BİLGİ GÜVENLİĞİ POLİTİKASI

INFORMATION SECURITY POLICY

FİGO TİCARİ BİLGİ VE UYGULAMA PLATFORMU A.Ş

1. AMAÇ VE KAPSAM

Bu politikanın amacı, Figo Ticari Bilgi ve Uygulama Platformu A.Ş.'nin ("Figopara" veya "Şirket") stratejik yönü ile uyumlu bilgi güvenliği prensiplerini belirleyerek tüm dijital ve fiziksel varlıklarını koruma altına almak ve temel bilgi güvenliği prensiplerini tanımlamaktır.

Bilgi güvenliği; Figopara bünyesinde yalnızca teknik bir konu olarak değil, kurumsal yönetişim, risk yönetimi, dijital operasyonel dayanıklılık, ISO/IEC 27701, ISO/IEC 27001, ISO 22301, KVKK, standartları ve sürdürülebilirlik yaklaşımının ayrılmaz bir parçası olarak ele alınır. Bu politika, bilgi güvenliği uygulamalarının Avrupa Birliği dijital dayanıklılık düzenlemeleri, OECD, ESG yönetişim ilkeleri, ISO standartları ve uluslararası iyi uygulamalarla uyumlu şekilde yürütülmesini esas alır.

Entegre Yönetim Sistemimizin (EYS) bir parçası olarak, Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) kurulması, işletilmesi, sürdürülmesi ve sürekli iyileştirilmesi yönetimin yönlendirmesi doğrultusunda yürütülür. Figopara'nın bilgi güvenliğine ilişkin yaklaşımı ve hedefleri; bilgi güvenliği yönetim sistemi gereklilikleri çerçevesinde tanımlanır ve bu gereklilikler ile hedeflerin tüm çalışanlara ve ilgili paydaşlara etkin şekilde duyurulması amaçlanır.

Bu politika, tüm bilgi varlıklarını (elektronik veya basılı formlardaki BGYS ile ilgili tüm politikalara, prosedürlere, formlara, kayıtlara vb. dokümanlar) ve çalışanlarını ve bilgi güvenliğiyle ilgili tüm belgeler ile bilgi ve iletişim teknolojileri (ICT) varlıklarını, bu varlıklar üzerinden sunulan kritik hizmetleri, üçüncü taraflar aracılığıyla sağlanan bilgi teknolojisi hizmetlerini ve bunların kurumun operasyonel dayanıklılığı üzerindeki etkilerini de kapsar.

1. PURPOSE AND SCOPE

The purpose of this policy is to determine the information security principles aligned with the strategic direction of Figo Ticari Bilgi ve Uygulama Platformu A.Ş. ("Figopara" or the "Company"), to bring all its digital and physical assets under protection, and to define the fundamental information security principles.

Information security is addressed within Figopara not only as a technical matter, but as an integral part of corporate governance, risk management, digital operational resilience, ISO/IEC 27701, ISO/IEC 27001, ISO 22301, KVKK, standards and the sustainability approach. This policy takes as a basis the conduct of information security practices in compliance with European Union digital resilience regulations, OECD, ESG governance principles, ISO standards and international good practices.

As a part of our Integrated Management System (IMS), the establishment, operation, maintenance and continuous improvement of the Information Security Management System (ISMS) is carried out in line with the guidance of the management. Figopara's approach and objectives regarding information security are defined within the framework of the information security management system requirements, and the effective communication of these requirements and objectives to all employees and relevant stakeholders is intended.

This policy covers all information assets (all documents related to ISMS in electronic or printed forms such as policies, procedures, forms, records, etc.) and its employees and all documents related to information security as well as information and communication technologies (ICT) assets, the critical services provided through these assets, the information technology services provided through third parties, and their effects on the organization's operational resilience.

Figopara, bilgi güvenliği yönetim sistemi bağlamında iklim değişikliğinin kurumsal faaliyetler, bilgi varlıkları ve operasyonel süreklilik üzerindeki potansiyel etkilerini ilgili bir konu olarak değerlendirir. İklim değişikliğine bağlı riskler, bilgi güvenliği risk değerlendirmesi kapsamında dikkate alınır.	Figopara considers the potential impacts of climate change on corporate activities, information assets and operational continuity as a relevant issue within the context of its information security management system. Climate change-related risks are taken into account within the scope of information security risk assessment.
Tüm Paydaşlar (çalışanlar, yöneticiler, iş ortakları vb.) ve ilgili taraflar bu politikaya uymakla yükümlüdür.	All Stakeholders (employees, managers, business partners, etc.) and relevant parties are obliged to comply with this policy.
2. TANIMLAR VE KISALTMALAR	**2. DEFINITIONS AND ABBREVIATIONS**
BGYS: Bilgi Güvenliği Yönetim Sistemi	**ISMS:** Information Security Management System
Bilgi Güvenliği Standartları: Bilgi güvenliği standartları, şirketlerin bilgi varlıklarını koruma, güvenliğini sağlama ve bilgiye yetkisiz erişimi önleme amacıyla belirlenmiş kurallar, yönergeler ve uygulama kriterleridir. Bu standartlar, bilgi güvenliği yönetim sistemlerinin (BGYS) kapsamını ve gereksinimlerini tanımlar ve bu sistemlerin güvenilirlik, gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun olarak nasıl kurulması ve işletilmesi gerektiğini belirler.	**Information Security Standards:** Information security standards are the rules, guidelines and implementation criteria established for the purpose of protecting companies' information assets, ensuring their security and preventing unauthorized access to information. These standards define the scope and requirements of information security management systems (ISMS) and determine how these systems should be established and operated in accordance with the principles of reliability, confidentiality, integrity and accessibility.
EYS Ekibi (Entegre Yönetim Sistemi Ekibi): EYS ekibi yönetimi temsil eden, Entegre Yönetim sistemi kapsamında yer alan BGYS'nin başarılı biçimde sürdürülebilmesi için sorumluluğu üstlenen ve gözetimini sağlayan ekiptir.	**IMS Team (Integrated Management System Team):** The IMS team is the team that represents the management, undertakes the responsibility and provides the oversight for the successful sustaining of the ISMS within the scope of the Integrated Management System.
Veri Sorumlusu: Kişisel verilerin işlenme amaçlarını ve bu veriler üzerinde yapılacak işlemleri belirleyen ve karar veren gerçek veya tüzel kişidir.	**Data Controller:** Real or legal person who determines and decides on the purposes of processing personal data and the operations to be carried out on these data.
Veri İşleyen: Veri sorumlusunun talimatları doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişidir.	**Data Processor:** Real or legal person who processes personal data in line with the instructions of the data controller.
İç Denetçi: EYS'nin bağımsız olarak denetimini yapan kişi veya ekip. EYS'nin uygulanmasından ve	**Internal Auditor:** The person or team who independently audits the IMS. The person who is

işletiminden bağımsız, EYSkapsamındaki Yönetim Sistemlerinin denetimini yerine getirebilecek deneyim, eğitim ve sertifikasyonlara sahip kişi olup; iç denetimi gerçekleştiren kişidir. İç denetçi şirket personeli olabileceği gibi şirket dışından da sağlanabilir.	independent of the implementation and operation of the IMS, has the experience, training and certifications to carry out the audit of the Management Systems within the scope of the IMS, and who performs the internal audit. The internal auditor may be company personnel or may be provided from outside the company.
Paydaş: Figopara'nın bilgi güvenliği kapsamındaki faaliyetleriyle ilişkili olan veya bu faaliyetlerden etkilenen çalışanlar, yöneticiler, iş ortakları, tedarikçiler, hizmet sağlayıcılar ve üçüncü taraflardır.	**Stakeholder:** Employees, managers, business partners, suppliers, service providers and third parties who are related to or affected by Figopara's activities within the scope of information security.
Müşteri: Figopara'nın sunduğu ürün ve hizmetlerden yararlanan, Figopara ile sözleşmesel ilişki içinde bulunan veya hizmetlerin sunulması kapsamında kendisine ait veriler işlenen gerçek veya tüzel kişiyi ifade eder.	**Customer:** Refers to the real or legal person who benefits from the products and services offered by Figopara, who is in a contractual relationship with Figopara, or whose data is processed within the scope of providing the services.
ISO: (International Organization for Standardization) ürünlerin ve hizmetlerin kalite, güvenlik, verimlilik ve uyumluluk açısından belirli kriterlere göre yürütülmesini sağlayan uluslararası standartlar bütünüdür.	**ISO:** (International Organization for Standardization) is the body of international standards that ensures the conduct of products and services according to certain criteria in terms of quality, security, efficiency and compliance.
DORA (Digital Operational Resilience Act): Avrupa Birliği finansal kuruluşlarının bilgi ve iletişim teknolojileri kaynaklı operasyonel risklere karşı dayanıklılığını güçlendirmeyi amaçlayan düzenlemedir.	**DORA (Digital Operational Resilience Act):** The regulation that aims to strengthen the resilience of European Union financial institutions against operational risks arising from information and communication technologies.
ESG (Environmental, Social, Governance): Kurumsal sürdürülebilirlik kapsamında çevresel, sosyal ve yönetişim faktörlerini içeren çerçevedir.	**ESG (Environmental, Social, Governance):** The framework that includes environmental, social and governance factors within the scope of corporate sustainability.
Dijital Operasyonel Dayanıklılık: Bilgi sistemleri, süreçler ve üçüncü taraf bağımlılıkları dâhil olmak üzere, dijital operasyonların kesintilere karşı sürdürülebilir şekilde devam edebilme yeteneğidir.	**Digital Operational Resilience:** The ability of digital operations, including information systems, processes and third-party dependencies, to continue in a sustainable manner against interruptions.
ICT (Information and Communication Technologies): Bilgi ve İletişim Teknolojileri-Figopara'nın faaliyetlerini yürütmek, hizmet sunmak, veri işlemek, depolamak, iletmek veya	**ICT (Information and Communication Technologies):** Refers to all of the information systems, software, hardware, network infrastructures, digital platforms, applications, data centers, cloud

erişilebilir kılmak amacıyla kullandığı bilgi sistemleri, yazılımlar, donanımlar, ağ altyapıları, dijital platformlar, uygulamalar, veri merkezleri, bulut hizmetleri ve bunlarla ilişkili teknolojik bileşenlerin tümünü ifade eder.

3. ROLLER VE SORUMLULUKLAR

3.1. ÜST YÖNETİM

Üst Yönetim, bilgi güvenliği, dijital operasyonel dayanıklılık, kişisel verilerin korunması ve iş sürekliliğini kurumsal yönetişim, risk yönetimi ve sürdürülebilirlik yaklaşımının ayrılmaz bir parçası olarak ele alır; bu alanların ESG ilkeleri, ISO/IEC 27001, ISO/IEC 27701, ISO 22301, ISO 14001, ISO 45001 ve KVKK ile uyumlu şekilde yönetilmesinden nihai olarak sorumludur. Üst Yönetim, Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte olmasını, uygulanması için gerekli kaynak ve desteğin sağlanmasını ve politikanın en az yılda bir kez veya gerekli görülen durumlarda gözden geçirilerek onaylanmasını sağlar. Üst yönetimi temsilen bu görevi Yönetim Temsilcisi yapar ve Genel Müdür ve/veya Yönetim Kurulu'na onaylatır.

3.2. YÖNETİM TEMSİLCİSİ

Üst Yönetimi temsilen Bilgi Güvenliği Yönetim Sistemi'nin kurulması, uygulanması, izlenmesi, yönetilmesi ve sürekli iyileştirilmesini koordine eden kişidir. Bilgi güvenliği ve dijital operasyonel dayanıklılık risklerini izler, BGYS performansını Üst Yönetime raporlar ve politika ile ilgili gerekli güncellemeleri Yönetim Kurulu ve/veya Genel Müdür onayına sunar.

3.3. EYS EKİBİ

Şirket'in üst yönetimi tarafından görevlendirilen EYS ekibi, Bilgi Güvenliği Politikasının Şirket ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

services and the technological components related to these, that Figopara uses for the purposes of carrying out its activities, providing services, processing, storing, transmitting or making accessible data.

3. ROLES AND RESPONSIBILITIES

3.1. TOP MANAGEMENT

Top Management addresses information security, digital operational resilience, the protection of personal data and business continuity as an integral part of corporate governance, risk management and the sustainability approach; it is ultimately responsible for the management of these areas in compliance with ESG principles, ISO/IEC 27001, ISO/IEC 27701, ISO 22301, ISO 14001, ISO 45001, and KVKK. Top Management ensures that the Information Security Policy is of a nature that meets the needs of the organization, that the necessary resources and support are provided for its implementation, and that the policy is reviewed and approved at least once a year or in cases deemed necessary. Representing top management, this duty is performed by the Management Representative and is approved by the General Manager and/or the Board of Directors.

3.2. MANAGEMENT REPRESENTATIVE

Representing the Top Management, this is the person who coordinates the establishment, implementation, monitoring, management and continuous improvement of the Information Security Management System. He/she monitors information security and digital operational resilience risks, reports the ISMS performance to the Top Management, and submits the necessary updates regarding the policy to the approval of the Board of Directors and/or the General Manager.

3.3. IMS TEAM

The IMS team, assigned by the top management of the Company, is responsible for ensuring that the Information Security Policy is of a nature that meets the needs of the Company, for providing the necessary support and oversight for its implementation, and for reviewing the policy at least once a year or in cases that may require changes in the corporate policy.

EYS Ekibi, bilgi güvenliği uygulamalarının uluslararası standartlara, kurumsal sürdürülebilirlik, yönetişim ve operasyonel dayanıklılık hedefleriyle uyumlu şekilde yürütülmesini gözetir.	The IMS Team oversees that information security practices are carried out in compliance with international standards and with corporate sustainability, governance and operational resilience objectives.
3.4. TÜM PERSONEL Bilgi Güvenliği Politikasının gereklerinin görev alanlarının gerektirdiği biçimde yerine getirilmesinden sorumludur.	**3.4. ALL PERSONNEL** Responsible for fulfilling the requirements of the Information Security Policy in the manner required by their areas of duty.
4. ÜST YÖNETİM TAAHHÜDÜ Figopara Üst Yönetimi, EYS/BGYS sürecinde kurumun hedef ve politikalarını gerçekleştirmek için ESG sürdürülebilirlik, IFC Guideline, OECD, GDPR, ISO/IEC 27001, ISO/IEC 27701, ISO 22301, ISO 14001, ISO 45001 ve benzeri bilgi güvenliği standartları ile yasal yükümlülüklerde yer alan tüm gereksinimlerin yerine getirilecek şekilde kurulmasını ve işletilmesini taahhüt eder.	**4. TOP MANAGEMENT COMMITMENT** Figopara Top Management commits, in the IMS/ISMS process, to establishing and operating in such a way that all the requirements contained in ESG sustainability, IFC Guideline, OECD, GDPR, ISO/IEC 27001, ISO/IEC 27701, ISO 22301, ISO 14001, ISO 45001 and similar information security standards as well as legal obligations are fulfilled, in order to realize the organization's objectives and policies.
Figopara Üst Yönetimi, yayımlanmış ve uygulanmakta olan Bilgi Güvenliği Yönetim Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli olan kaynakları ve gerekli altyapı yatırımlarını tahsis edeceğini, sürecin etkinliğini sürekli iyileştireceğini ve bunun tüm çalışanlar tarafından anlaşılmasını sağlayacağını taahhüt eder.	Figopara Top Management commits to complying with the Information Security Management System that has been published and is being implemented, to allocating the necessary resources and the required infrastructure investments for the efficient operation of the system, to continuously improving the effectiveness of the process, and to ensuring this is understood by all employees.
Figopara Üst Yönetimi, bilgi güvenliğini dijital operasyonel dayanıklılığın temel unsurlarından biri olarak kabul eder; bilgi güvenliği ihlallerini yalnızca teknik bir konu olarak değil, aynı zamanda uluslararası standartlara uyum, kurumsal yönetişim, itibar ve sürdürülebilirlik açısından risk teşkil eden hususlar olarak ele almayı taahhüt eder.	Figopara Top Management accepts information security as one of the basic elements of digital operational resilience; it commits to addressing information security breaches not only as a technical matter, but also as matters that constitute risk in terms of compliance with international standards, corporate governance, reputation and sustainability.
Üst yönetim, bilgi ve iletişim teknolojileri (ICT) kaynaklı risklerin yönetilmesi ile dijital operasyonel dayanıklılığın sağlanmasına ilişkin çerçevenin oluşturulması, uygulanması ve gözetiminden nihai olarak sorumludur.	The top management is ultimately responsible for the establishment, implementation and oversight of the framework relating to the management of risks arising from information and communication technologies (ICT) and the ensuring of digital operational resilience.

Figopara, bilgi güvenliği ve siber tehditlere ilişkin bilgilerin, yürürlükteki mevzuat ve gizlilik yükümlülükleri çerçevesinde, ilgili taraflarla kontrollü ve sorumlu şekilde paylaşılmasını sağlar.	Figopara ensures that information regarding information security and cyber threats is shared with relevant parties in a controlled and responsible manner, within the framework of applicable legislation and confidentiality obligations.
5. POLİTİKA Figopara, verilerinin ve sistemlerinin yeterince korunması ve bilgi teknolojilerinin işleyişiyle ilişkili her türlü güvenlik riskinin yönetilmesi için yasal ve ticari sorumluluklara sahiptir. Figopara, bilgi ve iletişim sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini garanti altına almak, güvenlik risklerini yönetmek, operasyonel ve finansal verilerini korumak için yasal gereklilikler, ESG sürdürülebilirlik, IFC Guideline, OECD, GDPR, ISO/IEC 27001, ISO/IEC 27701, ISO 22301 ve benzeri bilgi güvenliği standartlara uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamayı hedefler. Bilgi güvenliği uygulamaları, risk bazlı ve orantılı bir yaklaşımla yürütülür. Alınan önlemler, bilginin niteliği, hassasiyeti ve kurum faaliyetleri üzerindeki etkisi dikkate alınarak belirlenir.	**5. POLICY** Figopara has legal and commercial responsibilities for adequately protecting its data and systems and for managing all kinds of security risks associated with the operation of information technologies. Figopara aims to implement an Information Security Management System (ISMS) compliant with legal requirements, ESG sustainability, IFC Guideline, OECD, GDPR, ISO/IEC 27001, ISO/IEC 27701, ISO 22301 and similar information security standards, in order to guarantee the confidentiality, integrity and accessibility of its information and communication systems, to manage security risks, and to protect its operational and financial data. Information security practices are carried out with a risk-based and proportional approach. The measures taken are determined by considering the nature and sensitivity of the information and its impact on the organization's activities.
ISO/IEC 27001, ISO/IEC 27701 ve benzeri bilgi güvenliği standartları Bilgi Güvenliği Yönetim Sistemi gerekliliklerine uygun olarak, risk bazlı düşünme yaklaşımı ile gerçekleştirdiğimiz ve sürekli iyileştirdiğimiz süreçlerimiz sayesinde, sunduğumuz ürün ve hizmetlerin müşterilerimizin ihtiyaç ve beklentilerini karşılanmasını, çalışanlarımız, müşterilerimizin, tedarikçilerimizin ve iş ortaklarımızın bilgilerinin gerekli şekilde korunmasını taahhüt edip güvence altına almaktayız.	In compliance with the requirements of the Information Security Management System of ISO/IEC 27001, ISO/IEC 27701 and similar information security standards, thanks to our processes that we carry out and continuously improve with a risk-based thinking approach, we commit and guarantee that the products and services we offer meet the needs and expectations of our customers, and that the information of our employees, customers, suppliers and business partners is protected as required.
ISO/IEC 27701 kapsamında, kişisel verilerin korunmasına yönelik mahremiyet bilgisi yönetimi gereklilikleri mevcut Bilgi Güvenliği Yönetim Sistemi'ne (BGYS) entegre edilir. Kişisel veri işleme faaliyetlerine ilişkin gizlilik risklerinin belirlenmesi, değerlendirilmesi ve yönetilmesi BGYS süreçleri kapsamında yürütülür.	Under ISO/IEC 27701, privacy information management requirements for the protection of personal data are integrated into the existing Information Security Management System (ISMS). The identification, assessment, and management of privacy risks associated with personal data processing

	activities are carried out within the scope of ISMS processes.
Figopara tarafından onaylanmış olan bu Bilgi Güvenliği Politikasının amacı; • İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı kuruluşun bilgi varlıklarını korumak, • Bilginin gizliliğini ve bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimine karşı korumak, • Bilgiye erişilebilirliği iş süreçleriyle gerektiği şekilde sağlamak, • ESG, OECD, IFC, GDPR ve ISO/IEC 27701 ile ISO/IEC 27001 standartlarına uyumu sağlamak, • Yasal mevzuat gereksinimlerini karşılamak, • İş sürekliliği ve Kriz Yönetimi için planları hazırlamak, sürdürmek ve test etmek, • Tüm çalışanların bilgi güvenliği eğitimlerine katılımını ve BGYS farkındalığını sağlamak, • Bilgi Güvenliği Yönetim Sisteminin etkin bir şekilde yönetilmesini sağlamak amacıyla risk analizi çalışmalarını yapmak, • Bilgi güvenliği risklerini yönetmek için riskleri değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirmek, gerekli tedbirleri geliştirmek ve olası riskleri önlemek için çalışmalar yapmak, • Bilgi güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıkları, Etik ve İhlal Yönetim platformu FRED (Figo Risk and Ethics Desk) aracılığıyla bildirmek ve Etik ve İhlal Komitesi tarafından soruşturulmasını sağlamak, • Bilgiye erişilebilirlik ve bilgi sistemleri için iş gereksinimlerini karşılamak, • Kapsamda yer alan süreçleri Bilgi Güvenliği Yönetim Sistemi'ne uygun hale getirmek,	The purpose of this Information Security Policy, which has been approved by Figopara, is; • To protect the information assets of the organization against all kinds of threats that may arise from inside or outside, knowingly or unknowingly, • To protect the information against the access of unauthorized persons who will attempt to disrupt the confidentiality and integrity of the information, • To ensure accessibility to information as required by business processes, • To ensure compliance with ESG, OECD, IFC, GDPR and ISO/IEC 27701 and ISO/IEC 27001 standards, • To meet the legal legislation requirements, • To prepare, sustain and test plans for Business Continuity and Crisis Management, • To ensure the participation of all employees in information security trainings and ISMS awareness, • To carry out risk analysis activities for the purpose of ensuring that the Information Security Management System is effectively managed, • To carry out risk evaluation, risk analysis and risk treatment activities for the management of information security risks, to develop the necessary measures and to carry out activities for preventing potential risks, • To report all actually existing or suspected vulnerabilities in information security through the Ethics and Breach Management platform FRED (Figo Risk and Ethics Desk) and to ensure their investigation by the Ethics & Breach Committee, • To meet the business requirements for accessibility to information and for information systems, • To bring the processes within the scope into compliance with the Information Security Management System,

- Bilgi güvenliği yönetim sistemimizin amaçlanan sonuçları yerine getirme başarısını periyodik olarak gözden geçirmek, gerekli iyileştirmelerin zamanında hayata geçirilmesini güvence altına almak
- Bilgi güvenliğini dijital operasyonel dayanıklılığın temel unsurlarından biri olarak ele almak ve bilgi ve iletişim teknolojileri (ICT) kaynaklı risklerin kurumsal faaliyetler üzerindeki etkilerini yönetmek,
- Bilgi güvenliği ve ICT kaynaklı risklerin yönetimine ilişkin üst yönetim gözetimini ve hesap verebilirliği sağlamak,
- Üçüncü taraflar ve hizmet sağlayıcılar aracılığıyla yürütülen faaliyetlerde bilgi güvenliği ve dijital operasyonel dayanıklılık risklerini yönetmek,
- Bilgi güvenliği olaylarının ve siber güvenlik vakalarının, ilgili mevzuat kapsamında doğabilecek bildirim ve raporlama yükümlülükleri çerçevesinde ele alınmasını sağlamaktır.

Şirket bünyesindeki BGYS kapsamında yayımlanan tüm dokümanlar, Bilgi Güvenliği Politikasını destekler. Yönetim Temsilcisi bu politikanın sürdürülmesinden ve politikanın gerçekleştirilmesi konusunda tavsiyelerde bulunmaktan, yol göstermekten doğrudan sorumludur ve yetkili otoritedir.

6. GENEL İLKE VE ESASLAR

6.1. DİJİTAL OPERASYONEL DAYANIKLILIK İLKESİ

Figopara, bilgi güvenliğini dijital operasyonel dayanıklılığın ayrılmaz bir unsuru olarak ele alır. Bilgi ve iletişim teknolojileri (ICT) kaynaklı riskler, Figopara'nın kurumsal risk yönetimi ve operasyonel dayanıklılık çerçevesine entegre edilir ve üst yönetimin aktif gözetimi altında yönetilir.

- To periodically review the success of our information security management system in fulfilling the intended outcomes, and to guarantee the timely realization of the necessary improvements,
- To address information security as one of the basic elements of digital operational resilience and to manage the effects of risks arising from information and communication technologies (ICT) on corporate activities,
- To ensure top management oversight and accountability regarding the management of information security and ICT-related risks,
- To manage information security and digital operational resilience risks in activities carried out through third parties and service providers,
- To ensure that information security incidents and cyber security cases are addressed within the framework of notification and reporting obligations that may arise under the relevant legislation.

All documents published within the scope of the ISMS within the Company support the Information Security Policy. The Management Representative is directly responsible and is the authorized authority for sustaining this policy and for making recommendations and providing guidance regarding the realization of the policy.

6. GENERAL PRINCIPLES AND BASES

6.1. DIGITAL OPERATIONAL RESILIENCE PRINCIPLE

Figopara addresses information security as an integral element of digital operational resilience. Risks arising from information and communication technologies (ICT) are integrated into Figopara's corporate risk management and operational resilience framework and are managed under the active oversight of the top management.

Kritik bilgi sistemlerinin ve bu sistemler üzerinden sunulan hizmetlerin sürekliliğinin korunması, Figopara açısından temel bir kurumsal önceliktir. Bilgi güvenliği olayları ve siber güvenlik vakaları, kurumun operasyonel dayanıklılığını etkileyebilecek riskler olarak değerlendirilir ve ilgili mevzuat kapsamında yetkili otoritelere bildirim yükümlülüğü doğurabilecek nitelikteki olaylar dikkate alınır.	The preservation of the continuity of critical information systems and the services offered through these systems is a fundamental corporate priority for Figopara. Information security incidents and cyber security cases are evaluated as risks that may affect the operational resilience of the organization, and incidents that may give rise to a notification obligation to the competent authorities under the relevant legislation are taken into consideration.
6.2. ICT RİSK YÖNETİMİ VE OLAYLARA HAZIRLIK Bilgi güvenliği riskleri, Figopara'nın kurumsal risk envanterinin ayrılmaz bir parçası olarak ele alınır. Bu risklerin belirlenmesi, değerlendirilmesi ve yönetilmesi risk bazlı ve orantılı bir yaklaşımla yürütülür. Bilgi güvenliği olaylarının yönetimi, kurumsal risk yönetimi ve şeffaflık ilkeleri doğrultusunda ele alınır. Olayların sınıflandırılması, bildirimi ve müdahalesine ilişkin detaylar ilgili prosedürler aracılığıyla düzenlenir.	**6.2. ICT RISK MANAGEMENT AND PREPAREDNESS FOR INCIDENTS** Information security risks are addressed as an integral part of Figopara's corporate risk inventory. The identification, evaluation and management of these risks are carried out with a risk-based and proportional approach. The management of information security incidents is addressed in line with corporate risk management and transparency principles. Details regarding the classification, notification and response to incidents are regulated through the relevant procedures.
6.3. ÜÇÜNCÜ TARAF VE ICT HİZMET SAĞLAYICI YÖNETİMİ Üçüncü taraflar ve hizmet sağlayıcılar aracılığıyla erişilen bilgi ve sistemler, Figopara'nın bilgi güvenliği ilkelerine tabidir. Dijital operasyonel dayanıklılık açısından kritik nitelikte olan üçüncü taraf hizmet sağlayıcılar, bilgi güvenliği ve operasyonel risk perspektifiyle ayrıca değerlendirilir. Üçüncü taraflarla kurulan sözleşmelerde bilgi güvenliği, denetim ve gerekli hâllerde fesih hakları gözetilir.	**6.3. THIRD PARTY AND ICT SERVICE PROVIDER MANAGEMENT** Information and systems accessed through third parties and service providers are subject to Figopara's information security principles. Third party service providers that are critical in terms of digital operational resilience are additionally evaluated from an information security and operational risk perspective. In contracts established with third parties, information security, audit and, where necessary, termination rights are observed.
6.4. İŞ SÜREKLİLİĞİ VE BİLGİ GÜVENLİĞİ ENTEGRASYONU Bilgi güvenliği, Figopara'nın iş sürekliliği yaklaşımının temel bileşenlerinden biridir.	**6.4. BUSINESS CONTINUITY AND INFORMATION SECURITY INTEGRATION** Information security is one of the basic components of Figopara's business continuity approach.

Kritik bilgi varlıklarının ve bilgi sistemlerinin sürekliliğinin korunması, iş sürekliliği hedefleriyle bütünleşik şekilde ele alınır.	The preservation of the continuity of critical information assets and information systems is addressed in an integrated manner with business continuity objectives.
İş sürekliliği, felaket kurtarma, test ve tatbikatlara ilişkin detaylar ilgili prosedürler kapsamında düzenlenir.	Details regarding business continuity, disaster recovery, tests and exercises are regulated within the scope of the relevant procedures.
6.5. KURUMSAL YÖNETİŞİM, HESAP VEREBİLİRLİK VE ESG YAKLAŞIMI Bilgi güvenliği, Figopara'nın kurumsal yönetişim ve ESG (Environmental, Social, Governance) yaklaşımının ayrılmaz bir parçasıdır.	**6.5. CORPORATE GOVERNANCE, ACCOUNTABILITY AND ESG APPROACH** Information security is an integral part of Figopara's corporate governance and ESG (Environmental, Social, Governance) approach.
Üst yönetim, bilgi güvenliği risklerinin yönetilmesi konusunda hesap verebilirliğe sahiptir.	The top management has accountability regarding the management of information security risks.
Bilgi güvenliği uygulamaları, kurumsal şeffaflık, hesap verebilirlik ve etik yönetim ilkeleriyle uyumlu şekilde yürütülür.	Information security practices are carried out in compliance with the principles of corporate transparency, accountability and ethical management.
Bilgi güvenliği ihlalleri yalnızca teknik bir konu olarak değil; aynı zamanda yönetişim, itibar ve sürdürülebilirlik riski olarak değerlendirilir.	Information security breaches are evaluated not only as a technical matter; but also as a governance, reputation and sustainability risk.
6.6. VERİ ETİĞİ, GİZLİLİK VE MÜŞTERİ BİLGİLERİNİN KORUNMASI Veri güvenliği ve gizliliği, Figopara'nın paydaş güveninin korunmasına yönelik temel sorumluluklarındandır.	**6.6. DATA ETHICS, PRIVACY AND PROTECTION OF CUSTOMER INFORMATION** Data security and privacy are among Figopara's basic responsibilities for the preservation of stakeholder trust.
Kişisel veriler, finansal müşteri bilgileri ve ticari sırlar yüksek hassasiyetli bilgi varlıkları olarak kabul edilir ve amaçla sınırlılık, yetkilendirme ve gizlilik ilkeleri çerçevesinde ele alınır.	Personal data, financial customer information and trade secrets are accepted as highly sensitive information assets and are addressed within the framework of the principles of purpose limitation, authorization and confidentiality.
Yetkisiz erişimlerin önlenmesi ve veri güvenliğinin sağlanması, kurumsal etik yükümlülüğün bir parçasıdır.	The prevention of unauthorized access and the ensuring of data security are part of the corporate ethical obligation.

6.7. SÜREKLİ İZLEME VE YÖNETİMİN BİLGİLENDİRİLMESİ	**6.7. CONTINUOUS MONITORING AND INFORMATION OF MANAGEMENT**
Bilgi güvenliği ile ilgili riskler, önemli gelişmeler ve ortaya çıkan tehditler, üst yönetimin bilgilendirilmesini sağlayacak şekilde ele alınır.	Risks related to information security, important developments and emerging threats are addressed in a way that ensures the information of the top management.
Bilgi güvenliği yönetimi, değişen tehdit ortamı ve kurumsal ihtiyaçlar doğrultusunda sürekli gözden geçirilir ve geliştirilir.	Information security management is continuously reviewed and developed in line with the changing threat environment and corporate needs.
6.8. STANDARTLARA UYUMUN SAĞLANMASI ISO/IEC 27001 standardı kapsamında tanımlanan kontrol hedefleri ve kontroller, Figopara bünyesinde ilgili prosedürler aracılığıyla uygulanır.	**6.8. ENSURING COMPLIANCE WITH STANDARDS** The control objectives and controls defined within the scope of the ISO/IEC 27001 standard are implemented within Figopara through the relevant procedures.
7. İLGİLİ DOKÜMANLAR **7.1. DAHİLİ DOKÜMANLAR** 1. KP.001 Kapsam Analizi Dokümanı 2. PO.01 Entegre Yönetim Sistemi Politikası 3. PO.03 Kabul Edilebilir Kullanım Politikası 4. PO.04 Bilişim Teknolojileri Yönetim Politikaları 5. PO.08 Sürdürülebilirlik ve Çevre Politikası 6. PO.09 İnsan ve Kültür Yönetim Politikası 7. PR.02 Roller ve Sorumlulukların Tahsisi Prosedürü 8. PR.05 Yönetim Faaliyetleri Prosedürü 9. PR.06 Varlık Yönetimi ve Veri Sınıflandırma Prosedürü 10. PR.08 İş Sürekliliği Prosedürü 11. PR.09 İç Tetkik Prosedürü 12. PR.20 Disiplin Prosedürü 13. PR.32 Etik ve İhlal Olayları Yönetim Prosedürü 14. PR.34 Erişim Kontrol Ve Ayrıcalıklı Haklar Prosedürü 15. PR.40 Üçüncü Taraflarla Çalışma Prosedürü	**7. RELATED DOCUMENTS** **7.1. INTERNAL DOCUMENTS** 1. KP.001 Scope Analysis Document 2. PO.01 Integrated Management System Policy 3. PO.03 Acceptable Use Policy 4. PO.04 Information Technology Management Policies 5. PO.08 Sustainability and Environment Policy 6. PO.09 People and Culture Management Policy 7. PR.02 Procedure for the Allocation of Roles and Responsibilities 8. PR.05 Management Activities Procedure 9. PR.06 Asset Management and Data Classification Procedure 10. PR.08 Business Continuity Procedure 11. PR.09 Internal Audit Procedure 12. PR.20 Disciplinary Procedure 13. PR.32 Ethics and Breach Incidents Management Procedure 14. PR.34 Access Control and Privileged Rights Procedure 15. PR.40 Procedure for Working with Third Parties
7.2. HARİCİ DOKÜMANLAR 1. OECD Recommendation on Digital Security Risk Management 2. IFC Information Security & Risk Governance Guidelines	**7.2. EXTERNAL DOCUMENTS** 1. OECD Recommendation on Digital Security Risk Management 2. IFC Information Security & Risk Governance Guidelines

3. ISO / IEC 27001: 2022 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler 4. ISO 27701:2019 KVYS Kişisel Veri Yönetim Sistemi – Gereksinimler 5. ISO/IEC 27701:2025 Mahremiyet Bilgisi Yönetim Sistemleri – Gereksinimler ve Rehberlik 6. ISO 22301:2019 İş Sürekliliği Yönetimi Sistemi – Gereksinimler 7. ISO 14001:2026 – Çevre Yönetim Sistemleri Gereklilikleri ve Kullanım Kılavuzu 8. ISO 45001:2018 ve ISO 45001:2018/Amd 1:2024 – İş Sağlığı ve Güvenliği Yönetim Sistemleri Gereklilikleri 9. 6698 sayılı Kişisel Verilerin Korunması Kanunu, ilgili ikincil düzenlemeler, Kurul kararları ve KVKK rehberleri 10. 7545 sayılı Siber Güvenlik Kanunu ve uygulanabilir ikincil düzenlemeler 11. 7552 sayılı İklim Kanunu, 2872 sayılı Çevre Kanunu ve ilgili çevre, enerji ve atık yönetimi düzenlemeleri 12. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu, 4857 sayılı İş Kanunu ve ilgili yönetmelikler 13. Avrupa Birliği 2016/679 sayılı Genel Veri Koruma Tüzüğü (GDPR), uygulanabildiği ölçüde 14. Türkiye Sürdürülebilirlik Raporlama Standartları (TSRS 1 ve TSRS 2) ile ilgili kapsam kararları 15. Kişisel Verileri Koruma Kurumu Veri Güvenliği Rehberi (İdari ve Teknik Tedbirler)	3. ISO / IEC 27001: 2022 Information Technology - Security Techniques - Information Security Management Systems - Requirements 4. ISO 27701:2019 PIMS Personal Information Management System – Requirements 5. ISO/IEC 27701:2025 Privacy Information Management Systems – Requirements and Guidance 6. ISO 22301:2019 Business Continuity Management System – Requirements 7. ISO 14001:2026 – Environmental Management Systems – Requirements with Guidance for Use 8. ISO 45001:2018 and ISO 45001:2018/Amd 1:2024 – Occupational Health and Safety Management Systems – Requirements with Guidance for Use 9. Law No. 6698 – Personal Data Protection Law No. 6698, relevant secondary legislation, Board decisions and KVKK guidelines 10. Law No. 7545 – Cybersecurity Law No. 7545 and applicable secondary legislation 11. Law No. 7552 and Law No. 2872 – Climate Law No. 7552, Environment Law No. 2872 and related environmental, energy and waste management regulations 12. Law No. 6331 and Law No. 4857 – Occupational Health and Safety Law No. 6331, Labour Law No. 4857 and related regulations 13. EU Regulation 2016/679 – Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR), to the extent applicable 14. TSRS 1 and TSRS 2 – Türkiye Sustainability Reporting Standards (TSRS 1 and TSRS 2) and related scope decisions 15. Personal Data Protection Authority Data Security Guide (Administrative and Technical Measures)

8. DAĞITIM Bu dokuman elektronik ortamda tüm paydaşlarla paylaşılmaktadır.	**8. DISTRIBUTION** This document is shared with all stakeholders in electronic environment.
9. YAPTIRIM Bu dokumana aykırı davranılması durumunda **Disiplin Prosedürü** dikkate alınarak işlem yapılacaktır.	**9. SANCTION** In case of acting contrary to this document, action will be taken by taking the Disciplinary Procedure into consideration.
9.1. UYUM Bu politikanın ihlali, veri koruma mevzuatı kapsamındaki veri ihlallerine, şirketin itibarının zarar görmesine ve çalışanların veya diğer ilgili üçüncü şahısların haklarının ihlal edilmesine neden olabilir.	**9.1. COMPLIANCE** The breach of this policy may cause data breaches within the scope of data protection legislation, damage to the reputation of the company and the violation of the rights of employees or other related third parties.
9.2. İSTİSNALAR Politika ile ilgili herhangi bir istisna, önceden Genel Müdür ve / veya Veri Sorumlusunun kendisine bildirilecektir.	**9.2. EXCEPTIONS** Any exception related to the policy will be notified in advance to the General Manager and/or the Data Controller themselves.
9.3. UYUMSUZLUK Bu politikalara uyulmaması, Şirketin disiplin prosedürlerine uygun olarak disiplin cezasına yol açabilir. Üçüncü taraf bir yüklenicinin (veya alt yüklenicilerin) bu politikaya uymaması, sözleşmenin ve / veya yasal işlemin feshine yol açabilir. Uygunsuzluk, Genel Müdür ve / veya Veri Sorumlusunun kendisine bildirilecektir.	**9.3. NON-COMPLIANCE** Failure to comply with these policies may lead to disciplinary penalty in accordance with the Company's disciplinary procedures. Failure of a third party contractor (or subcontractors) to comply with this policy may lead to the termination of the contract and/or legal action. Non-compliance will be notified to the General Manager and/or the Data Controller themselves.