1. Kapsam

Bu politika, bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanmasını, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini ve gözetimini kapsar.

2. Amaç

Şirket bilgi sistemlerinin ve bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla gerekli gereksinimlerini tanımlamak, bilgilerin ve tüm destek iş sistemlerinin, süreçlerinin ve uygulamalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmektir. Bunun anlamı; bilgilerin yetkili ellerde kalması, bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması ve bilgilerin, sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır.

Bilgi Güvenliği Politikası, halka açık şirketler için Sermaye Piyasası Kurulu tarafından yürürlüğe konan VII-128.9 Bilgi Sistemleri Yönetimi Tebliği (Tebliğ), TS EN ISO 27001 Standardı, Kişisel Verilerin Korunması Kanunu ve diğer düzenlemeler dikkate alınarak hazırlanmıştır.

Şirket, Bilgi Güvenliği Yönetim Sistemi süreçlerinin işletilmesi ve sürekliliğinin sağlanması için gereken kontrollerin tesis edilmesini ve gözetimini bu politikaya bağlı alt politikalar, prosedürler ve talimatlar vasıtasıyla sağlar.

Şirket özellikle aşağıda belirtilen konuların yerine getirilmesini benimsemiştir:

− Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak.

− Bilgi varlıkları, değerleri, güvenlik ihtiyaçları, zafiyetleri, varlıklara yönelik tehditlerin, tehditlerin sıklıklarının saptanması için yöntemlerin belirleyeceği çerçeveyi tanımlamak.

− Tehditlerin varlıklar üzerindeki gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamak.

− Risklerin işlenmesi için çalışma esaslarını ortaya koymak.

− Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek.

− Tabi olduğu ulusal veya uluslararası düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.

− Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak.

− Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak.

− Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.

− Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak.

− Bilgi Güvenliği Yönetim Sisteminin sürekliliğini sağlamak.

− Bilgi Güvenliği Yönetim Sistemini sürekli iyileştirmek amacıyla tüm çalışmalara destek vermek.

Üst yönetim: Yönetim kurulu tarafından belirlenen kişi ya da grubu, yönetim kurulu tarafından belirleme yapılmadığı durumlarda ise Şirket'in en üst yetkilisini ifade eder.

3. Sorumlular

A. Yönetim Kurulu

Bilgi güvenliği politikası üst yönetim tarafından hazırlanır ve yönetim kurulu tarafından onaylanır. Bilgi güvenliği politikası kapsamında bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi yönetim kurulunun sorumluluğundadır. Yönetim Kurulu, politikanın gözetiminden sorumlu "Üst Yönetim1" i yetkilendirir. Atanacak yetkiler ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olur.

B. Üst Yönetim

Üst Yönetim, Bilgi Güvenliği ile ilgili genel yönetim çerçevesinin oluşturulmasından, sürekliliğinin sağlanmasından, bu politikanın, güncel olarak yaşamasını ve Şirket ve iştiraklerinin işle ilgili gerekliliklerini veya bilgilerinin ve bilgi sistemlerinin karşı karşıya olduğu risk ortamındaki ya da tehditlerdeki değişimleri yansıtmaya devam etmesini temin edecek şekilde devamlı gözden geçirilmesinden sorumlu olacaktır. Politika kapsamında hazırlanması gereken tüm standart, prosedür ve talimatların onaylanması için Yönetim Kurulu tarafından, ***Kurumsal Yönetim Genel Müdür Yardımcısından*** oluşmak üzere ***Üst Yönetim*** yetkilendirilmiştir.

Bilgi güvenliği politikasının uygulanması Üst Yönetim tarafından gözetilir. Üst Yönetim, bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak üzere bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesini, işletilmesini, güncelliğini sağlar ve gerekli yönetsel sorumlulukları tanımlar.

Üst Yönetim'in gözetimi ve sorumluluğu aşağıdaki gibidir:

− Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,

− Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,

− Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,

− Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi.

− Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürler, organizasyonel ve yönetsel yapı içerisinde fiili olarak işleyecek şekilde yerleştirilir ve işlerliğine ilişkin gözetim ve takipler gerçekleştirilir.

− Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir Bilgi Sistemleri Güvenliği Sorumlusu belirlenir.

− Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanır. Planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı belirlenir.

Üst yönetim: Yönetim kurulu tarafından belirlenen kişi ya da grubu, yönetim kurulu tarafından belirleme yapılmadığı durumlarda ise Şirket'in en üst yetkilisini ifade eder.

C. Bilgi Sistemleri Güvenliği Sorumlusu

Bilgi Güvenliği Yönetim Ekibi (BGYS Ekibi)' nden oluşmak üzere **Bilgi Sistemleri Güvenliği Sorumlusu,** bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olup, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip kişidir. Genel olarak bilgi güvenliği olaylarının ele alınmasında rehberlik eder, politikanın ayrıntılı standartlar, prosedürler ve süreçlerle desteklenmesini ve bunların gerek doğdukça kullanıma hazır olmasını sağlar. Ayrıca bu politika gereklerinin tüm çalışanlara (daimî veya dönemsel) ve tüm yüklenici personeline aktarılmasını sağlamaktan sorumlu olacaktır. Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği Bilgi Sistemleri Güvenliği Sorumlusu tarafından yürütülecek ve bu yöneticilik, aynı zamanda politikanın tüm Şirket bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.

D. Diğer Paydaşlar

Tüm çalışanlar, Bilgi Güvenliği Yönetim Sistemi kategorisinde yayınlanmış tüm politika ve prosedürlere uymakla, gerçekleşmiş ya da olası güvenlik ihlallerini ve zafiyetlerini bildirmek ve Şirket tarafından talep edilen tüm faaliyetleri gerçekleştirmekle yükümlüdür. Şirket çalışanları konumları veya görevleri ne olursa olsun işlerini, bilgilerin Şirket bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur. Bilgi Güvenliği Politikaları ister tam zamanlı ister yarı zamanlı, daimî ya da sözleşmeli olsun, tüm bilgileri veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu bağlamda Varlık ve Süreç Sahipleri;

− Kendilerine duyurulan Bilgi Güvenliği Politikasına ve prosedürlerine uymak.

− Kendi süreç ve sistemlerinin yönetimleri için oluşturacakları süreç, akış, talimat, kılavuz, form gibi dokümanlarda Bilgi Güvenliği dokümanlarına uyumu sağlamak.

− Bilgi Güvenliği politikalarına ve/veya prosedürlerine uyumun sağlanmadığı veya bilgi güvenliği ihlal olaylarında **info@kafein.com.tr** adresine bildirmek

− Bilgi sistemlerinin çalışmasını olumsuz etkileyebilecek veya bilgi güvenliğini tehlikeye atacak faaliyetlerde bulunmamak.

− Bilgi Güvenliği dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi Sistemleri Güvenliği Sorumlusu bildirmek.

− Bilgi ve kurumsal kaynaklarına iş ihtiyaçları ölçüsünde erişim talebinde bulunmak.

− Sahibi olunan varlığın ve Kişisel Verilerin, erişim haklarını ve kimlerin yönetici ve kullanıcı bazında hangi ayrıcalıkla erişilebileceğini tayin etmek.

− Varlık envanterini gözlemlemek ve güncelliğini sağlamak,

− Sahibi oldukları varlıkların Kişisel Verileri dahil olmak üzere sınıflandırmasını, güncellenmesini ve gözden geçirilmesini sağlamaktan sorumludur.

Bilgi Güvenliği Politikası ilkeleri, Şirket İnsan Kaynaklarının Personel Yönetmeliği Kurallarına paralel uygulanmalıdır. Çalışanlar ayrıca Bilgi Güvenliği Politikasının farkında olmaktan ve bu ilkelere uymaktan sorumludur.

Üst yönetim: Yönetim kurulu tarafından belirlenen kişi ya da grubu, yönetim kurulu tarafından belirleme yapılmadığı durumlarda ise Şirket'in en üst yetkilisini ifade eder.

Herhangi bir Şirket çalışanı Bilgi Güvenliği Politikaların gelişmesi ve Şirket' in ihtiyaç duyduğu kontrolleri daha iyi yansıtması amacıyla politikaların değiştirilmesi konusunda *Bilgi Sistemleri Güvenliği Sorumlusu' na* talepte bulunabilir. Yapılan talepler *Bilgi Sistemleri Güvenliği Sorumlusu* tarafından ele alınır ve değerlendirilir.

Üçüncü Partiler

Şirket'e mal ve hizmet sağlayan üçüncü kişilerin ve bunların çalışanlarının uyması gereken bilgi güvenliğine ilişkin düzenlemeler ilgili sözleşmeler ve güvenlik protokolleri ile belirlenir. Bunlar asgari aşağıdaki hususları kapsar:

− Sözleşmeler veya protokoller ile bildirilen bilgi güvenliği kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen Şirket Politika ve Prosedürleri' ne uygun hareket etmek.

− Şirket'e ait bilgi ve varlıkları Şirket onayı ve izni olmadan başkaları ile paylaşmamak.

− Şirket tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak

− Şirket'in onay ve izni olmadan, Şirket'in cihazlarındaki hiçbir veri ve yazılımı kopyalamamak, ortamın ses kaydını almamak, resmini, videosunu çekmemek, veri güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak.

− Şirket lokasyonlarında yapılacak sistem erişimlerini Bilgi Teknolojileri ekiplerinin gözetiminde gerçekleştirmek.

Şirket personeli sınıflandırmasına girmeyen ve Şirket bilgilerine erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.

4. Denetim ve Kontrol

Bilgi Güvenliği politikaları Şirket bilgi varlıklarının karşı karşıya olduğu güncel riskleri yansıtması amacıyla yapılan varlık ve risk güncellemelerine paralel olarak en az yılda bir kez bilgi sistemlerine ilişkin "Risk Analizi ve İç Tetkikler" yapılır. Yeni riskleri ve risklerde meydana gelen değişiklikleri kontrol altında tutmak için Bilgi Güvenliği Politikaları gerekli eklemeler veya değişiklikler yapılarak güncellenir. Şirket, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından en az yılda bir kez "Sızma Testi" ne tabi tutulur. Sızma testine ilişkin usul ve esaslarda SPK Bilgi Sistemleri Yönetimi Tebliği ekinde yer alan şartlar esas alınır.

Kafein, "TS EN ISO 27001" standardı gerekliliklerini sağlamakta ve (TÜRKAK'tan Akredite kuruluşlar tarafından) denetimlerine tabi tutulmaktadır. Her 3 yılda 1 kez "Yeniden Belgelendirme" yapılır. Bütün bir çevrim içerisinde ise her yıl "Gözetim denetimleri" gerçekleştirilir.

Bilgi Sistemleri Güvenliği Sorumlusu başta Bilgi Güvenliği Politikası olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyumun periyodik olarak denetiminden ve Üst Yönetim'e raporlanmasından sorumludur. Üst yönetim politikanın uygulanmasını gözetir, sorumluları atar, hazırlanması gereken tüm standart, prosedür ve talimatları onaylar.

Bilgi sistemleri kontrollerine ilişkin etkinlik, yeterlilik ve uygunluk ile öngörülen risk ya da risklerin etkisini azaltmaya yönelik faaliyetler devamlı bir şekilde takip edilir ve değerlendirilir.

HAZIRLAYAN	ONAYLAYAN
KALİTE YÖNETİCİSİ	KURUMSAL YÖNETİM GENEL MÜDÜR YRD

Üst yönetim: Yönetim kurulu tarafından belirlenen kişi ya da grubu, yönetim kurulu tarafından belirleme yapılmadığı durumlarda ise Şirket'in en üst yetkilisini ifade eder.

Değerlendirme neticesinde tespit edilen önemli kontrol eksiklikleri Üst Yönetime raporlanır ve gerekli önlemlerin alınması sağlanır.

Bilgi Güvenliği Politikası ihlalleri, Şirket'in risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca yeni Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda Şirket Personel Yönetmeliği ihlali olup disiplin cezası sonucunu doğurabilir. Gerek gözetim gerek denetim gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri şirket içi disiplin cezalarının uygulanması, istihdama son verilmesi hatta Adli ve Cezai yasal işlemler başlatılması sonuçlanabilecektir.

5. Yürürlük

Bu Bilgi Güvenliği Politikası Yönetim Kurulu kararı ile yürürlüğe girmiştir. Bilgilendirme Politikasında herhangi bir değişiklik gerektiğinde, değişiklik yapılan hususlar Yönetim Kurulu onayından geçtikten sonra geçerlilik kazanır. Onaylanan bilgi güvenliği politikası personele duyurulur.

Şirket Yönetim Kurulu

Üst yönetim: Yönetim kurulu tarafından belirlenen kişi ya da grubu, yönetim kurulu tarafından belirleme yapılmadığı durumlarda ise Şirket'in en üst yetkilisini ifade eder.