall protect, term of agreement, observance of laws and legal liability for prevention of unfair competition, etc.

D. In the event of a permanent employee resigning or termination, the employee's ID card is taken/biometric scanning systems are restricted and their entry to the facilities is prevented.
E. In the event of a permanent employee resigning or termination, the employee's passwords are blocked and their access to information systems is prevented.

F. In the event of a temporary employee leaving or termination, the employee's ID card is taken/biometric scanning systems are restricted and their entry to the facilities is prevented.

G. In the event of a temporary employee leaving or termination, the employee's passwords are blocked and their access to the facilities and information systems is prevented.

H. If the employee continues to work in your company between the date of the resignation letter or termination notice and the employee's termination, the transactions of this employee are monitored.

I. Replacement personnel who can replace the employee who is known or expected to leave the job are assigned

3.3 Üçüncü Şahıs (Genel İşgücü Hizmeti, Alt Taşeron Çalışanları)

A. Genel işgücü hizmetini de içerisine alan alt taşeron çalışanları üçüncü şahıs güvenlik teminatını hazırlar ve müteahhite verirler. Müteahhitin idari işlerinden sorumlu olan kişi söz konusu teminatı Şirket'in taşeronluk hizmetleriyle ilgili olan idari departmanına verir.

B. Şirketin belirlediği standart bir sözleşme kullanılır. Standart sözleşme şunları içerir: Şirketin güvenlik yönetmeliğinin incelenmesi, alt taşeron personeli ve müteaahit için güvenlikten sorumlu olması.

C. Teknik hizmet ya da verilerin değiştirilmesi durumunda, Şirketin bilgi varlıklarının korunması ve yönetimi için alt taşeronun Şirket adına güvenlik denetiminden sorumlu kişi olacağına belirten bir sözleşme imza edilir.

D. Taşeron firma personellerinin şirkete ait arşiv, bilgi işlem odası, yönetim ofisi, muhasebe vb. kısıtlanmış odalara sorumlu kişiler haricinde girişi yasaklanmıştır. Belirtilen odaların giriş – çıkışı kartlı sistem ve kilit ile korunmaktadır.

4.Güvenlik Eğitimi

4.1 CSO

A. CSO tüm çalışanlar için yılda birden fazla kere bir güvenlik eğitimi organize eder ve gerekirse CEO katılımını da talep edebilir.

B. CSO yeni ve meslekten yetişme olan çalışanları idari, fiziki ve teknik güvenlik gibi güvenlik sahalarıyla ilgili Şirket politikaları konusunda olduğu kadar çalışanların Şirkete girdikleri andan itibaren bilmeleri gereken asıl yönetmelikler, yönergeler ve prosedürlerle ilgili olarak da eğitir. CSO böyle bir eğitimin sonuçlarını da yazılı hale getirir.

C. Güvenlik politikalarının değişimi vb. bir sebep olması durumunda, CSO ekibin (departmanın) güvenlik personelini bildirim ya da eğitim yoluyla değişimle ilgili olarak bilgilendirir.

D. Dışarıdan biri görev icabı geldiğinde, CSO bir oryantasyon (eğitim) çalışmasıyla söz konusu kişi göreve başlamadan güvenlik konularında bilgilendirme yapar.

E. Güvenlik Eğitimi ve Farkındalık
Talimatların etkili olabilmesi için düzenli güvenlik eğitimleri ve farkındalık programları da organize edilir.

3.3 Third Party (General Labor Service, Subcontractor Personnel)

A.The subcontractor personnel including general labor service shall prepare and submit a third party security covenant to a contractor. A person in charge of the administration of the contractor shall submit the said covenant to a subcontract service administration department of the Company.

B.A standard contract that the Company defines shall be used. The standard contract shall include the following: to observe security regulations of the Company; for subcontractor personnel and contractor to be responsible for security.

C.In case the technical service or data is exchanged, a contract that includes a phrase to prescribe the fact that a subcontractor shall be an object of security inspection of the Company in order to protect and manage the information assets of the Company.

D. Subcontractor company personnel are prohibited from entering restricted rooms such as the company's archive, data processing room, management office, etc., except for responsible persons. Entry and exit of the specified rooms are protected by a card system and lock.

4.Security Training

4.1 CSO

A.The CSO shall implement security training for all employees more than once a year and, if necessary, may request attendance of CEO.

B.The CSO shall educate new and career employees about the Company policies on security domains such as administrative, physical, and technical security as well as about the major regulations, guidelines and procedures that the said employees shall know upon joining the Company. The CSO shall maintain the results of such education in writing.

C.In case there is reason such as a change of security policies, etc., the CSO shall inform the security staff of team (department) of such change through an announcement or training.

D.In case an outside resides on duty, the CSO shall implement an orientation (training) regarding security prior to the commencement of his or her duties

E. Regular safety training and awareness programs are also organized for the instructions to be effective.

4.1.1 Talimatların Yazılı Olarak Duyurulması
Yazılı Bildirimler: Güvenlik talimatları, tüm çalışanlara yazılı olarak duyurulur. Bu duyurular, genellikle fabrika içindeki duyuru panolarında, e-posta ile veya fabrikadaki iç iletişim platformlarında yapılır.

Duyuru Panoları: Fabrikada çeşitli güvenlik talimatları, acil çıkış planları, tehlikeli alanlar ve iş sağlığı ve güvenliği ile ilgili bilgilere yönelik yazılı duyurular duyuru panolarına asılır.

E-posta ve Dijital Platformlar: Güvenlik talimatları, çalışanlara e-posta yoluyla da duyurulabilir. Ayrıca, fabrikada kullanılan iç iletişim yazılımları veya intranet platformları üzerinden de bu bilgilere kolay erişim sağlanabilir.

4.2 Ekibin (Departmanın) Güvenlik Müdürü
A. Ekibin (departmanın) güvenlik müdürü güvenlik için gerekli olduğunu tespit ederse, iç / dış güvenlik olaylarının meydana gelmesi vb. durumlarda, ekibin (departmanın) güvenlik müdürü ekip üyeleri için güvenlik eğitimi organize edebilir.

B. İç yönetmeliklerde değişiklik gibi iletilmesi gereken bir durum olması halinde ekibin (departmanın) güvenlik personeli ekibe söz konusu durumları bildirir.

5.Emekli Yönetimi
5.1 Personel Departmanı
A. "Emekli Olanlar İçin Ticari Sır Koruma Teminatı Beyanı" emeklilik dokümanlarının içerisinde yer alır ve emekliden talep edilir.

B. Emekli bildirim sözleşmesini veremeyen kişi söz konusu sözleşmeyi göndermeye teşvik edilir. Söz konusu kişi bunun verilmemesi halinde emeklilik işlemlerindeki gecikme ihtimaliyle ilgili olarak da bilgilendirilir.

C. Personel Departmanı emeklinin Şirketle bir konuda karşı karşıya geldiğini fark ederse, söz konusu emeklinin Şirket içerisindeyken edindiği ticari sırların Şirkete verilip verilmediğini teyit eder ve iş değişikliğinin yasaklanması adına ihtiyati tedbir dilekçesi vermek gibi ilgili yasal aksiyonları alır.

D. Personel Departmanı emekli tarafından şirketle ilgili önemli bilgilerin sızdırılmasının önüne geçmek adına güvenliği gözden geçirir.

4.1.1 Written Announcement of Instructions
Written Notifications: Safety instructions are announced to all employees in writing. These announcements are usually made on bulletin boards in the factory, by e-mail or on internal communication platforms in the factory.

Notice Boards: Written announcements regarding various safety instructions, emergency exit plans, hazardous areas and occupational health and safety information are posted on bulletin boards in the factory.

E-mail and Digital Platforms: Safety instructions can also be announced to employees via e-mail. In addition, easy access to this information can be provided through internal communication software or intranet platforms used in the factory.

4.2 Security Manager of Team (Department)
A.In case a security manager of team (department) determines that it is needed for security, such as an occurrence of internal / external security incidents, etc., the security manager of team (department) may implement security training for team members.
B.In case there is a matter to be conveyed, such as changes of internal regulations, security staff of team (department) shall convey such facts within the team.

5. Retiree Management
5.1 Personnel Department
A.The "Retiree Trade Secret Protection Pledge Statement" shall be included in retirement documents and requested from a retiree.

B.A person who fails to submit the retiree notification agreement shall be encouraged to send the said agreement. The said person shall be notified of the possibility of delay in retirement procedures by the said non-submission.

C.In case the personnel department recognizes a fact that a retiree leaves the Company within the same field, the personnel department shall verify whether the trade secrets of the Company that the said retiree has acquired in this Company are provided and take related legal actions, such as petition for preliminary injunction to prohibit a change of employment, etc.

D.The personnel department shall review security in order to prevent critical information from being leaked by a retiree.

5.2 Ekibin (Departmanın)Güvenlik Müdürü

A. Ekibin (departmanın) güvenlik müdürü, şirket içerisinde çalıştığı zamanda edindiği tüm ticari sırların dışarıya hiçbir koşulda sızmaması adına, emekli olması planlanan ya da emekliliği için talimat verilen ekip üyesini bildirme sorumluluğunu üstlenir ve eğer bu yükümlülüğün bir şekilde ihlali olursa "Emekli Olanlar İçin Ticari Sır Koruma Teminatı Beyanı"na göre hukuken ve cezai olarak sorumluluğu oluşabilir.

B. Ekibin (departmanın) güvenlik müdürü emekli olacak kişinin hizmet süresi boyunca edindiği tüm ticari sırları ekibine (departmanına) aktarmasını sağlar ve Şirkete geri aktarmasını talep eder ya da sahip olduğu tüm ticari sırları ortadan kaldırmasını talep eder. Ekibin (departmanın) güvenlik müdürü bu tür durumların hepsini emekli (muhtemel emekli) randevu dokümanları, vb. kaydeder.

5.3 Çalışan

A. Bir çalışanın emekli olan bir kişinin aynı sektörde ya da rakip bir firmada yeni bir iş bulduğunu tespit etmesi durumunda, bu tür durumları gecikmeden Kurumsal Güvenlik Departmanına bildirir.

5.4 Teknik Güvenlik Personeli ve Fiziki Güvenlik Personeli

A. Teknik güvenlik personeli ve fiziki güvenlik personeli emekli olan bir çalışanın system giriş ve sisteme erişim yetkilerini emekli olunan tarihten itibaren en geç 24 saat içerisinde prosedürlere uygun bir şekilde kaldırır.
B. Teknik güvenlik personeli ve fiziki güvenlik personeli emekli olan kişinin yetkilerinin normal bir şekilde geri alınıp alınmadığını periyodik olarak teyit eder. Bir ihmal tespit edilmesi halinde, ihmalin sebebini belirler ve düzeltici aksiyonu alır.
C. Ekibin (departmanın) güvenlik personeli görev ve sorumluluklarının yazılı olarak devrini talep ederse, teknik güvenlik personeli ve fiziki güvenlik personeli yetki kaldırılmasını en fazla iki haftaya kadar askıya alabilir. Yetki kaldırılmasının askıya alınmasıyla ilgili bir sorun oluşması halinde, ekibin (departmanın) güvenlik personeli de bu sorundan sorumlu olur.
D. Yetki kaldırma işleminin emeklilik talimatı vb. Iletilmesinde gecikme olması durumunda olacağı gibi normal şekilde halledilememesi durumunda, teknik güvenlikten sorumlu bir kişi ve fiziki güvenlikten sorumlu bir kişi söz konusu gecikme sırasında giriş / system kayıtlarını teyit eder ve ekibin (departmanın) güvenlik sorumlusunda teyit talep eder. Teknik güvenlikten sorumlu olan kişi ve fiziki güvenlikten sorumlu olan kişi sonuçları CSO'ya rapor eder.

5.2 Security Manager of Team (Department)

A.A security manager of team (department) shall bear an obligation to notify a team member who is scheduled or ordered to retire of the fact that all trade secrets that he or she has acquired during his or her service shall not be leaked to the outside under any circumstances and in case where the aforementioned obligation is violated, he or she may be civilly and criminally liable in accordance with the "Retiree Trade Secret Protection Pledge Statement."
B.A security manager of team (department) shall cause a retiree (prospective retiree) to transfer all trade secrets that he or she has acquired during his or her service to his or her team (department) and request to return to the Company or destroy trade secrets that he or she possesses. The security manager of team (department) shall record such facts in retiree (prospective retiree) interview documents, etc.

5.3 Employee

A.In case where an employee recognizes the fact that a retiree finds a job within the same field or in a competitor, he or she shall notify such facts to the Corporate Security Department without delay.

5.4 Technical Security Staff and Physical Security Staff

A.Technical security staff and physical security staff shall remove a retiree's authority to enter and access to system no later than 24 hours from a retirement order date in accordance with procedures.
B.Technical security staff and physical security staff shall periodically verify whether a retiree's authority is being collected normally. In case an omission is identified, they shall identify cause of the omission and take a corrective action.
C.In case security staff of team (department) requests for the transfer of duties and responsibilities in writing, Technical security staff and physical security staff may suspend the authority removal up to the maximum of two weeks. In case where a problem occurs due to the suspension of authority removal, security staff of team (department) shall also be responsible for such problem.
D.In case where the authority removal is not normally handled due to delay in the posting of the retirement order, etc., a person in charge of technical security and a person in charge of physical security shall verify records of entry / system usage during the said delay and request the confirmation thereof from a person in charge of team (department) security. A person in charge of technical security and a person in charge of physical security shall report the results to CSO.

6. Güvenliği İhlal Edenin Yönetimi
6.1 Güvenlik İhlali İdaresi

A. Minör ihlal olması durumunda, ilgili kişiye ve kendisinin ekip liderine (departmanın yöneticisi) CSO'nun ismi altında bir uyarı verilir. Ciddi bir ihlal söz konusu ise, bu durum CDO'ya rapor edilir ve bununla ilgili olarak işbu yönetmeliğe göre gereken aksiyon alınır.

B. Güvenlik ihlali durumunda, çalışma kuralları ve personel ve güvenlik hükümlerinde yazılı olan disiplin cezası tür ve prosedürlerine göre bir disiplin işlemi uygulanır.

C. Benzer olayların yeniden yaşanması engellemek adına önlemler alınır ve uygulanır. Disiplin işlemlerini sonuçları tüm çalışanlarla paylaşılır.

6.2 Çalışan

A. Bir çalışanın "Bilgi Güvenliği Yönetmeliği" ve ilgili yönerge/prosedürlerin ihlalini fark etmesi durumunda, çalışan durumu Kurumsal Güvenlik Departmanına bildirir.

B. Bir çalışan bilginin kendi hatası sonucunda ya da dikkatsizliği sonucunda açığa çıkarıldığını ya da sızdığını saptarsa, bu durumla ilgili olarak Kurumsal Güvenlik Departmanına bildirimde bulunur.

6.3 İhlal Ciddiyetini Belirleme Standartları

6.3.1 Önemsiz İhlal
A. Kurallar/yönergelerin bir hata ya da yanlışlık sonucunda ihlali fark edildiğinde.

B. Önceden ihlal gerçekleştirmemiş bir çalışan farkında olmadan kuralları/yönergeleri ihlal ederse ve söz konusu ihlal önemli ihlal kategorisinde değilse.

C. İhlali gerçekleştiren kişi kendi ihlalini bildiriyorsa ve söz konusu ihlal önemli ihlal kategorisinde değilse.

D. İhlal edilme sayılarına bağlı olarak önlemler alınır.

D-a) İlk ihlal: İhlal edene sözlü uyarı

D-b) İkinci ihlal: İhlal edene yazılı uyarı (yazılı açıklama) ve ekip liderine (departman yöneticisine) sözlü uyarı

D-c) Üçüncü ihlal: İhlal edene ve ekip liderine (departman yöneticisine) yazılı uyarı (yazılı açıklama)

D-d) Dördüncü ve daha fazla ihlal: Şirket politikalarına kasti olarak uyumsuzluğa bağlı olarak önemli ihlal olarak işlem görür.

6. Management of Security Violator

6.1Security Violation Handling

A.A warning under the name of CSO shall be issued to a relevant employee and his or her team leader (department head) for a minor violation. A major violation shall be reported to CSO and an action shall be taken therefor in accordance with the regulations herein.

B.A disciplinary action for security violation shall be taken in accordance with the types and procedures for disciplinary action that are prescribed in employment rules and personnel or security provisions.
C.The measures to prevent recurrence of similar incidents shall be established and implemented. The results of disciplinary actions shall be notified to all employees.

6.2 Employee

A.In case where an employee recognizes a violation of the "Information Security Regulations" and related guidelines / procedures, he or she shall notify the Corporate Security Department of such facts.

B.In case an employ ascertains that the information is exposed or leaked by his or her mistake or inadvertently, he or she shall notify the Corporate Security Department of such facts.

6.3 Standards to Determine Severity of Violation
6.3.1 Minor Violation
A.In case it is acknowledged that the rules/guidelines are violated due to a mistake or a fault.

B.In case an employee without prior violations violates the rules/guidelines due to unawareness thereof and the said violation does not fall under a major violation.

C.In case a violator notifies his or her violation and the said violation does not fall under a major violation.

D.The measures shall be taken based on the number of times they have been violated.
D-a)First violation: Verbal warning to a violator

D-b)Second violation: Written warning (written explanation) to a violator and verbal warning to a team leader (department head) thereof

D-c)Third violation: Written warning (written explanation) to a violator and a team leader (department head)

D-d)Fourth or more violation: To be treated as a major violation due to an intentional non-compliance of policies

6.3.2. Önemli İhlal

Önemli bir ihlal olması halinde durum Disiplin İşlemi Komitesine iletilir ve söz konusu durum uyarı ya da daha fazlasıyla cezalandırılır.

A. Güvenlik yönetmeliği, prosedürleri veya politikalarını bozucu bir eylem olması durumunda

B. Bir güvenlik olayıyla doğrudan ya da dolaylı olarak algılanabilecek bir durum olması halinde

C. Büyük bir ihmal olması veya aynı ihlalin tekrarlanması hallerinde.

7.Bilgi Varlıklarının Sınıflandırılması

7.1 Sınıflandırmanın Konusu ve Döngüsü

A. Ekibin (departmanın) güvenlik müdürü Şirketin mal varlıklarının sınıflandırılma standardını anlar. Ekibin (departmanın) güvenlik müdürü bilgiyi (dokümanı) söz konusu standartlara dayanarak sınıflandırmak için bilgiyi oluşturan (bir doküman hazırlayan kişiyi) kişiyi fark eder ve kontrol eder.

B. Bir çalışan, sınıflandırma standartlarına dayalı olarak bir dokümanı sınıflandırmak ve Şirketin güvenlik politikalarına uyum sağlamak adına, sınıflandırma standartlarını bilir ve dokümanları her zaman sınıflandırılmış bir şekilde tutar.

C. Bir ekibin içerisindeki görevlerin değişmesi durumunda, ekibin (departmanın) güvenlik personeli sınıflandırma standartlarını söz konusu değişiklikler bakımından iki haftadan geç olmayacak şekilde inceler ve düzenler. Ekibin içerisinde görev değişikliği olmasa bile, ekibin (departmanın) güvenlik personeli sınıflandırma standartlarını altı ayda bir düzenli olarak inceler ve düzenler.

D. Sınıflandırılan bilgi varlıkları bir yönetici, varlık numarası, saklama yeri, vb. bilgilerin de eklenmesiyle yönetilir.

6.3.2. Major Violation

A major violation shall be referred to the Disciplinary Action Committee and punished by warning or more.

A.In case of an act to intentionally circumvent security regulations, procedures or policies

B.In case of a matter that is recognized to be directly or indirectly related to a security incident

C.In case of gross negligence or the same violation has been repeatedly pointed out.

7.Classification of Information Assets

7.1 Subject and Cycle of Classification

A.A security manager of team (department) shall understand the property classification standards of the Company. The security manager of team (department) shall notice and check for the person who generates information (a person who prepares a document) to classify the information (document) on the basis of the said standards.

B.An employee shall recognize the classification standards and manage documents in a classified state at all times in order to classify a document that is being prepared based on the classification standards and to comply with security policies of the Company.

C.In case of the changes of duties within a team, security staff of team (department) shall review and adjust the classification standards no later than two weeks from the said changes. Even if there is no changes of duties within a team, security staff of team (department) shall regularly review and adjust the classification standards once per six months.

D.The classified information assets shall be managed by attaching an index which may identify an administrator, property number, storage location, etc.

7.2 Bilgi Varlıklarının Bölümleri

A. Bilgi varlıkları “Sır”, “Kısıtlı” ve “”Halka Açık” olarak bölümlere ayrılır.

B. "Sır" veya "Kısıtlı" bilgiler Şirketin ticari sırları ve "Bölüm 8 Ticari Sırları Yönetme Standartları” olarak ikiye ayrılır ve ilgili hükümlere uyulur. “Halka Açık” doküman yönetilen konudan çıkarılır.

C. "Kısıtlı" bilgi tüm çalışanların kullanabileceği veriler anlamına gelir ancak bunun dışarıya çıkması Şirkete zarar verebilecek ya da zararlı sonuçlar getirebilecektir.

D. "Sır" bilgileri görevleri sadece ilgili olan çalışanların kullanabileceği veriler anlamına gelir ve bunların dışarıya çıkması Şirket için önemli kayıplara, bir iş planının bırakılması ya da değişmesi, iş kayıpları vb. sebep olabilir.

E. "Halka Açık" bilgiler dışarıya çıkması ya da verilmesi önemli bir soruna sebep olmayacak ve halka açık duyurular gibi paylaşım için oluşturulan veya Internet araştırmasıyla kolayca erişim sağlanabilecek vb. veriler anlamına gelir.

F. Bir çalışanın hazırladığı tüm dokümanlar (sözleşmesel ilişki kurulan kişi dahil olmak üzere) sınıflandırılma öncesi “Kısıtlı” olarak işlem görür ve ilgili hükümler uygulanır.

G. Bir güvenlik sınıfının ek olarak tahsis edilmesi durumunda, “çok gizli” seviyesi atanabilir ve CSO onayı ile kullanılabilir.

H. Dışarıdan gelen bir dokümanı sınıflandırma standartları CSO’nun ön onayı ile oluşturulur ve uygulanır.

7.3 Bilgi Varlıklarının Yönetimi

A. Kurumsal Güvenlik Departmanı bilgi varlıklarını sınıflandırmak için, ekibin (departmanın) hazırlayabileceği, standartlar (şablon) oluşturur.

B. Kurumsal Güvenlik Departmanı ekip (departman) tarafından yılda birden fazla kere tutulan bir bilgi varlığı listesi yapar ve yönetir, ve etkinliğini az ya da aşırı sınıflandırma duurmlarını kontrol ederek teyit eder.

7.2 Division of Information Assets

A.The information assets shall be divided into "Secret," "Restricted" and "Public."

B."Secret" or "Restricted" information shall be classified as trade secrets of the Company and "Chapter 8. Standards to Manage Trade Secrets" and related provisions shall be complied. "Public" document will be excluded from the object to be managed.

C."Restricted" information refers to the data that all employees may use but whose exposure to the outside is likely to cause damages or bring about harmful consequences to the Company.

D."Secret" information refers to the data that only employees whose duties are related to may use and whose exposure to the outside is likely to cause substantial losses to the Company, abandonment or amendment of a business plan thereof, business losses, etc.

E."Public" information refers to the data whose exposure or disclosure to the outside is not likely to cause any special problem and which are generated for disclosure, such as public announcement or which may be easily accessed through Internet search, etc.

F.All documents that an employee (including a person in privity of contract) prepares shall be treated as "Restricted" information prior to classification thereof and related provisions shall be complied.

G.In case a security class shall be additionally assigned, "top secret" level may be assigned and used with the approval of the CSO.

H.The standards to classify an outside document shall be established and operated with a prior approval of the CSO.

7.3 Management of Information Assets

A.The Corporate Security Department shall provide the standards (template) to classify information assets, which a team (department) may prepare.

B.The Corporate Security Department shall collect and manage information assets list that is apprehended by a team (department) more than once a year and validate its effectiveness by checking under or excess classification therein.

8. Ticari Sır Yönetimi Standartları

8.1 Ticari Sırların Korunması ve Yönetimi

A. Asıl bir ticari sır dokümanı hazırlanması sırasında bir seviyede işaretlenir ve orta derecede ya da bir kısım ticari sır kullanan bir doküman da yine aynı yöntemle yönetilir. Halihazıra bir güvenlik sınıfı olmaksızın hazırlanan bir doküman geçmişe dönük olarak sınıflandırılır.

B. Basımı alınmış olan ticari sırların beher sayfasına, kolayca ayrıştırılması adına, bir güvenlik sınıfı işareti konur. Basımı alınan ticari sırların güvenlik sınıfı işareti koyulmamış olan beher sayfasına bir mühürle güvenlik sınıfı işareti konur.

C. Basımı alınmış olan ticari sırlar açık bir yerde değil, kilitli bir yerde dosyalanır. Ekibin (departmanın) güvenlik müdürünün belirleyeceği bir kişi basımı alınan ticari sırları yönetir.

D. Basımı alınmış olan ticari sırların saklama süresinin dolması halinde, ticari sırlar tekrar eski konumuna gelmemeleri adına bu sürenin sona erme tarihinden en geç bir ay sonra yok edilir. Ancak basımı alınmış bir ticari sırrın imhasının ertelenmesinin gerekli olması şartıyla, basımı alınmış olan ticari sır karardan sonra saklanır ve erteleme süresi güvenlik departmanın rapor edilir.

E. Bir ticari sırrın çalışanın kontrol edemeyeceği çöp, ortak konferans odası vb. herhangi bir yerde bırakılması durumunda, söz konusu ticari sırrın basımını alan personel ve kendisinin ekip lideri için güvenlik yönetmeliği ihlali işlemi başlatılır.

8.2 Ticari Sırrın İletimi

A. Bir kişinin pozisyonundaki değişikliğe bağlı olarak ticari sırrı elinde bulundurmasına gerek kalmazsa, söz konusu kişi "İş Devir Teslim Formu" doldurur ve elektronik doküman, basılı doküman, vb. tüm ticari sır türlerini devralan kişiye devreder.

B. Ekibin (departmanın) güvenlik müdürü bir ticari sırrın devralma / devretme prosedürlerine uygun olarak düzgün bir şekilde iletilip iletilmediğini ve ticari sırrı elinde bulunduran kişinin ticari sırrı imha edip etmediğini teyit eder.

8. Standards to Manage Trade Secrets

8.1Custody and Management of Trade Secrets

A.An original document of trade secret shall be marked with a level at the time of its preparation and a document which uses an intermediate or a part of trade secret shall be managed with the same method. A document already prepared without a security class shall be classified retroactively.

B.A security class shall be marked on each page of printed trade secrets so as to be easily identified. A security class shall be marked using a stamp on each page of the printed trade secretes that is printed without it.

C.The printed trade secrets shall be filed not in an open place but in a locked place. A person that the security manager of team (department) designates shall manage the printed trade secrets.

D.In case a retention period of a printed trade secret expires, it shall be destroyed so as not to be restored no later than one month from the expiration date thereof. Provided, however, that it is necessary to postpone the destruction of a printed trade secret, the printed trade secret shall be stored after the purpose and the period of postponement shall be reported to a security department.

E.In case a trade secret is left in a place, such as trash can, common conference room, etc., which an employee may not control, an action for the violation of security regulations shall be taken against a person who prints the trade secret and a team leader thereof.

8.3 Transfer of Trade Secret

A.In case a person does not need to possess a trade secret due to the change in position, the person shall prepare the "Work Handover Form" and hand over all types of trade secrets, such as electronic document printed document, etc. to the person who takes over.

B.A security manager of team (department) shall verify whether a trade secret is appropriately transferred in accordance with taking over / hand over procedures and whether a trade secret that a person who hands over the trade secret possesses is destroyed.

C. Ticari sır devrinin olduğu departmanın devredilen ticari sırların bir kısmını kullanması gerekirse, söz konusu departman söz konusu ticari sırları devreden ekibin (departmanın) güvenlik müdürüne kullanım amacı ve bir dosya listesini yazılı olarak rapor etmesi sonrasında kullanabilir. Bir ticari sırrın devredileceği departman ticari sırrı yazılı bir rapor olmadan elinde bulundurursa, sebeplerinden bağımsız olarak güvenlik ihlaliyle ilgili yönetmeliğe göre kasti bilgi edinme söz konusu olacağından departman için işlem başlatılır.

8.3 Ticari Sırrın Dağıtımı ve Dışarı Çıkarılması

A. İşle direkt ya da dolaylı olarak ilgili olmayan bir ticari sırrın dışarı çıkması durumunda ya da bir devlet kurumunun ticari sırrı talep etmesi durumunda, ticari sır CSO ön onayı olmaksızın dışarı çıkartılır.

B. Önceki maddede iletilen durumda, ticari sırrı dışarı çıkartan yer, dışarı çıkarma tarihi, dışarı çıkarma detayları vb. Şirketin hazırladığı bir forma uygun olarak hazırlanır ve bu da ekibin (departmanın) güvenlik müdürüne rapor edilir ve alınan onayla saklanır. Ancak, teknik verilerin (çizimin) kabul edileceği bir sistem halihazırda geliştirilmişse, bir sistem kaydı ayrı olan kayıtların yerine geçer.

C. Ticari sırları dışarı çıkarma detayları bunların iki yıl ya da daha fazla süre boyunca kolayca geri alınabileceği bir durumda saklanır ve yönetilir. Bir ticari sırrın içerde dağıtımı gerektiğinde, ticari sır, ticari sırrı elinde bulunduran (hazırlayan) kişinin belirlenmesine dayalı olarak Şirketin tanımladığı koruyucu önlemlere uygun şekilde, sadece buna ihtiyacı olan kişiye verilir.

D. Bir kişi kendi hazırlamadığı ticari sırrı dağıtmaz ya da dışarı çıkarmaz. Söz konusu kişi ticari sırrın dağıtımı ya da dışarı çıkarılması için hazırlayan kişiden onay ya da talebini alır.

8.4 Ticari Sırların İmhası

A. Elektronik doküman halinde ya da bu şekilde bir kopyası olan bir ticari sır Şirket'in belirlediği bir yazılım kullanılarak geri dönülmez bir şekilde imha edilir.

B. Elektronik doküman formatı dışında bir formatta olan bir ticari sır bir kağıt imha makinesi kullanılarak tamamen ve tanımlanamaz bir şekilde imha edilir. Bir çalışanın kullandığı bir kağıt imha makinesi kurulu değilse, CSO farklı imha prosedürleri belirler ve uygulanmasını sağlar.

C. Elektronik doküman imhası için bir yazılım belirlenmemesi ya da bildirilmemesi durumunda, CSO imhadan sorumlu olacak kişidir.

C.In case a department in which a trade secret is transferred needs to use a part of the transferred trade secrets, the said department may use the said trade secrets after it has reported its purpose of use and a file list to the transferring security manager of team (department) in writing. In case a department to which a trade secret is transferred possesses the trade secret without a written report, an action shall be taken against the department as an intentional information acquisition in accordance with the regulations related to security violation irrespective of the causes.

8.3 Distribution and Taking Out of Trade Secret

A.In case a trade secret shall be taken out to a place which is not directly or indirectly related its business or a governmental institution requests a trade secret, the trade secret shall be taken out with a prior approval of the CSO.

B.In case of the former case, the place that takes out a trade secret, date of taking out, details of taking out, etc., shall be prepared in accordance with a form that the Company prescribes, which is reported to a security manager of team (department), and stored with an approval thereof. However, in case a system to distribute / accept the technical data (drawing) is already developed, a system log will substitute the separate records.

C.The details of taking out the trade secrets shall be stored and managed in a state in which they can be easily retrieved for two years or more. In case a trade secret shall be distributed internally, the trade secret shall be distributed only to a person who needs the trade secret in accordance with the protective measures that the Company defines based on determination of a person who possesses (prepares) the trade secret.

D.A person may not distribute or take out a trade secret that he or she does not prepare. The said person shall get an approval or request for the distribution or the taking out of the trade secret from a person who prepares.

8.4 Destruction of Trade Secrets

A.A trade secret in a form of an electronic document and a copy thereof shall be irrecoverably destroyed using a software that the Company defines.

B.A trade secret in a form other than an electronic document shall be utterly and unidentifiably destroyed using a paper shredder. In case a paper shredder that an employee may use is not installed, the CSO shall establish and operate separate destruction procedures.

C.In case a software for electronic document destruction is not designated or notified, the CSO shall bear responsibility for the destruction thereof.

9. Uyum

A. Güvenlikle alakalı kanun maddelerinin revize edilmesi ya da bir müşteri şirketinin güvenlik yönetmeliğinde değişiklik yapılması durumunda, Kurumsal Güvenlik Müdürü, Kurumsal Güvenlik Personelinden bunun iç yönetmelikler, prosedürler ve politikalar üzerinde yarattığı etkiyi incelemesini ve gerekirse iç yönetmelikler, prosedürler ve politikaları revize etmesini talep eder.

B. Revizyonun gerekmediği kanaatine varılması durumunda, inceleme detayları yazılı hale getirilir.

C. CSO kanun maddeleri, müşteri şirketin politikaları vb. yapılan revizyonları iç yönetmeliklerin revizyonuyla beraber resmi bir bildiri kanalıyla ya da duyuru panosunda konuya yer vererek duyurur. Gerekirse, CSO ayrı bir eğitim planlaması yapar.

D. Teknik güvenlik personeli sistem hasar görebilirliğini periyodik olarak inceler ve iç yönetmeliklerin ya da dış kanunların ihlalinin söz konusu olup olmadığını teyit eder. Bir geliştirmenin gerekli olması durumunda, bunu Kurumsal Güvenlik Müdürü ve CSO'ya rapor eder ve önlem alır.

10.Güvenlik Denetimleri

10.1 Amaç

Güvenlik denetimlerinin amacı olası bilgi güvenliği ihlali riskini ve söz konusu ihlal dolayısıyla oluşabilecek zararları, Şirket'in belirlediği güvenlik kontrolünün düzgün bir şekilde uygulanıp uygulanmadığını teyit ederek, en aza indirgemektir.

10.2 Uygulama Konusu ve Döngüsü

A. CSO güvenlik denetimlerini önceden yapılan plana göre uygular ve Kurumsal Güvenlik Müdürü CSO onayıyla güvenlik denetimlerini gerçekleştirecek bir çalışan atar.

B. Güvenlik denetimleri çeyrekler bazında düzenlenir.

C. Güvenlik denetimleri esas olarak bir çalışanın rutin olarak uygulaması gereken durumlar için düzenlenir.

D. Yukarıda belirtilenden ayrı olan güvenlik denetimleri aşağıdaki koşullarda düzenlenebilir:

D-a) CSO'nun gerekli görmesi durumunda;

D-b) Bir güvenlik olayının olması ya da olma ihtimali olması halinde;

9. Compliance

A. In case where security related laws are revised or the security regulations of a client company are altered, the Corporate Security Manager shall request the Corporate Security Staff to review effect thereof on internal regulations, procedures and policies and, if necessary, revise internal regulations, procedures and policies.

B. In case it is determined that the revision is not necessary, the details of the review shall be maintained in writing.

C. The CSO shall announce the revisions of laws, policies of the client company, etc., with the revision of internal regulations through an official notice or by posting it on the bulletin board. If necessary, the CSO shall implement a separate training.

D. Technical security staff shall examine the system vulnerability periodically and verify whether there is a violation of internal regulations or external laws. If an improvement is necessary, he or she shall report such facts to the Corporate Security Manager and the CSO and take measures.

10.Security Inspections

10.1 Purpose

The objective of security inspections is to minimize the risk of potential information security intrusion and the damages caused by the said intrusion by verifying whether the security control that the Company prescribes is properly implemented.

10.2 Subject and Cycle of Implementation

A.The CSO shall implement the security inspections in accordance with a prearranged plan and the Corporate Security Manager shall nominate an employee to implement the security inspections with the approval of the CSO.

B.The security inspections shall be implemented quarterly.

C.The security inspections shall be implemented mainly for matters that an employee shall comply with routinely.

D.The separate security inspections other than those specified above may be implemented under the following circumstances:

D-a)In case the CSO acknowledges as necessary;

D-b)In case a security incident occurs or is likely to occur;

10.3 Güvenlik Denetimlerinin Amacı

Güvenlik denetimleri 1.2 Uygulama Kapsamı bölümünde belirtilen kapsamda uygulanabilir.

10.4 Güvenlik Denetimleri Uygulaması

A. Bir çalışan güvenlik denetimi talebini sebepsiz yere ertelemez ya da reddetmez. Bir çalışan, sadece CSO'ya önüne geçilemez durumları yazılı olarak rapor ettiğinde ve CSO da bu ayarlamayı onayladığında, zaman planlamasını yapabilir.

B. Güvenlik denetiminin tamamlanması halinde, Kurumsal Güvenlik Müdürü sonuçlarını CSO'ya bildirir. Önemsiz bir ihlalle ilgili olarak Kurumsal Güvenlik Müdürü bir ekibin (departmanın) güvenlik müdüründen bunun düzeltilmesini talep eder.

C. Ekibin (departmanın) güvenlik müdürü talep edilen düzeltme işlemiyle ilgili tedbir yöntemi / planını Kurumsal Güvenlik Müdürüne tekrarlar ve plana uygun olarak düzeltme önlemlerini tamamlar ve tamamlanmasını takiben Kurumsal Güvenlik Müdürüne bilgi verir. Önlemler talep edilmesinden sonra en geç dört hafta içerisinde tamamlanır. Kurumsal Güvenlik Müdürü dört haftadan fazla süreceğini belirlerse, bunu ayrıca CSO'ya Kurumsal Güvenlik Personeli üzerinden rapor eder.

D. Kurumsal Güvenlik Müdürü bir ekibin (departmanın) talep ettiği düzeltmelerin tamamlandığını teyit ederse, düzeltmelerin tamamlandığını CSO'ya rapor eder. Ancak bu geliştirmelerin tamamlandığının rapor edilmesi güvenlik denetiminin tamamlanmasından en geç 30 gün sonra yapılmış olacaktır. Eki (departman) dört hafta içerisinde söz konusu tamamlanma işlemini bildiremezse, bu "aksiyonsuz" olarak kabul edilir.

E. Kurumsal Güvenlik Müdürünün güvenlik denetimi sonucunda önemli bir ihlal belirlemesi durumunda, bunu CSO'ya rapor eder ve Şirket yönetmeliğinde açıklanan prosedürlere göre aksiyon alır.

10.3 Object of Security Inspections

The security inspections may be implemented for a scope that is prescribed 1.2 Scope of Application herein.

10.4 Implementation of Security Inspections

A.An employee shall not postpone or refuse to security inspection request without a just cause. An employee may adjust schedules only if he or she reports unavoidable circumstances to the CSO in writing and the CSO approves the said adjustment.

B.In case a security inspection is completed, the Corporate Security Manager shall report its results to the CSO. With respect to a minor violation, the Corporate Security Manager shall request its improvement from a security manager of team (department).

C.A security manager of team (department) shall replay to a method / schedule of measures with respect to the requested improvement to the Corporate Security Manager and complete the improvement measures by taking measures in accordance with the plan and notifying the Corporate Security Manager of its completion. The measures shall be completed no later than four weeks from the date of request. If the Corporate Security Manager determines that it will take more than the said four weeks, he or she shall separately report such facts to the CSO through the Corporate Security Staff

D.In case the Corporate Security Manager verifies the completion of improvements that a team (department) requests, he or she shall report the completion of improvements to the CSO. However, the said report of improvement completion shall be reported no later than 30 days from the completion date of the security inspection. The team (department) that fails to notify the completion no later than four weeks shall be handled as "no action."

E.In case where the Corporate Security Manager determines as a major violation through a security inspection, he or she shall report such facts to the CSO and take actions in accordance with the procedures prescribed in the regulations of the Company.

F. Tüm güvenlik denetimlerinin sonuçları ve ihlal edenlere karşı olan aksiyonlar üç yıl boyunca ya da daha fazla süre muhafaza edilir.

G. Bir güvenlik denetiminin uygulanmaması veya önemli bir ihlale karşı aksiyon alınmasının ihlali halinde, CSO buradaki sorumluluğu üstlenir ve bu tğr durumlar güvenlik denetimleri / Müşteri olan bir şirketin denetimi için dezavantaj olarak not edilir.

Fiziki Güvenlik
11. Koruma Alanı Tahsisi

A. "Koruma alanı" sır korumasının gerekli olduğu alan anlamına gelmektedir. Koruma alanı "sınırlı alan" ve "kısıtlı alan" olarak sınıflandırılır ve ayrıca koruma alanının detaylı bir şekilde yönetimi için "iş yeri alanı" olarak da sınıflandırılabilir.

B. Sınırlı Alan: Güvenlik için önemli olan bir alan ya da sadece orada ikamet eden bir çalışanın erişimine izin verilen alan. Yetkisi olmayan birinin girişinin engellenmesi adına sınırlı alanın yönlendirmesinin olması gerekir.

C. Kısıtlı Alan: Aşırı derecede önemli olan bir alandır ve yetkisi olmayan kişinin girişi yasaktır. Yetkisiz bir kişi sadece yönetimden olan bir kişinin ön onayıyla kısıtlı alana giriş sağlayabilir.

D. İş Yeri Alanı: Sır olan, kritik derece önemi olan tesisleri, materyalleri, önemli dokümanları vb. korumak adına genel bir ziyaretçi üzerinden gözetimin gerekli olduğu alandır. Bir ziyaretçi ayrı bir onay olmadan iş yeri alanına girebilse bile, iş yeri alanı Şirket'in güvenlik yönetiminin kapsamındadır.
Tesis Bina Yapısı : Tesis binası 39500 metrekare arsa üzerine 14830 metrekare alan şeklinde etrafı 2,5 metre yüksekliğindeki çitlerle çevrili, giriş kapısı güvenlik kontrolünde olan çelik konstrüksiyon yapıdan oluşmaktadır. Kaçak girişleri engelleyecek türde dayanıklı malzemeden inşa edilmiştir.

F.The results of all security inspections and actions against violators shall be maintained three years or more.

G.In case where a security inspection is not implemented or an action against a major violation is neglected, the CSO shall bear responsibility therefor and such facts may be the grounds for disadvantages in security inspections / audit of a client company.

Physical Security
11**. Institution of Protection Area**

A."Protected area" means the area where the protection of secrets is required. The protected area is classified as "restricted area" and "restricted area" and can also be classified as "workplace area" for detailed management of the protected area.

B.Restricted Area: An area that is important for security or an area that is only allowed to an employee residing there. The restricted area must have a direction to prevent unauthorized access.

C.Restricted Area: An area that is extremely important and unauthorized access is prohibited. An unauthorized person can only enter the restricted area with the prior approval of a management person.

D.Workplace Area: An area where surveillance is required over a general visitor to protect secret, critically important facilities, materials, important documents, etc. Even if a visitor can enter the workplace area without separate approval, the workplace area is within the scope of the Company's security management. Facility Building Structure: The facility building is built on a 39,500 square meter land with an area of 14,830 square meters, surrounded by 2.5 meter thick fences, and consists of a steel construction structure with a security-controlled entrance gate

E. Ziyaretçi Girişinin Takibi ve İzlenmesi

Gelen ziyaretçinin güvenlik personeli tarafından kaydı yapıldıktan sonra geçici ziyaretçi kartı verilir. Geçici ziyaretçi kartı ile ziyaretçinin girebileceği alanlar kısıtlandırılır, yalnızca ilgili alanlar için giriş izni karta tanımlanır.

Ziyaretçilerin, fabrikanın farklı katlarına giriş-çıkışları güvenlik sistemi tarafından izlenir. Ziyaretçilerin hangi alanlara ve katlara erişim sağladığı, İnsan Kaynakları departmanı tarafından kontrol edilir.

Ziyaretçilerin katlara girişlerini kontrol etmek amacıyla, fabrika ofislerinde kartlı geçiş sistemleri kullanılır. Bu sistemler, ziyaretçilerin belirli bölgelere geçiş yaparken, güvenlik sistemleri aracılığıyla erişim iznini denetler.

11.1 Koruma Alanının Belirlenmesi

A. İş yeri güvenlik müdürü sır koruma durumunun önemine bağlı olarak koruma alanını belirler.

B. Ticari sırların ve Şirket'in mal varlıklarının korunması adına ziyaretçinin sınırlı olarak erişimi olan bir alan sınırlı alan vb. olarak belirlenir. Bir çalışan ve bir ziyaretçi bu alana prosedürlere göre onay almaları sonrasında erişim sağlayacaklardır.

C. Yetkisiz bir kişinin koruma alanına erişimini engellemek adına bir denetim ekipmanı kurulur ve koruyucu aksiyon alınır. Erişim kayıtları muhafaza edilir.

D. Sır koruması için bir çalışanın erişiminin denetlenmesi gereken bir alan Kısıtlı Alan olarak belirlenir. Resim çekmek ve yetkisiz bir çalışanın erişimi yasaktır.

E. Fiziki güvenlik personeli ekibin (departmanın) güvenlik müdürünün görüşünü alarak kısıtlı alanı tahsis eder, bu durumu Kurumsal Güvenlik Müdürüne rapor eder ve Kısıtlı alanın belirlenmesini sağlar.

F. Şüpheli Durumun Tespiti: Yetkisiz girişten şüphelenilen kişi veya taşıtlar tespit edilir. Şüpheli davranışlarda bulunan kişiler ya da normalden farklı hareket eden taşıtları dikkatle izlenir. Örneğin, araçların park yeri dışına park etmesi veya kişilerin güvenlik alanlarına izinsiz yaklaşması gibi.

E. Monitoring and Tracking of Visitor Entry

After the visitor is registered by the security personnel, a temporary visitor card is given

Visitors' entrances and exits to different floors of the factory are monitored by the security system. The Human Resources department controls which areas and floors visitors have access to.

Card pass systems are used in the factory offices to control visitors' entrances to floors. These systems monitor visitors' access permissions through security systems as they pass through certain areas.

11.1 Definition of Protection Area

A.A business location security manager shall designate a protection area based on the importance of secret protection.

B.An area to which an access of a visitor shall be limited to protect the trade secrets and the properties of the Company shall be designated as a limited area, etc. An employee and a visitor shall access thereto after receiving an approval in accordance with the procedures.

C.A control equipment shall be installed and a protective action shall be performed to prevent an unauthorized person from accessing to the protection area. Access records shall be maintained.

D.An area to which an access of an employee needs to be controlled for secret protection shall be designated as the Restricted Area. Taking pictures and access of an unauthorized employee shall be prohibited.

E.Physical security staff shall institute the restricted area by collecting the opinion of the security manager of team (department), report such facts to the Corporate Security Manager, and implement the designation of the Restricted Area.

F. Detection of Suspicious Situation: Persons or vehicles suspected of unauthorized entry are detected. Persons behaving suspiciously or vehicles behaving differently than usual are carefully monitored. For example, vehicles parking outside parking areas or people approaching security areas without permission.

G. İhbarın Yapılması: Şüpheli kişi veya taşıt tespit edildikten sonra, durum anında güvenlik merkezine bildirilir. Bu bildirim, telefon aracılığı ile duyuru panolarında bulunan şüpheli durum ihbarı +90 262 310 10 87 numarasına yapılır.

H. İhbarın kayda alınması: İhbar edilen kişinin veya taşıtın detayları (kimlik bilgileri, araç plaka numarası, şüpheli hareketler, saat ve yer gibi) kayda alınır. Bu bilgiler, ileride yapılacak soruşturmalar için kullanılabilir.

I. Fiziksel Güvenlik Önlemleri:

Fiziksel güvenlik önlemleri dış sınırların kapsamlı bir şekilde korunması, izinsiz giriş ve çıkışların engellenmesi amacıyla tasarlanmıştır.
Tesisin dış sınırının güvenliği beton üzerinde bulunan çit, giriş ve çıkışlarda bulunan bariyer ve sürgülü demir kapı, kapalı devre kamera sistemi ile sağlanmaktadır.

Çitler ve Bariyerler: Tesisin dış sınırları çevresinde yüksek güvenlikli beton duvar üzerinde çitler bulunur.

Güvenlik Kapıları: Giriş ve çıkışların kontrollü bir şekilde yapılabilmesi sağlayan güvenlik kapıları, turnikeler, açılır kapanır bariyer ve sürgülü demir kapılar bulunur.

İ. Fiziksel Güvenlik Önlemleri ve Kontrolü
Tesisin dış sınırları çevresinde yer alan çitler, duvarlar veya bariyerler izlenir ve herhangi bir hasar, zayıf nokta veya aşınma tespit edilirse hemen tesis bakım personelleri tarafından onarılır.

Güvenlik personeli, günlük olarak düzenli aralıklarla (fabrikanın tatil günlerinde yemek saatleri hariç saatte bir olarak toplamda 21 defa, tatil olmayan günlerde 21.00-05.00 saatleri arası 8 defa) devriye gezerek çitlerin veya bariyerlerin sağlamlığını kontrol eder. Güvenlik görevlisi, belirlenen rotaya uygun olarak hareket eder ve her kontrol noktası için devriye kalemini ilgili etiket veya sensöre tutarak kaydeder. Bu işlem, görevlilerin tüm noktaları kontrol ettiğini doğrular. Kalem okuma yaptıktan sonra, her kontrol noktasına ait veriler (zaman, tarih, konum) cihazın belleğinde saklanır. Bu veriler, güvenlik yöneticisi tarafından raporlama amacıyla kullanılabilir.

Aydınlatma ve güvenlik ekipmanlarının bakımı ve kontrolü tesis bakım personelleri tarafından elle ve gözle, ölçü aletleri ile kontrol edilerek yapılmaktadır. Bakım işleri aylık periyotlar halinde düzenlenir ve yapıldıktan sonra form tutulur.

G.Reporting: After the suspicious person or vehicle is detected, the situation is immediately reported to the security center. This notification is made via telephone to the suspicious situation report number on the bulletin boards at +90 262 310 10 87.

H.Recording the report: Details of the person or vehicle reported (such as identity information, vehicle license plate number, suspicious movements, time and location) are recorded. This information can be used for future investigations.

I. Physical Security Measures:

Physical security measures are designed to prevent unauthorized entry and exit in order to further protect the external borders.
The security of the outer border of the facility is provided by a concrete fence, a barrier and sliding iron gate at the entrances and exits, and a closed circuit camera system.

Fences and Barriers: There are fences on the high-security concrete wall around the external borders of the facility.

Security Gates: There are security gates, turnstiles, retractable barriers and sliding iron gates that allow controlled entry and exit.

İ. Physical Security Measures and Control
Fences, walls or barriers located around the outer boundaries of the facility are monitored by cameras and if any damage, weakness or wear is detected, they are repaired immediately by facility team members.

Security personnel patrol regularly and check the integrity of the fences or barriers. (Total of 21 times a day, excluding meal times on holidays, and 8 times a day between 21:00-05:00 outside of holidays.) The security officer moves in accordance with the determined route and records each checkpoint by holding the patrol pen to the relevant tag or sensor. This process confirms that the officers have checked all points. After the pen reads, the data (time, date, location) of each checkpoint is stored in the device's memory. This data can be used by the security manager for reporting purposes

Maintenance and control of lighting and security equipment is carried out by facility maintenance personnel through manual and visual inspection. Maintenance work is organized in monthly periods and a form is kept after completion.

Aydınlatma ve güvenlik ekipmanlarının kontrolü sonrası arıza veya olumsuz bir durum ile karşılaşılması durumunda arıza bildirim formu tutularak tesis bakım personellerine konu ile ilgili bilgi verilir. Tamir işlemi tesis bakım personellerince gerçekleştirilecek olup işlemin zaman alacak olması halinde arızalı ekipman elde sürekli yedek tutulan ekipman ile değiştirilir. Gerekli görüldüğü takdirde arızalı ekipmanın olduğu bölgede güvenliğin arttırılması amacıyla güvenlik personeli görevlendirilir.

11.2 Koruma Alanının İşaretlemesi

A. Koruma alanı işaretlemesi, koruma alanına giriş yapılması esnasında kolay bir şekilde tanınabilmesi adına, giriş kapısının merkezine ya da düz bir yere yapılır.

B. Koruma alanı Tesis Koruması ve Erişim Denetimi Yönergelerindeki Madde 3.3.2'ye göre işaretlenir.

11.3 Koruma Alanının İhlali

1. İhlalin Tespiti

Dış sınırda meydana gelen herhangi bir ihlal, güvenlik sistemleri (kameralar, sensörler, devriye kalemi, vb.) aracılığıyla tespit edilir. Ayrıca, güvenlik görevlilerinin devriye sırasında gözlem yaparak fark ettiği durumlar da ihlal olarak kaydedilir.

2. İhlal Durumunda İlk Müdahale

İhlal tespit edildikten sonra, güvenlik personeli hemen durumu değerlendirmek ve müdahale etmek için harekete geçer.

İhlalin Yeri ve Türü: İhlalin gerçekleştiği alan belirlenir (örneğin, çitin aşılması, kapının izinsiz açılması). Olayın türü (kötü niyetli giriş, hırsızlık, vandalizm vb.) tanımlanır.

Müdahale için Güvenlik Ekibi: Güvenlik görevlisi, belirli acil müdahale prosedürlerine uygun olarak, olay yerine en yakın güvenlik ekibini yönlendirir. Acil durumlarda güvenlik personelinin hızlı müdahale etmesi önemlidir.

3. Acil Durum Planı ve Yardım Çağrısı

İhlalin büyüklüğüne göre, önceden belirlenmiş acil durum planı devreye sokulur. Eğer dış sınır ihlali, yüksek tehdit seviyesine sahipse (örneğin, silahlı saldırı veya terör saldırısı), güvenlik ekibi ve yerel kolluk kuvvetleri ile iletişim kurulur.

İhlal durumu, tesisin yöneticilerine ve yerel güvenlik güçlerine (polis, jandarma) hemen bildirilir.

İhlal durumunun büyüklüğüne göre, iç güvenlik ekiplerinin ve kolluk kuvvetlerinin koordinasyonu sağlanır.

Tehdit altındaki alanlar tahliye edilir veya geçici olarak güvenlik önlemleri artırılır (örneğin, alanın kapatılması, yol blokajları).

If a malfunction or negative situation is encountered after the control of lighting and security equipment, a malfunction notification form is kept and the facility maintenance personnel are informed about the issue. If the repair process will take a long time, it is replaced with a spare equipment that is always kept on hand.

11.2 Marking of the Protection Area

A. The protection area marking is made at the center of the entrance gate or on a flat area so that it can be easily recognized when entering the protection area.

B. The protection area is marked in accordance with Article 3.3.2 of the Facility Protection and Access Control Directives.

11.3 Violation of the Protection Area

1. Detection of Violation

Any violation occurring at the outer border is detected by security systems (cameras, sensors, patrol pens, etc.). In addition, situations noticed by security officers during patrols are also recorded as violations.

2. First Response in the Event of a Violation

After a violation is detected, security personnel immediately take action to assess and intervene.

Location and Type of Violation: The area where the violation occurred is determined (e.g., breaching a fence, opening a gate without permission). The type of incident (malicious entry, theft, vandalism, etc.) is defined.

Security Team for Response: The security officer directs the nearest security team to the scene in accordance with specific emergency response procedures. In emergencies, it is important for security personnel to intervene quickly.

3. Emergency Plan and Call for Help

A predetermined emergency plan is activated according to the magnitude of the breach. If the external border breach has a high threat level (for example, an armed attack or a terrorist attack), the security team and local law enforcement are contacted.

The breach is immediately reported to the facility managers and local security forces (police, gendarmerie).

Depending on the magnitude of the breach, coordination of internal security teams and law enforcement is ensured.

The threatened areas are evacuated or security measures are temporarily increased (for example, closing the area, road blockades).

4. İhlalin Belgelendirilmesi
İhlalin tespit edildiği zaman, yeri, türü, güvenlik sistemlerinin verdiği uyarılar, devriye raporları ve güvenlik personelinin müdahale süreci idari işler çalışanı tarafından raporlanır ve kaydedilir.
CCTV kameralarından alınan görüntüler, sensörlerden alınan veriler ve diğer dijital kayıtlar saklanır. Bu veriler, ihlalin doğruluğunu kanıtlamak için kullanılabilir.
Güvenlik ekibi, ihlal durumu hakkında bir tutanak hazırlar. Bu tutanak, tesisin güvenlik yönetimi ve ilgili yetkili birimlere iletilir.

5. Güvenlik Önlemlerinin Artırılması
Tesis genelinde yaşanan herhangi bir ihlal sonrasında, tespit ve müdahale raporlamaları incelenerek ihlalin tekrarlanmaması için alınması gereken önlemler belirlenir. Alınacak yeni önlemler veya geliştirilmesi gereken hususlar üzerine çalışmalar ivedilikle başlatılır.
CCTV cihazlarının güncellenmesi sağlanır. Örneğin, kamera açıları değiştirilir.
Güvenlik personelinin eğitimi, yeni durumlarla başa çıkabilmeleri için güncellenir.

11.4 Erişim Denetimi

A. Bir çalışan çalışma alanına ve sınırlı alana erişim sağlayabilir. Ayrıca, bir ziyaretçinin gerekli olduğunda Şirket'le ilgili iş için ziyaret talebini, ziyaretçiyi yönetebilecek / denetleyebilecek bir departmandan talep eder.

B. Ziyaretçi beher giriş kapısı ya da danışma masasına kimliğini bırakıp geçiş hakkı alarak erişim sağlar.

C. İş ilişkisi olan bir kişi ya da iş yerine uzun süreli giriş sağlayacak olan bir kişi sadece uzun süreli geçiş izni aldıktan sora erişim sağlar. Geçiş İzni Yönetimi

11.4.1.Çalışan Geçiş İzni
Sadece Şirket'in bir çalışanı için verilen geçiş iznidir.

- Çalışan Kimlik No: Bütün çalışanlar için olması zorunlu olan bir kimlik numarasıdır ve giriş için kullanılır.

Kimlik Doğrulama
Personelin tesisin kapılarından giriş yapabilmesi için kimlik doğrulaması yapılır. Bu işlem, fiziksel kimlik belgeleri veya dijital sistemler aracılığıyla yapılabilir.

4. Documentation of the Breach
When a violation is detected, the time, place, type, warnings given by security systems, patrol reports and the intervention process of the security personnel are reported and recorded by the administrative affairs. employee.Images from CCTV cameras, data from sensors and other digital records are stored. This data can be used to prove the accuracy of the breach.
The security team prepares a report about the breach. This report is sent to the facility's security management and relevant authorized units.

5. Increased Security Measures
After any violations throughout the facility, detection and intervention reports are reviewed and precautions to be taken to prevent the violation from recurring are determined. Studies on new precautions to be taken or issues to be developed are initiated immediately.
CCTV devices are updated. For example, camera angles are changed.

The training of security personnel is updated so that they can cope with new situations.

11.4 Access Control
A. An employee can access the work area and restricted area. In addition, when a visitor is required for Company-related business, he/she requests a visit from a department that can manage/supervise the visitor.

B. The visitor gains access by leaving his/her ID at each entrance door or information desk and obtaining a pass
.
C. A person with a business relationship or a person who will enter the workplace for a long time can only access after obtaining a long-term pass. Passage Permit Management

11.4.1. Employee Passage Permit: It is a pass granted only to an employee of the Company

- Employee ID Number: It is an ID number that is mandatory for all employees and is used for entry.

Identity Verification
Identity verification is performed for personnel to enter the facility gates. This process can be done through physical identity documents or digital systems.

Kartlı Geçiş Sistemi: Personel, kendilerine tahsis edilen giriş kartını kullanarak geçiş yapar. Sistem, her geçişi kaydeder ve yetkili olmayan kişilerin girişini engeller.
Biyometrik Kimlik Doğrulama: Parmak izi gibi biyometrik doğrulama yöntemleriyle giriş yapılır. Bu yöntemler, personelin yetkisini doğrular.(CCR)
Fiziksel Kimlik Kontrolü: Özellikle, dijital sistemlerin çalışmadığı veya olağan dışı durumların yaşandığı zamanlarda güvenlik görevlisi, personelin kimliğini fiziksel olarak kontrol eder.
Geçici Erişim Kartı: Geçici İzin Kartı olmayan veya kimlik kartı olmayan personele temin edilen karttır. Bu geçici kartlar personelin yalnızca belirli bir süre için tesisin belirli alanlarına girişine izin verir. Güvenlik görevlisi, kaybolan kartın yerine geçecek geçici bir kart hazırlar, personelin kimliğini verilen bilgiler ile sistemden kontrol eder, sistemde bulunan bilgi ve fotoğraflarla karşılaştırma yaparak personelin girişine izin verir. Geçici kart, yalnızca belirli bir süre için geçerlidir.
Güvenlik görevlisi geçici kart ve personel için manuel bir liste tutar.

11.4.2. Ziyaretçi Geçiş İzni:
Bir çalışanın erişim yetkisi talep ettiği bir ziyaretçi için verilen geçiş iznidir.

- Günlük Ziyaretçi Geçiş İzni: Bir çalışanın erişim yetkisi talep ettiği, günübirlik olarak gelen bir ziyaretçi için verilen geçiş iznidir.
- Uzun Dönem Ziyaretçi Geçiş İzni: İş sözleşmesi, alt taşeron vb. için uzun süreli olan bir ziyaretçiye şirket adını, ismi, resmi ve giriş süresi üzerinde basılı olan bir geçiş izni verilir.

Mobis çalışanı gelecek olan ziyaretçi için sistem üzerinden (SPS) ziyaret talebinde bulunur. Talepte ziyaretin amacı, tarihi, saati ve geldiği firma belirtilir. Ziyaretçi ulaştığında sistem üzerinden talep kontrolü yapılır ve ilgili çalışana teyidi amacıyla ulaşılır.

Ziyaretçi ve çanta vb. eşyaları metal dedektöründen geçerek tesise girişi yapılır.Metal dedektörü gibi cihazlarla tarama yapıldıktan sonra, hala şüpheli bir durum varsa, güvenlik görevlisi tarafından el ile arama yapılabilir. Ancak, el araması yalnızca güvenlik görevlisinin izni ile ve uygun şartlarda gerçekleştirilir. Bu tür aramalar, ziyaretçinin onayı ve saygılı bir şekilde yapılmalıdır.

Card Pass System: Personnel pass using the entry card assigned to them. The system records each passage and prevents unauthorized persons from entering.
Biometric Identity Verification: Entry is made with biometric verification methods such as fingerprints. These methods verify the authority of the personnel. (CCR)
Physical Identity Control: Especially when digital systems do not work or unusual situations occur, the security guard physically checks the identity of the personnel.
Temporary Access Permit Card or personnel without an ID card can obtain a temporary access card. These temporary cards only allow the personnel to enter certain areas of the facility for a certain period of time.
Temporary Access Card: The security guard prepares a temporary card to replace the lost card and allows the personnel to enter. The temporary card is only valid for a certain period of time.
The security guard keeps a manual list for temporary cards and personnel.

11.4.2.Visitor Pass:
It is a pass granted for a visitor to whom an employee requests access authority

- Daily Visitor Pass: It is a pass granted for a visitor to whom an employee requests access authority.
- Long-term Visitor Pass: A pass with the company name, name, picture and entry period printed on it is granted to a visitor with a long-term employment contract, subcontractor, etc.

The Mobis employee requests a visit through the system (SPS) for the upcoming visitor. The purpose, date, time and the company the visitor came from are specified in the request.

After the visitor has passed through devices such as metal detectors, if there is still a suspicious situation, a security guard may perform a manual search. However, a manual search is only performed with the permission of the security guard and under appropriate conditions. Such searches must be performed with the visitor's approval and in a respectful manner.

Ziyaretçi, güvenlik birimince karşılanır. Resmi kimlik (nüfus cüzdanı, ehliyet, pasaport vb.) ibraz edilir. Ziyaretçiye "ziyaretçi kartı" ve bununla birlikte bir broşür verilir. Bu broşürde ziyaretçinin uyması gereken güvenlik kuralları belirlenmiştir. Ziyaret süresince bu kart görünür şekilde takılır. Güvenlik birimi sistem üzerinden ziyaretçinin girişini yapar (check in). Güvenlik birimi ilgili kişiye ya da departmana telefon ile haber verir ve teyidini alır. Ziyaretçilerin yalnızca belirlenen alanlarda bulunmasına izin verilir. Ziyaretçi güvenlik kontrolleri sonrasında yalnızca ilgili olduğu alana yönlendirilir, ziyaret edeceği çalışan tarafından karşılanana kadar güvenlik görevlisi ile gözle takip edilir. Ziyaret sona erdiğinde güvenlik birimi çıkış işlemini (check out) yapar. Ziyaretçinin giriş çıkış ve tesiste kaldığı süre sistem üzerinden(SPS) kaydedilmiş olur. Ziyaretçi kartı iade edilir.

11.4.3. Araç Geçiş İzni:

İş yerine giriş yapan bir araç için verilen geçiş iznidir.

Taşıtın tesis girişinde kaydı yapılır. Girişte, taşıtın kimlik, sürücü ve irsaliye ile ilgili bilgiler toplanır.

Taşıt Bilgilerinin Kaydı: Taşıtın plaka numarası, marka/modeli, tipi (kamyon, tır, minibüs vb.), taşıma türü (yük, personel, malzeme vb.) gibi bilgiler kaydedilir.

Sürücü Kimliği: Sürücünün geçerli kimlik belgesi (kimlik kartı, ehliyet vb.) kontrol edilir ve kaydedilir.

Yük Tarama: Taşıtın yük kısmı detaylı bir şekilde kontrol edilir. Özellikle tehlikeli, yasaklı veya şüpheli materyallerin taşınmadığına emin olunur.

Yol Haritası veya Yönlendirme: Taşıtın belirli bir alana yönlendirilmesi gerekiyorsa, güvenlik görevlisi veya ilgili personel tarafından taşıta bir yol haritası veya yönlendirme bilgisi sağlanır.

Çalışan Aracı Geçiş İzni: Çalışan aracı fabrikanın dışında bulunan otoparka yönlendirilir. Fabrika içerisine izin verilmez.

Ziyaretçi Aracı Geçiş İzni: Ziyaretçi aracı fabrikanın dışında bulunan otoparka yönlendirilir. Park yeri ile ilgili düzenlemeler girişte ziyaretçilere güvenlik birimi tarafından aktarılır. Fabrika içerisine izin verilmez.

Geçici Araç Geçiş İzni: Önceden erişim izni alan bir ziyaretçi aracına verilen geçiş iznidir. Bu günlük bir araç geçiş izni ve uzun dönem araç geçiş izni olarak sınıflandırılır.

The visitor is welcomed by the security unit. Official identification (identity card, driver's license, passport etc.) is presented. The visitor is given a "visitor's card" and a brochure with it. The security rules that the visitor must follow are specified in this brochure. This card is worn visibly during the visit. The security unit checks in the visitor through the system. The security unit notifies the relevant person or department by phone and receives confirmation. Visitors are only allowed to be in designated areas. When the visit is over, the security unit checks out. The visitor's entry and exit and the duration of his/her stay in the facility are recorded through the system (SPS). The visitor card is returned.

11.4.3. Vehicle Passage Permit:

It is a passage permit given for a vehicle entering the workplace.

The vehicle is registered at the entrance of the facility. At the entrance, information about the vehicle's identity, driver and delivery note is collected.

Vehicle Information Recording: Information such as the vehicle's license plate number, brand/model, type (truck, TIR, minibus, etc.), type of transportation (load, personnel, material, etc.) are recorded.

Driver Identity: The driver's valid identity document (ID card, driver's license, etc.) is checked and recorded.

Load Scanning: The load section of the vehicle is checked in detail. It is especially ensured that no dangerous, prohibited or suspicious materials are carried.

Road Map or Direction: If the vehicle needs to be directed to a specific area, a road map or direction information is provided to the vehicle by the security guard or relevant personnel.

- Employee Vehicle Passage Permit: The employee vehicle is directed to the parking lot outside the factory. No permission inside the factory

-Visitor Vehicle Permit: Visitor vehicle is directed to the parking lot outside the factory. No permission inside the factory. The arrangements regarding the parking lot are conveyed to the visitors by the security unit at the entrance.

-Temporary Vehicle Permit: This is a pass granted to a visitor vehicle that has received prior access permission. This is classified as a daily vehicle pass and a long-term vehicle pass.

11.4.4 Fabrika Park Yeri

Fabrika park yeri ile ilgili kurallar, fabrika içindeki ve dışındaki araç parkının düzenli ve güvenli bir şekilde yapılmasını sağlamak amacıyla güvenlik personeli tarafından kullanıcılara açıklanır. Bu kurallar, personel, ziyaretçiler, servis araçları ve diğer taşıtlar için belirli park alanlarının ayrılması, düzenin korunması ve güvenliğin sağlanması için gereklidir.

Personel Park Yeri : Personel için park alanları ayrılır ve bu alanlar çalışanların ve ziyaretçilerin kullanımına sunulur. Personel ve ziyaretçi park alanları, güvenlik amacıyla fabrikanın dışına ve ana kapısına yakın yerlerde konumlandırılır.

Ziyaretçi Park Yeri: Ziyaretçiler için park alanları ayrılır ve bu alanlar çalışanların ve ziyaretçilerin kullanımına sunulur. Fabrika girişine yakın bir yerde olur ve belirli süreler için park etmelerine izin verilir.

Servis Araçları Park Yeri: Fabrikada personel taşımacılığında kullanılan servis araçları için özel park alanları ayrılır. Bu araçlar sadece belirlenen alanlarda park edebilir.

Yükleme/Boşaltma Park Alanları: Yükleme ve boşaltma yapan araçlar için de ayrı bir park alanı ayrılır. Bu alanlarda araçlar, malzeme transferi bitene kadar park edebilir. İthal ve ihracat eşyalarını taşımakta olan çzel taşıtların yükleme /boşaltma ve depolama alanlarının yakınlarına park etmenin yasak olduğuna dair işaret levhaları bulunmaktadır.

Park Alanı Denetimleri: Güvenlik personeli, park alanlarında düzeni sağlamak amacıyla CCTV ve fiziksel olarak düzenli olarak kontroller yapar. Hatalı park etme, park süresi aşımı gibi durumlar tespit edildiğinde gerekli uyarılır ilgili kişiye, ilgili firmaya, ya da ilgili departmana yapılır.

12. Mal Kabulü / Çıkışı Denetimi

12.1 Denetimi yapılacak maddeler

Denetimi yapılacak maddeler genel varlıklar ve bilgi varlıkları olarak sınıflandırılır.

1.Denetimi Yapılacak Genel Varlık Maddeleri

- Üretim ve operasyon için gerekli olan malzeme ve parça, bitmiş ürün veya buna eşdeğer varlıklar
- Güvenlik operasyonu departmanı (ekibi) tarafından seçilen diğer genel varlıklar

11.4.4 Factory Parking

The rules regarding the factory parking lot are explained to users by the security personnel in order to ensure that the vehicle parking inside and outside the factory is organized in an orderly and safe manner. These rules are necessary to ensure that certain parking areas are reserved for personnel, visitors, service vehicles and other vehicles, to maintain order and ensure security.

Personnel Parking: Parking areas are reserved for personnel and are offered to the use of employees and visitors. Personnel and visitor parking areas are located outside the factory and close to the main gate for security purposes.

Visitor Parking Area: Parking areas are allocated for visitors and are offered to employees and visitors. It is located close to the factory entrance and they are allowed to park for certain periods of time.

Service Vehicles Parking Area: Special parking areas are allocated for service vehicles used for personnel transportation in the factory. These vehicles can only park in designated areas.

Loading/Unloading Parking Areas: A separate parking area is also allocated for loading and unloading vehicles. Vehicles can park in these areas until the material transfer is completed. Signs indicating that parking is prohibited near loading/unloading and storage areas of private vehicles are placed.

Parking Area Inspections: Security personnel regularly perform CCTV and physical checks in order to maintain order in parking areas. When situations such as incorrect parking or exceeding parking time are detected, the necessary warnings are made to the relevant person, relevant company or relevant department.

12. Goods Receiving/Exit Inspection

12.1 Items to be inspected

Items to be inspected are classified as general assets and information assets.

1. General Asset Items to be Audited

- Materials and parts required for production and operation, finished products or equivalent assets
- Other general assets selected by the security operations department (team)

2.Denetimi Yapılacak Bilgi Varlığı Maddeleri

- Bilgisayar (cep telefonu dahil), sunucu, saklama aracı vb. veri işleme ve saklama cihazı veya eşdeğer varlıklar
- Güvenlik operasyonu departmanı (ekibi) tarafından seçilen diğer bilgi varlıkları

3.Diğer detaylı maddelerle ilgili olarak güvenlik operasyonu departmanı (ekibi) denetimi zor olan detaylı yönergeler belirlese bile, güvenlik operasyonu departmanı (ekibi) bunları minimize edecek şekilde sınıflandıracaktır.

12.2 Kabul/Çıkış İşlemlerinin Denetim ve Yönetimi

A. Şirket'in sahip olduğu ve olmadığı tüm kontrollü varlıkların kabulü/çıkışını yönetebilecek bir departmanın (ekibin) onaylanması için prosedürler yapılır.

B. Yetkisi olmayan bir ziyaretçinin işle ilişkisi olmayan amaçlarla bile mal kabulü veya çıkışı yapması halinde, bu durumu onaylayan çalışan sorumlu tutulur.

C. Bir departman (ekip) varlıkların Kabul ve çıkış işlemlerinin onamasını yönetiyorsa ya da denetliyorsa bile, bir güvenlik operasyonu departmanı (ekibi) güvenlik amaçlarının yerine getirilmesini engelleyen varlıkların kabul/çıkışını denetleyebilir.

D. Kargo Kategorileri

Ticari Kargolar: Fabrika adına gelen ticari kargolar, genellikle işyeri malzemeleri, makineler veya hammaddelerdir. Fabrikaya gelen kargo ilgili departmana haber verilir. Araç malzeme teslim edilecek alana yönlendirilir.

Kişisel Paketler : Kişisel paketler, çalışanlar tarafından teslim alınan kargolardır ve genellikle kişisel kullanım içindir. Bu tür kargoların teslimi, işyeri eşyalarının karışmaması adına dikkatli yapılır.

Kişisel kargolar ilgili kişiye bilgi verilir. Kişinin bilgisi dahilinde güvenlik kapısında teslim alınır. Kişisel kargoların fabrika içerisine girişine izin verilmez.

2. Information Asset Items to be Audited

- Computer (including mobile phone), server, storage device, etc. data processing and storage device or equivalent assets
- Other information assets selected by the security operations department (team)

3.Even if the security operations department (team) determines detailed instructions that are difficult to audit regarding other detailed items, the security operations department (team) will classify them in a way that minimizes them.

12.2 Supervision and Management of Acceptance/Exit Procedures

A. Procedures are made for the approval of a department (team) that can manage the acceptance/exit of all controlled assets owned and not owned by the Company.

B. If an unauthorized visitor accepts or exits goods even for purposes unrelated to work, the employee who approves this situation is held responsible.

C. Even if a department (team) manages or supervises the approval of the acceptance and exit of assets, a security operations department (team) can supervise the acceptance/exit of assets that prevent the fulfillment of security objectives.

D. Cargo Categories

Commercial Cargo: Commercial cargoes arriving on behalf of the factory are usually workplace materials, machinery or raw materials. The relevant department is notified of the cargo arriving at the factory. The vehicle is directed to the area where the material will be delivered.

Personal Packages: Personal packages are cargoes received by employees and are generally for personal use. Delivery of such cargo is done carefully in order not to mix workplace belongings.

Personal cargo is informed to the relevant person. It is received at the security gate with the person's knowledge. Personal cargo is not allowed to enter the factory.

13. Kapalı Devre Televizyon (CCTV) Operasyonu ve Tesis İzleme

13.1 Temel İlkeler

A. Araçların ve kişilerin girişlerinin olduğu, yangın, hırsızlık ihtimali olan alanlar ve sınırlar her zaman güvenlik personeli tarafından kapalı devre kamera sistemi aracılığıyla izlenir ve 90 gün süre ile kaydedilir.

B. Kritik (güvenlik) tesisler CCTV ile ve güvenlik personeli tarafından izlenir. Eğer söz konusu izleme iş yerinin özelliklerine göre uygulanabilir değilse, isimsiz bir güvenlik sistemi de kullanılabilir.

C. CCTV sistemi sadece güvenlik, yangın, hırsızlık, sınır kontrolü vb. kesin ve gerçek kaygıların olduğu alanlara kurulur ve kurulum amaçlarına göre işletilir.

D. CCTV'nin kurulduğunu ve çalıştığını gösteren bir bildiri ana giriş vb. düz bir yere asılır (yapıştırılır).

13.2 Yönetim Sorumluluğu

A. Fiziki güvenlik sorumlusu güvenlik personelinin yönetimi ve çalışmasından sorumludur. Bu görevlerin emanet edilmesi halinde, bir emanet sözleşmesi gizliliğin ilgili Kanun ve bağımlı yasalara uygun bir şekilde korunmasıyla ilgili konuları inceler.
B. Kurumsal Güvenlik Müdürü fiziki güvenlik personelini seyreder ve gözetler ve böylece söz konusu personel iş yeri erişimi vb. için toplanan kişisel bilgileri ve CCTV kanalıyla toplanan görüntüleri kendi çıkarları için kullanmaz ya da sızdırmaz.

13.3 Bilgi İşleme

A. Saklama süresi dolan herhangi bir kişisel bilgi (görüntü bilgisi dahil) gecikmeksizin onarılamaz bir şekilde silinir.
B. Görüntü bilgilerini tutan (izleyen) yer sınırlı alan, vb olarak belirlenir ve buraya ilgili bir kişinin dışında başka birinin girişi denetlenir.
C. Görüntü bilgileri CCTV kurulumu dışında amaçlarla kullanılamaz ya da yetkisi olmayan bir kişiye verilmez (gösterilmez). Ancak, bu verilerin kanunlar ve yönetmelikler tarafından sağlandığı ya da okunduğu veya bir bilgi yöneticisinden talep edilmiş olması şartıyla, CSO'dan ön onay alınacaktır.

13. Closed Circuit Television (CCTV) Operation and Facility Monitoring

13.1 Basic Principles

A. Areas and borders where vehicles and people enter, where there is a risk of fire or theft are always monitored by security personnel and recorded for 90 days.

B. Critical (security) facilities are monitored by CCTV and security personnel. If such monitoring is not applicable according to the characteristics of the workplace, an anonymous security system can also be used.

C.CCTV system shall be installed only in areas where there are definite and real concerns such as security, fire, theft, border control, etc. and shall be operated in accordance with the installation purposes.

D.A notice indicating that the CCTV has been installed and is operating shall be hung (pasted) on a flat place such as the main entrance, etc.

13.2 Management Responsibility

A.The physical security officer shall be responsible for the management and operation of the security personnel. If these duties are entrusted, an entrustment agreement shall examine the issues related to the protection of confidentiality in accordance with the relevant Law and dependent laws.
B.The Corporate Security Manager shall monitor and supervise the physical security personnel so that the personnel in question shall not use or leak the personal information collected for workplace access, etc. and the images collected through the CCTV channel for their own benefit.

13.3 Information Processing
A.Any personal information (including image information) whose storage period has expired shall be irreparably deleted without delay.
B. The place that holds (monitors) the image information is determined as a restricted area, etc. and the access of anyone other than the relevant person is controlled.
C. The image information cannot be used for purposes other than the CCTV installation or given (not shown) to an unauthorized person. However, prior approval will be obtained from the CSO, provided that this data is provided or read by laws and regulations or requested from an information manager.

14. İş Sürekliliği Yönetimi

14.1 İş Sürekliliği Yönetimi için Güvenliğin Prosedürlere Yansıtılması

A. Doğal afetler, yangın, ayaklanma vb. acil durumlar için bir iş sürekliliği planı geliştirmek ve sağlamak adına bir organizasyon ve yönetim süreci tanımlanır.
B. Acil durumlar olması halinde bilgi sisteminin sürekli olarak çalışması ve iş durması olması halinde işin en kısa sürede devamının sağlanması için iş önceliklerine uygun bir şekilde bir acil durum planı yapılır ve uygulanır.

C. İş sürekliliği planını değiştirme prosedürleri oluşturulur ve ilgili çalışanlar değişen iş süreklilik olanı konusunda bilgilendirilirler.
D. İş sürekliliği planının etkinliği test edilir ve düzenli olarak onanır.

14.2 Diğer Detaylı Konular

Burada belirtilmeyen konularla ilgili "Tesis Koruması ve Erişim Kontrolü Yönergeleri", "CCTV Tesis Görüntüleme Yönergeleri" ve "Bilgi Varlıklarının Kontrolünü Yerine Getirme Yönergeleri" incelenir.

Teknik Güvenlik

15. Kullanıcı Güvenliği Yönergeleri

15.1 Amaç

Kullanıcı Güvenliği Yönergelerinin amacı Şirketin iş için sağladığı bir terminalin bilgi güvenliği koruması için gereklilikleri belirlemektir.

15.2 Yönetim Maddesi

A. İş için bir terminalin tanıtımı, operasyonu ve imha edilmesi için yönergeler hazırlanır.

B. İş terminali için harf ve rakam kombinasyonlu, 8 veya daha fazla haneli ve ekran koruyuculu bir giriş şifresi ve tanımlanır.

C. Şirketin dağıttığı bir iş programı tüm kişisel bilgisayarlara kurulur. Yasadışı bir yazılım yükleyen kişi söz konusu yazılımın sorumluluğunu alır.

D. Zararlı kodların yapılmasını engelleyen bir çözüm gibi bir güvenlik sistemi tüm kişisel bilgisayarlara kurulur ve kişisel bilgisayarın kullanıcısı son güncellenmiş halini ve güvenlik yamasını muhafaza eder.

14 Business Continuity Management

14.1 Reflecting Security in Procedures for Business Continuity Management
A. An organization and management process is defined to develop and provide a business continuity plan for emergencies such as natural disasters, fire, riots, etc.
B. An emergency plan is made and implemented in accordance with business priorities to ensure that the information system operates continuously in case of emergencies and that the work continues as soon as possible in case of a work stoppage.
.Procedures for changing the business continuity plan are established and relevant employees are informed about the changed business continuity plan.
D.The effectiveness of the business continuity plan is tested and regularly approved.

14.2 Other Detailed Topics

The "Facility Protection and Access Control Guidelines", "CCTV Facility Imaging Guidelines" and "Guidelines for Performing Control of Information Assets" are reviewed for topics not specified here.

Technical Security

15. User Security Guidelines

15.1 Purpose

The purpose of the User Security Guidelines is to determine the requirements for information security protection of a terminal provided by the Company for business.

15.2 Management Article

A. Guidelines are prepared for the introduction, operation and disposal of a terminal for business.

B. A login password with a combination of letters and numbers, 8 or more digits and a screen saver for the business terminal is defined.

C. A business program distributed by the company is installed on all personal computers. The person who installs illegal software takes responsibility for the software in question.

D. A security system, such as a solution that prevents malicious code from being created, is installed on all personal computers, and the user of the personal computer keeps the latest update and security patch.

E. Kişisel bilgisayardaki bir dosyanın paylaşılması gerektiğinde, şifrelenmiş bir paylaşımlı klasör seçilir ve bu klasöre sadece yetkisi olan bir kullanıcının erişim hakkı olur.

F. Ortak bir kişisel bilgisayar yöneticisi belirlenir ve bir güvenlik dosyası ortak bir kişisel bilgisayara kaydedilmez.

G. Şirket'in internet güvenliği politikası incelenir ve onaylanmamış bir internet ağı kullanılmaz.

I. Güvenlik dosyası genel bir ağ (internet vb.) üzerinden iletilmez. Kaçınılmaz koşulların olması durumunda önden ya da sonradan bir yönetici onayı alınır.

İ. Bir kullanıcı Şirket'in sağladığı donanım ve yazılımı izin almadan değiştiremez. Bir kullanıcı gereken onayı alması sonrasında taşınabilir bir saklama cihazı kullanabilir.

J. İş için bir taşınabilir cihazın kullanılması durumunda, ilgili güvenlik yönergeleri uygulanır.

K. Anahtar, şifre, kumanda veya kart gibi erişim araçlarından sorumlu kişiler, her departman için unvan bazında belirlenir ve sorumlulukları ilgili departman hiyerarşisine tabidir. Anahtar ve kumanda kullanımına ilişkin sorumluluklar MTR-GA-I001 numaralı talimatla belirlenmiştir. Bariyer anahtarları yalnızca Güvenlik Görevlileri tarafından kullanılabilmektedir. Sayılan erişim araçlarının teslimi gerektiği hallerde yetkilendirilmiş Güvenlik Personeli tarafından imza karşılığında teslim gerçekleştirilir. Erişim araçlarının sayımı periyodik olarak yetkili güvenlik personeli tarafından yapılır.

15.3 Diğer Detaylı Konular

Diğer detaylı konularla ilgili olarak "Kullanıcı Güvenliği Yönergeleri" incelenir.

16. Ağ Güvenliği

16.1 Amaç

Ağ güvenliğinin amacı dışarıdaki ağlara bağlanmak için gerekli olan, iç ağın kurulumunu ve bilgi teknolojisi koruması standartlarını geliştirerek güvenli istikrarlı bir ağ altyapısı elde etmektir.

E. When a file on a personal computer needs to be shared, an encrypted shared folder is selected and only an authorized user has access to this folder.

F. A common personal computer administrator is determined and a security file is not saved on a common personal computer.

G. The company's internet security policy is reviewed and an unapproved internet network is not used.

I. The security file is not transmitted over a public network (internet, etc.). In case of unavoidable conditions, prior or subsequent approval from an administrator is obtained.

İ. A user cannot change the hardware and software provided by the Company without permission. A user may use a portable storage device after receiving the necessary approval.

J. In case a portable device is used for work, the relevant security guidelines are applied.

K. Persons responsible for access tools such as keys, passwords, remotes or cards are determined on a title basis for each department and their responsibilities are subject to the relevant department hierarchy.

15.3 Other Detailed Topics

The "User Security Guidelines" are reviewed regarding other detailed topics.

16. Network Security

16.1 Purpose

The purpose of network security is to obtain a secure and stable network infrastructure by developing the internal network setup and information technology protection standards required to connect to external networks.

16.2 Yönetim Maddesi

A. İç ağ dışarıdan erişimin kontrollü olacağı şekilde ayrı bir ağ olarak kurulur.

B. Bir kullanıcının iç ağa gene bir ağ üzerinden bağlanmaya çalışması durumunda, iç ağı, kodlama ve kimlik kanıtlama süreci üzerinden, sadece iş için kullanır. Erişim kayıtları dosya üzerinde tutulur.

C. Yüksek derece önemli olan system ve ağ ayrılır.

D. Şirket'in ağlarını yetkisiz olan bir elektronik cihaz kullanamaz.

E. Bir ziyaretçi ya da çalışan sadece Bilgi Teknolojileri Güvenliği Müdüründen onay alması sonrasında ağı kendi kişisel bilgisayarında kullanılabilir.

F. Yeni bir ağın kurulumu ve ayarlarındaki değişiklik, testler gibi bir doğrulama süreci sonrasında, onaylama sürecine uygun bir şekilde yapılır.

G. Yetkisiz bir kablosuz iletişim aracı kullanılamaz.

H. Yetkili bir kablosuz iletişim aracı için, iletişimi koruma noktasında uygun bir aksiyon alınır.

I. Ağ ekipmanlarının kurulumuna ait içerikler ağın çalışmaması durumuna karşılık yedeklenir.

İ. Ağ ekipmanlarına erişim denetlenir.

J. Bir ağın tanıtımı, operasyonu ve imhası için yönergeler hazırlanır.

16.3 Diğer Detaylı Konular

Diğer detaylı konularla ilgili olarak "Ağ Güvenliği Yönergeleri" incelenir.

16.2 Management Article

A. The internal network is established as a separate network in a way that external access is controlled.

B. If a user tries to connect to the internal network via another network, the internal network is used only for work, through the coding and authentication process. Access records are kept on file.

C. The highly important system and network are separated.

D. An unauthorized electronic device cannot use the Company's networks.

E. A visitor or employee can only use the network on their own personal computer after receiving approval from the Information Technology Security Manager.

F. The installation of a new network and changes in its settings are made in accordance with the approval process after a verification process such as tests.

G. An unauthorized wireless communication device cannot be used.

H. For an authorized wireless communication device, an appropriate action is taken to protect communication.

I. The contents of the network equipment installation are backed up in case the network does not work.

İ. Access to network equipment is controlled.

J. Guidelines are prepared for the introduction, operation and destruction of a network.

16.3 Other Detailed Topics

"Network Security Guidelines" are examined regarding other detailed topics.

17. Sistem Güvenliği

17.1 Amaç

Sistem güvenliğinin amacı sistemi çeşitli tehditler ve saldırılara karşı korumak ve sistemi çalıştırmak ve yönetmektir.

17.2 Yönetim Maddesi

A. Sistemin tanıtımı, operasyonu ve imhasıyla ilgili olarak yönergeler hazırlanır.

B. Bir sistemin tanıtımı ve değişikliği uygun prosedürlere göre belirlenir ve güvenlik denetimi maddeleri belirlenir.

C. Sistem kurulumu sırasında oluşturulan bir varsayılan hesap ve kullanılmayan bir hesap silinir ve değiştirilir. Tüm hesaplar yılda iki kere incelenir.

D. Bir sunucu sistemine erişim kayıtları üç yıl ya da daha fazla süre boyunca muhafaza edilir.

E. Bir system kullanıcısı hesabı resmi onaylama prosedürleri kanalıyla kayıt altına alınır, değiştirilir ve silinir, ve bununla ilgili geçmiş bilgiler yönetilir.

F. Bir kullanıcı eşsiz bir hesapla kaydedilir ve hesap paylaşımının mevcut durumu incelenir.

G. Şifre harf ve rakamlardan oluşan, en az 8 haneli olacak şekilde belirlenir ve üç ayda bir değiştirilir.

H. Önemli bir iş sisteminin gelişimi ve operasyonu ayrılır.

I. Resmi onaylama prosedürlerine göre bir uygulama geliştirilir ve değiştirilir ve buradaki operasyona güvenlik incelemesi ve performans doğrulama testi sonrasında yansıtılır.

İ. Test verileri vatandaşlık numarası, banka hesap numaraları vb. önemli bilgileri veya kişisel bilgileri içermez.

J. Veritabanına erişim denetlenir ve erişim kaydı üç yıl ya da daha fazla süre boyunca saklanır.

17. System Security

17.1 Purpose

The purpose of system security is to protect the system against various threats and attacks and to operate and manage the system.

17.2 Management Article

A. Guidelines are prepared for the introduction, operation and destruction of the system.

B. Introduction and modification of a system are determined according to appropriate procedures and security control items are determined.

C. A default account created during system installation and an unused account are deleted and replaced. All accounts are reviewed twice a year.

D. Access records to a server system are maintained for three years or more.

E. A system user account is registered, modified, and deleted through formal approval procedures, and the associated historical information is managed.

F. A user is registered with a unique account and the current status of the account sharing is reviewed.

G. The password is determined to be at least 8 digits long, consisting of letters and numbers, and is changed every three months.

H.The development and operation of a significant business system are separated.

I. An application is developed and modified according to formal approval procedures, and the operation here is reflected after the security review and performance verification test.

İ. The test data does not include important information such as citizenship number, bank account numbers, etc. or personal information.

J. Access to the database is controlled and the access record is kept for three years or more.

K. Sistem periyodik olarak saldırılara karşı denetlenir ve periyodik olarak önlemler alınır. Her yıl planlı olarak sızma testi yapılır. Önlem olarak dış kaynak firmasından DDOS saldırılarına karşı monitörleme hizmeti alınır

L. Bir işletim sistemi ve veritabanı yedeklenir ve uzaktan düzenlenir.

M. Bir sistem hatası sonrasında systemin düzeltilmesi planı hazırlanır ve en az yılda bir kere bir simülasyon çalışması yapılır.

17.3 Diğer Detaylı Konular

Diğer detaylı konularla ilgili olarak "Sistem Güvenliği Yönergeleri" incelenir.

18. Güvenlik Sistemi Operasyonu

18.1 Amaç

Güvenlik sistemi operasyonunun amacı bir güvenlik sisteminin güvenli ve etkili bir şekilde operasyonu ve yönetimi için yönergeleri oluşturmaktır.

18.2 Yönetim Maddesi

A. Bir güvenlik sisteminin tanıtımı, operasyonu ve imhası için yönergeler hazırlanır.

B. Her güvenlik sistemi için bir işletim kitapçığı hazırlanır.

C. Sadece yetkili bir kullanıcı güvenlik sistemine erişim sağlayabilir ve harf ve rakamlardan oluşan en az 8 haneli bir şifre oluşturulur.

D. Güvenlik sistemi yöneticisi her zaman çalışmak üzere bir kayıt sistemi kurar, sistemi periyodik olarak izler ve inceler ve ilgili bir kaydı üç yıl ya da daha fazla zaman boyunca tutar.

E. Güvenlik sistemi yöneticisi güvenlik sistemi saldırılarını periyodik olarak inceler ve bu saldırıların düzeltilmesini sağlar.

18.3 Diğer Detaylı Konular

Diğer detaylı konularla ilgili olarak "Güvenlik Sistemi Yönergeleri" incelenir.

K. The system is periodically inspected against attacks and precautions are taken periodically. A planned penetration test is conducted every year. As a precaution, monitoring service against DDOS attacks is received from an outsourcing company.

L. An operating system and database are backed up and remotely edited.

M. A system recovery plan is prepared after a system failure and a simulation study is conducted at least once a year.

17.3 Other Detailed Topics

The "System Security Guidelines" are reviewed regarding other detailed topics.

18. Security System Operation

18.1 Purpose

The purpose of security system operation is to establish guidelines for the safe and effective operation and management of a security system.

18.2 Management Article

A.Guidelines are prepared for the introduction, operation and disposal of a security system.

B.An operation manual is prepared for each security system.

C.Only an authorized user can access the security system and a password of at least 8 digits consisting of letters and numbers is created.

D. The security system administrator shall establish a recording system that is always operational, periodically monitors and examines the system, and maintains a relevant record for three years or more.

E. The security system administrator shall periodically examine security system attacks and ensure that such attacks are corrected.

18.3 Other Detailed Topics

Regarding other detailed topics, the "Security System Guidelines" shall be examined.

19. BT Güvenlik Olayı Yönetimi

19.1 Amaç

BT güvenlik olayı yönetiminin amacı BT ihlali olayına reaksiyon ve bu olaydan sonra onarım konularını ele alma ve bilgi varlıklarının güvenliği ve istikrarlılığını BT altyapısına gelecek zararları en aza indirgeyerek ve bu tür olayların tekrar etmesinin önüne geçerek sağlama konusunda yönergeler oluşturmaktır.

19.2 Yönetim Maddesi

A. Teknik güvenlik personeli bir BT güvenlik olayına derhal cevap verir ve bununla ilgili sonuçları Kurumsal Güvenlik Müdürü ya da CSO'ya rapor eder.

B. Bir kullanıcının bir izinsiz olay tespit etmesi halinde, bu durumu teknik güvenlik personeli ya da Kurumsal Güvenlik Müdürüne gecikmeden iletmesi gerekir.

C. Dışarıdan bir ihlal durumunun söz konusu olması halinde, teknik güvenlik personeli bir güvenlik tanı aracı ya da kontrol listesi aracılığıyla hizmeti kontrol eder. Sahtecilik ya da verilere izinsiz erişim olması hallerinde teknik güvenlikten sorumlu kişi hizmeti durdurur.

D. İhlal eden kişiyi tespit etmek için delil toplanır ve tüm kayıtlar muhafaza edilir.

E. İşbirliğinin gerekli olduğunun tespiti halinde, dışarıdan bir işletme ve bir kurum bu durumla ilgili bilgilendirilir ve yardım talep edilir.

F. İhlal olayı olması durumunda bilgi sistemi bu hatayla ilgili onarılır ve söz konusu onarımla ilgili olarak periyodik şekilde bir simülasyon çalışması gerçekleştirilir.

G. İhlal olayının yeniden meydana gelmesinin önüne geçilmesi adına esas bir çözüm ve karşı önlemler belirlenir.

H. Bildirilmesi gereken ihlal olayıyla ilgili çalışanlar da bilgilendirilir ya da eğitilir.

19.3 Diğer BT Güvenliği Olayları
Diğer detaylı konularla ilgili olarak "BT Güvenliği Olaylarına Cevap Verme Yönergeleri" incelenir.

19. IT Security Incident Management

19.1 Purpose

The purpose of IT security incident management is to establish guidelines for responding to an IT breach incident and addressing the issues of recovery after such an incident, and ensuring the security and stability of information assets by minimizing damage to the IT infrastructure and preventing such incidents from recurring.

19.2 Management Clause

A. Technical security personnel shall promptly respond to an IT security incident and report the results to the Corporate Security Manager or CSO.

B. If a user detects an unauthorized event, they must immediately report it to the technical security personnel or Corporate Security Manager.

C. In the event of an external breach, the technical security personnel checks the service using a security diagnostic tool or checklist. In the event of fraud or unauthorized access to data, the person responsible for technical security will stop the service.

D. Evidence is collected to identify the violator and all records are retained.

E. If it is determined that cooperation is necessary, an external business or institution is notified of the situation and assistance is requested.

F. In case of a violation, the information system is repaired for this error and a simulation study is performed periodically regarding the repair in question.

G. A basic solution and countermeasures are determined to prevent the recurrence of the violation.

H. Employees are also informed or trained regarding the violation that needs to be reported.

19.3 Other IT Security Incidents
The "IT Security Incident Response Guidelines" are reviewed regarding other detailed issues

20.Özel Güvenlik Hizmeti

1.Hizmet alımı

Firmanın fiziksel güvenliği dış kaynaktan yıllık olarak yapılan sözleşme ile özel güvenlik firması tarafından sağlanır. Özel güvenlik firması güvenliğin etkin bir şekilde yapılmasını ayrıca hukuki ve idari gerekliliklere uyulması sağlar. Ek:Güvenlik hizmet sözleşmesi

2. İhtiyaç Analizi ve Güvenlik Planı Hazırlığı

İhtiyaç Belirleme: Kurum, hangi alanlarda güvenlik hizmetine ihtiyaç duyduğunu belirler (örneğin; bina güvenliği, çevre güvenliği, iç mekan güvenliği, taşıma güvenliği, alarm sistemleri vb.).

Güvenlik Planı Oluşturma: Alınacak hizmetin kapsamı, güvenlik planı doğrultusunda belirlenir. Bu plan, görevli güvenlik personelinin sayısını, çalışma saatlerini, güvenlik sistemlerini, acil durum prosedürlerini içerir.

3. Hizmet Alımı İhale Süreci

İhale Hazırlığı: Güvenlik hizmeti alımı için gerekli belgeler hazırlanır (ihale dokümanı, sözleşme şartları, güvenlik hizmeti gereksinimleri vb.).

İhale İlanı: Güvenlik şirketlerine başvuru yapılır.

Teklif Toplama: Güvenlik hizmeti sağlayan firmalardan teklifler alınır. Bu teklifler, firma geçmişi, deneyimi, personel eğitimi, teklif edilen fiyat gibi kriterlere göre değerlendirilir.

4. Firma Seçimi ve Sözleşme

Firma Değerlendirmesi: Gelen teklifler değerlendirilir. Firma, güvenlik hizmetinin kalitesi, profesyonellik seviyesi, personel yeterliliği ve maliyet gibi faktörlere göre seçilir.

Sözleşme İmzalanması: Seçilen firma ile güvenlik hizmetleri sözleşmesi yapılır. Bu sözleşme; hizmetin süresi, çalışma şartları, ücretler, sorumluluklar, cezai şartlar ve diğer detayları içerir.

5. Personel Temini

Güvenlik Personelinin Sağlanması: Firma, gerekli güvenlik personelini temin eder. Personelin eğitim durumu, kimlik bilgileri ve sertifikaları kontrol edilir (Örneğin, özel güvenlik sertifikası ve mesleki yeterlilik belgeleri).

6. Eğitim

Güvenlik personeli, kurumun özel güvenlik ihtiyaçlarına uygun olarak eğitilir. Bu eğitimler, güvenlik prosedürleri, acil durum yönetimi, iletişim becerileri, temel ilk yardım ve şirketin iç kuralları gibi konuları kapsar.

20. Private Security Service

1. Service purchase

The physical security of the company is provided by a private security company with an annual contract from an external source. The private security company ensures that security is carried out effectively and that legal and administrative requirements are met. Annex: Security service contract

2. Needs Analysis and Security Plan Preparation

Determining Needs: The institution determines in which areas it needs security services (e.g. building security, environmental security, indoor security, transportation security, alarm systems, etc.).

Creating a Security Plan: The scope of the service to be received is determined in line with the security plan. This plan includes the number of security personnel on duty, working hours, security systems, and emergency procedures.

3. Service Procurement Tender Process

Tender Preparation: Necessary documents for security service procurement are prepared (tender document, contract terms, security service requirements, etc.).

Tender Announcement: Applications are made to security companies.

Bid Collection: Bids are received from companies providing security services. These bids are evaluated according to criteria such as company history, experience, personnel training, and the offered price.

4. Company Selection and Contract

Company Evaluation: Incoming offers are evaluated. The company is selected based on factors such as the quality of the security service, level of professionalism, personnel adequacy and cost.

Signing the Contract: A security services contract is made with the selected company. This contract includes the duration of the service, working conditions, wages, responsibilities, penal terms and other details.

5. Provision of Personnel

Provision of Security Personnel: The company provides the necessary security personnel. The education status, identity information and certificates of the personnel are checked (For example, private security certificate and professional qualification documents).

6. Training

Security personnel are trained in accordance with the specific security needs of the organization. This training covers topics such as security procedures, emergency management, communication skills, basic first aid and the company's internal rules.

7. Hizmetin Başlaması
Güvenlik hizmeti, belirlenen tarihte ve şartlarda başlatılır. Firma, güvenlik hizmetinin her aşamasını izler ve raporlar.

8. Sözleşme Süresi ve Yenileme
Sözleşme Süresi: Güvenlik hizmeti genellikle bir yıl süre için alınır.
Sözleşme Yenileme veya Sonlandırma: Sözleşme süresi sonunda, hizmetlerin devam etmesi veya sözleşmenin yenilenmesi konusunda karar verilir. Eğer hizmetten memnun kalınmazsa, sözleşme sonlandırılabilir.

9. Yasal Yükümlülükler
1. Güvenlik hizmetlerinin yasal çerçevede verilmesi gereklidir. Özel güvenlik hizmetleri, **Özel Güvenlik Hizmetlerine Dair Kanun** ve ilgili yönetmelikler doğrultusunda yürütülmektedir. Güvenlik personelinin **Özel Güvenlik Kimlik Kartı**na sahip olması zorunludur.
2. Kanunda belirtilen bildirimleri süresi içinde yapmak, denetimler sonucu tespit edilen eksiklerin giderilmesini sağlamak, personel sayısını belirlemek, gerekirse özel güvenlik hizmet şeklinin değiştirilmesi sağlamak üzere görevli personel bulunur. Ek: Kişi Kurum ve Kuruluş yetkilisi belgesi
3. Özel güvenlik görevlilerinin görev ve sorumluluklarını belirten valilik onaylı koruma ve güvenlik planı bulunur. Ek: Koruma ve güvenlik planı
4. Tesiste 5188 sayılı kanun ve uygulama yönetmeliğine göre düzenlenen ve valilik tarafından verilen özel güvenlik belgesi bulunur. Ek: Özel güvenlik belgesi
5. Tesiste özel güvenlik hizmet şekline göre, yerleşim planına göre, tesisin büyüklüğüne göre silahlı ve silahsız personel sayısı belirlenir. Valilik tarafından onaylı komisyon kararı bulunur. Ek: Komisyon kararı

7. Service Start
Security service is started on the specified date and conditions. The company monitors and reports every stage of the security service.

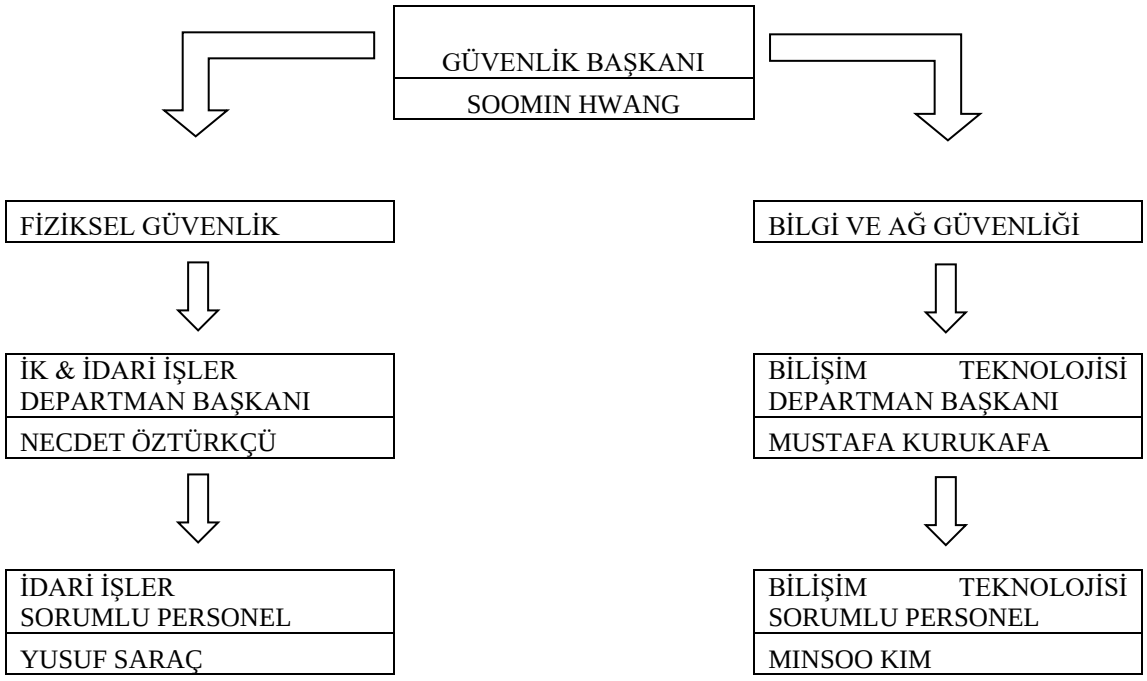
8. Contract Term and Renewal
Contract Term: Security service is usually taken for a period of one year.
Contract Renewal or Termination: At the end of the contract term, a decision is made on whether to continue the services or renew the contract. If the service is not satisfied, the contract can be terminated.

9.Legal Obligations
1.Security services must be provided within the legal framework. Private security services are carried out in accordance with the Law on Private Security Services and relevant regulations. Security personnel are required to have a Private Security Identity Card.
2.There is a staff assigned to make the notifications specified in the law within the time limit, to ensure that the deficiencies detected as a result of inspections are eliminated, to determine the number of personnel, and to ensure that the type of private security service is changed if necessary.Annex:Person, Institution and Organization Authorized Document
3.There is a protection and security plan approved by the governor's office that specifies the duties and responsibilities of private security officers. Annex:Protection and security plan
4.There is a private security document issued by the governor's office and issued in accordance with Law No. 5188 and its implementation regulation in the facility. Annex: Private security document
5. The number of armed and unarmed personnel is determined according to the type of private security service in the facility, according to the layout plan, and the size of the facility. There is a commission decision approved by the governor's office. Annex: Commission decision

Bölüm 5 Ek

21.Ek

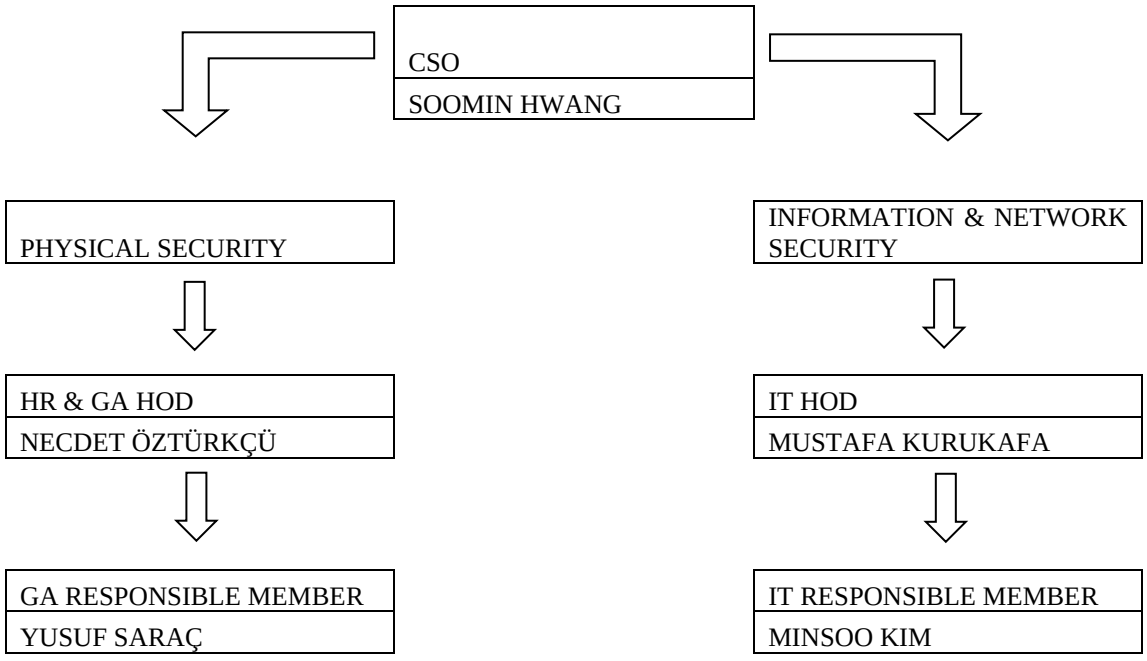
21.1 Güvenlik Organizasyon Şeması



Chapter 5 Attachment

21. Enclosure

21.1 Security Organization Chart



Her Departman için Sorumlu kişi

No	Bölüm	ID	İsim	Başlık
1	Bilgi Teknolojileri	7901677	Minsoo Kim	Personel
2	İdari İşler	7901003	Yusuf Saraç	Müdür
3	Parça Geliştirme	7901072	Celil Çeliker	Müdür
4	Üretim	7901638	Erman Cinoğlu	Müdür
5	Kalite	7901845	Minel Erdem	Müdür Yardımcısı
6	Finans	7901038	Ramazan Akcan	Müdür
7	Üretim Kontrol	7901300	Oğuzhan Aydın	Müdür
8	Satış	7901987	Vedat Küçükbaş	Personel

Responsible Person of Each Department

No	Department	ID	Name	Title
1	IT	7901677	Minsoo Kim	Staff
2	GA	7901003	Yusuf Saraç	Manager
3	PD	7901072	Celil Çeliker	Manager
4	Production	7901638	Erman Cinoğlu	Manager
5	Quality	7901845	Minel Erdem	Asistant Mgr
6	Finance	7901038	Ramazan Akcan	Manager
7	PC	7901300	Oğuzhan Aydın	Manager
8	Sales	7901987	Vedat Küçükbaş	Staff

22. İlgili Yönergeler ve Formlar	**21. Related Guidelines and Forms**
22.1Yönetsel	**21.1 Administrative**
22.1.1 Genel Standartta Güvenlik Formları	**21.1.1** Global Standard Safety Forms
22.1.2 Kişisel Bilgilerin Korunması için Yönergeler	**21.1.2** Guidelines for Personal Information Protection
22.1.3 Hareketli Güvenlik Yönetmeliği	**21.1.2** Mobile Security Regulations
22. 2 Fiziki	**21.2 Physical**
22.2.1 Tesis Koruma ve Erişim Kontrolü Yönergeleri	**21.2.1** Guidelines for Facility Protection and Access Control
22.2.2 CCTV Operasyonu ve Tesis İzleme Yönergeleri	**21.2.2** Guidelines for CCTV Operation and Facility Monitoring
22.2.3 Bilgi Varlıklarının Kabulü/Çıkışı için Yönergeler	**21.2.3** Guidelines for Information Assets Taking In/Out
22.3.Teknik	**21.3 Technical**
22.3.1 Kullanıcı Güvenliği Yönergeleri	**21.3.1** Guidelines for User Security
22.3.2 Ağ Güvenliği Yönergeleri	**21.3.2** Guidelines for Network Security
22.3.3 Sistem Güvenliği Yönergeleri	**21.3.3** Guidelines for System Security
22.3.4 Güvenlik Sistemi Operasyonu Yönergeleri	**21.3.4** Guidelines for Security System Operation
22.3.5 BT Güvenliği Olaylarına Cevap Verme Yönergeleri	**21.3.5** Guidelines to Respond to IT Security Incidents