

Bilgi Güvenliği

Politikası

**V.01 – 01.05.2024**

Bu dokümanın amacı

Bilgi Güvenliği Politikası, kuruluşun yeterli bilgi güvenliğini sağlamayı taahhüt eden gerekli bir dokümandır.

Standardın ele alınan maddeleri

ISO/IEC 27001 standardının şu alanları bu belgede ele alınmaktadır:

* 5 Liderlik
	+ 5.1 Liderlik ve bağlılık
	+ 5.2 Politika
* A.5 Bilgi güvenliği politikaları
	+ A.5.1 Bilgi güvenliği için yönetim yönü
		- A.5.1.1 Bilgi güvenliği politikaları

Gözden geçirme sıklığı

Bu belgenin, risk değerlendirmesi ve eğitim planı gibi önemli belgeleri de kapsayan yıllık bir çalışmanın parçası olarak gözden geçirilmelidir. Bu uygulama, değişen gereksinimlerin yakalanmasını ve müşteri geri bildirimlerinin alınmasını sağlamak için kurum çalışanlarının katılımını içermelidir.

|  |  |
| --- | --- |
| **BELGE SINIFLANDIRMASI** | Herkese açık |
| **BELGE REFERANSI** | DOK.05.04 |
| **SÜRÜM** | 1 |
| **TARİH** | 01.05.2024 |
| **DOKÜMAN YAZARI** |  |
| **DOKÜMAN SAHİBİ** |  |

Revizyon geçmişi

|  |  |  |  |
| --- | --- | --- | --- |
| **SÜRÜM** | **TARİH** | **REVIZYON YAZARI** | **DEĞIŞIKLIKLERIN ÖZETI** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Dağıtım

|  |  |
| --- | --- |
| **AD** | **BAŞLIK** |
|  |  |
|  |  |
|  |  |

Onay

|  |  |  |  |
| --- | --- | --- | --- |
| **AD** | **KONUM** | **İMZA** | **TARİH** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

İçerik

[1 Giriş 5](#_Toc163388539)

[2 Bilgi güvenliği politikası 6](#_Toc163388540)

[2.1 Bilgi güvenliği gereksinimleri 6](#_Toc163388541)

[2.2 Hedef belirleme çerçevesi 6](#_Toc163388542)

[2.3 BGYS’nin sürekli iyileştirilmesi 7](#_Toc163388543)

[2.4 Bilgi güvenliği politikası alanları 8](#_Toc163388544)

[2.5 Bilgi güvenliği politikasının uygulanması 10](#_Toc163388545)

# Giriş

Bu belge, Yukato bilgi güvenliği politikasını tanımlar.

Modern, ileriye dönük bir işletme olarak Yukato müşterilerinin, hissedarlarının ve diğer paydaşlarının yararına sorunsuz ve kesintisiz çalışmasını sağlama ihtiyacını üst düzeylerde kabul eder.

Böyle bir sürekli çalışma düzeyi sağlamak için Yukato Uluslararası Bilgi Güvenliği Standardı ISO/IEC 27001, Uluslararası İş Sürekliliği Standartı ISO 22301 ve Uluslararası Bilgi Teknolojileri Hizmet Yönetim Sistemi Standartı ISO 20000-1 ile uyumlu bir Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamıştır. Bu standartlar, uluslararası kabul görmüş en iyi uygulamalara dayalı bir BGYS – İSYS – HYS için gereksinimleri tanımlar.

BGYS'nin işletilmesinin, işletme için aşağıdakiler de dahil olmak üzere birçok faydası vardır:

* Gelir akışlarının ve şirket karlılığının korunması
* Müşterilere mal ve hizmet tedarikinin sağlanması
* Hissedar değerinin korunması ve geliştirilmesi
* Yasal ve düzenleyici gerekliliklere uygunluk

Yukato, en iyi bilgi güvenliği uygulamasının etkin bir şekilde benimsenmesinin bağımsız bir üçüncü taraf olan Akredite Sertifikasyon Kuruluşu tarafından doğrulanabilmesi için ISO/IEC 27001'e göre tam sertifika almaya karar vermiştir. Buna ek olarak, ISO/IEC 27017 ve ISO/IEC 27018 uygulama kodlarında yer alan kılavuz, Bulut Hizmeti Sağlayıcıları (CSP'ler) için özel bir öneme sahip olduğu için benimsenmiştir.

Bu politika, yönetim kurulu üyeleri, yöneticiler, çalışanlar, tedarikçiler ve Yukato sistemlerine erişimi olan diğer üçüncü taraflar dahil olmak üzere kuruluşun bilgi sistemlerini oluşturan tüm sistemler, kişiler ve süreçler için geçerlidir .

Aşağıdaki destekleyici belgeler bu bilgi güvenliği politikasıyla ilgilidir ve nasıl uygulandığı hakkında ek bilgi sağlar:

* *Risk Değerlendirmesi ve İyileştirme Süreci*
* *Uygulanabilirlik Beyanı*
* *Tedarikçi Bilgi Güvenliği Değerlendirme Süreci*
* *İnternet Kabul Edilebilir Kullanım Politikası*
* *Bulut Bilişim Politikası*
* *Mobil Cihaz Politikası*
* *BYOD Politikası*
* *Uzaktan Çalışma Politikası*
* *Erişim Kontrol Politikası*
* *Kullanıcı Erişim Yönetimi Süreci*
* *Şifreleme Politikası*
* *Fiziksel Güvenlik Politikası*
* *Kötü Amaçlı Yazılımdan Koruma Politikası*
* *Yedekleme İlkesi*
* *Günlüğe Kaydetme ve İzleme Politikası*
* *Yazılım Politikası*
* *Teknik Güvenlik Açığı Yönetimi Politikası*
* *Ağ Güvenliği Politikası*
* *Elektronik İleti Politikası*
* *Güvenli Kalkınma Politikası*
* *Tedarikçi İlişkileri için Bilgi Güvenliği Politikası*
* *Kullanılabilirlik Yönetimi Politikası*
* *Fikri Mülkiyet ve Telif Hakları Uyum Politikası*
* *Kayıt Saklama ve Koruma Politikası*
* *Gizlilik ve Kişisel Verilerin Korunması Politikası*
* *Temiz Masa Temiz Ekran Politikası*
* *Sosyal Medya Politikası*
* *İK Güvenlik Politikası*

Bu belgelerin her birinin en son sürüm numarasının ayrıntılarına BGYS Doküman Listesi'nden ulaşılabilir.

# Bilgi güvenliği politikası

## Bilgi güvenliği gereksinimleri

Yukato içindeki bilgi güvenliği gereksinimlerinin net bir tanımı, tüm BGYS faaliyetlerinin bu gereksinimlerin yerine getirilmesine odaklanması için dahili iş ve bulut hizmeti müşterileriyle kararlaştırılacak ve sürdürülecektir. Yasal, düzenleyici ve sözleşmeye dayalı gereklilikler de belgelenecek ve planlama sürecine girilecektir. Yeni veya değiştirilmiş sistemlerin veya hizmetlerin güvenliği ile ilgili özel gereksinimler, her projenin tasarım aşamasının bir parçası olarak ele alınacaktır.

Uygulanan kontrollerin iş ihtiyaçları tarafından yönlendirildiği ve bunun ekip toplantıları ve brifing belgeleri aracılığıyla tüm personele düzenli olarak iletileceği Yukato Bilgi Güvenliği Yönetim Sistemi'nin temel bir ilkesidir.

## Hedef belirleme çerçevesi

Bilgi güvenliği, iş sürekliliği ve hizmet yönetimine yönelik hedeflerin belirlenmesinde, bütçe planlama döngüsüne denk gelecek şekilde düzenli bir döngü kullanılacaktır. Bu, belirlenen iyileştirme faaliyetleri için yeterli finansmanın elde edilmesini sağlayacaktır. Bu hedefler, ilgili tarafların görüşlerinin alınabileceği yönetimin gözden geçirme süreci tarafından bilgilendirilen iş gereksinimlerinin net bir şekilde anlaşılmasına dayanacaktır.

Yönetim sistemi hedefleri, kararlaştırılan bir süre boyunca, bunların nasıl gerçekleştirileceğine ilişkin ayrıntılarla birlikte belgelenecektir. Bunlar, geçerliliklerini koruduklarından emin olmak için yönetim incelemelerinin bir parçası olarak değerlendirilecek ve izlenecektir. Değişiklik yapılması gerekiyorsa, bunlar değişiklik yönetimi süreci aracılığıyla yönetilecektir.

ISO/IEC 27001 uyarınca, standardın Ek A'sında ayrıntıları verilen referans kontrolleri, uygun olduğunda Yukato tarafından benimsenecektir. Bunlar, risk değerlendirmelerinden elde edilen sonuçlar ışığında ve bilgi güvenliği risk tedavi planları doğrultusunda düzenli olarak gözden geçirilecektir. Hangi Ek A kontrollerinin uygulandığı ve hangilerinin hariç tutulduğu hakkında ayrıntılı bilgi için lütfen *Uygulanabilirlik Beyanı'na bakın*.

Buna ek olarak, aşağıdaki uygulama kurallarından geliştirilmiş ve ek kontroller benimsenecek ve uygun olduğunda uygulanacaktır:

* ISO/IEC 27002 – Bilgi güvenliği kontrolleri için uygulama kodu
* ISO/IEC 27017 – Bulut hizmetleri için ISO/IEC 27002'ye dayalı bilgi güvenliği kontrolleri için uygulama kodu
* ISO/IEC 27018 – PII işlemcileri olarak hareket eden genel bulutlarda kişisel olarak tanımlanabilir bilgilerin (PII) korunması için uygulama kodu

Bu uygulama kurallarının benimsenmesi, müşterilerimize ek güvence sağlayacak ve uluslararası veri koruma mevzuatına uyumumuza daha fazla yardımcı olacaktır.

## BGYS’nin sürekli iyileştirilmesi

Yukato sürekli iyileştirme ile ilgili politika:

* BGYS'nin etkinliğini sürekli iyileştirmek
* ISO/IEC 27001 ve ilgili standartlarda tanımlanan iyi uygulamalarla uyumlu hale getirmek için mevcut süreçleri geliştirmek
* ISO/IEC 27001 sertifikasını almak ve sürekliliğini sağlamak
* Bilgi güvenliği ile ilgili proaktiflik düzeyini (ve paydaşların proaktiflik algısını) artırmak
* Bilgiye dayalı kararlar için sağlam bir temel sağlamak amacıyla bilgi güvenliği süreçlerini ve kontrollerini daha ölçülebilir hale getirmek
* Toplanan geçmiş verilere dayanarak bunları değiştirmenin uygun olup olmadığını değerlendirmek için ilgili metrikleri yıllık olarak gözden geçirmek
* Bulut hizmeti müşterileri de dahil olmak üzere ilgili taraflarla düzenli toplantılar ve diğer iletişim biçimleri aracılığıyla iyileştirme fikirleri edinmek
* Zaman çizelgelerini ve faydaları önceliklendirmek ve değerlendirmek için düzenli yönetim toplantılarında iyileştirme fikirlerini gözden geçirmek

İyileştirme fikirleri, çalışanlar, müşteriler, tedarikçiler, BT personeli, risk değerlendirmeleri ve hizmet raporları dahil olmak üzere herhangi bir kaynaktan elde edilebilir. Tanımlandıktan sonra, yönetim incelemelerinin bir parçası olarak kaydedilecek ve değerlendirilecektir.

## Bilgi güvenliği politikası alanları

Yukato, bu kapsamlı bilgi güvenliği politikasına eşlik eden kapsamlı bir politika dokümantasyonu setinde ayrıntılı olarak açıklanan bilgi güvenliği ile ilgili çok çeşitli alanlarda politikayı tanımlar.

Bu politikaların her biri, ilgili alanda yetkinliğe sahip bir veya daha fazla kişi tarafından tanımlanır ve kabul edilir ve resmi olarak onaylandıktan sonra, kuruluşun hem içinde hem de dışında uygun bir kitleye iletilir.

Aşağıdaki tablo, belge kümesindeki tek tek ilkeleri gösterir ve her bir ilkenin içeriğini ve ilgili tarafların hedef kitlesini özetler.

| POLİTİKA BAŞLIĞI | ADRESLENİLEN ALANLAR | HEDEF KİTLE |
| --- | --- | --- |
| İnternet Kabul Edilebilir Kullanım Politikası | İnternet'in iş amaçlı kullanımı, İnternet'in kişisel kullanımı, İnternet hesap yönetimi, güvenlik ve izleme ve İnternet hizmetinin yasaklanmış kullanımları. | İnternet hizmeti kullanıcıları |
| Bulut Bilişim Politikası | Durum tespiti, kayıt, kurulum, yönetim ve bulut bilişim hizmetlerinin kaldırılması. | Bulut hizmetlerinin satın alınması ve yönetiminde yer alan çalışanlar |
| Mobil Cihaz Politikası | Dizüstü bilgisayarlar, tabletler ve akıllı telefonlar gibi mobil cihazların bakımı ve güvenliği, kuruluş tarafından iş kullanımı için sağlanıp sağlanmadığı. | Şirket tarafından sağlanan mobil cihazların kullanıcıları  |
| BYOD Politikası | Personelin kurumsal bilgilere erişmek için kendi mobil cihazlarını kullanmak istediği durumlarda Kendi Cihazını Getir (BYOD) ile ilgili dikkat edilmesi gereken noktalar. | Kısıtlı iş kullanımı için kişisel cihaz kullanıcıları |
| Uzaktan Çalışma Politikası | Bir uzaktan çalışma sahasının kurulması ve işletilmesinde bilgi güvenliği hususları ve düzenlemesi, örneğin fiziksel güvenlik, sigorta ve ekipman | Bir tele-çalışma sahasının kurulması ve sürdürülmesinde yer alan yönetim ve çalışanlar |
| Erişim Kontrol Politikası | Kullanıcı kaydı ve kayıt silme, erişim haklarının sağlanması, dış erişim, erişim gözden geçirmeleri, parola politikası, kullanıcı sorumlulukları ve sistem ve uygulama erişim kontrolü. | Erişim kontrolünün kurulması ve yönetilmesinde yer alan çalışanlar |
| Şifreleme Politikası | Risk değerlendirmesi, teknik seçimi, dağıtımı, kriptografinin test edilmesi ve gözden geçirilmesi ve anahtar yönetimi | Kriptografik teknoloji ve tekniklerin kullanımının kurulması ve yönetilmesinde yer alan çalışanlar |
| Fiziksel Güvenlik Politikası | Güvenli alanlar, kağıt ve ekipman güvenliği ve ekipman yaşam döngüsü yönetimi | Tüm çalışanlar |
| Kötü Amaçlı Yazılımdan Koruma Politikası | Güvenlik duvarları, anti-virüs, spam filtreleme, yazılım yükleme ve tarama, güvenlik açığı yönetimi, kullanıcı farkındalığı eğitimi, tehdit izleme ve uyarılar, teknik incelemeler ve kötü amaçlı yazılım olay yönetimi.  | Kuruluşun altyapısını kötü amaçlı yazılımlardan korumaktan sorumlu çalışanlar |
| Yedekleme İlkesi | Yedekleme döngüleri, bulut yedeklemeleri, tesis dışı depolama, dokümantasyon, kurtarma testi ve depolama ortamının korunması | Yedekleme rejimlerinin tasarlanmasından ve uygulanmasından sorumlu çalışanlar |
| Günlüğe Kaydetme ve İzleme Politikası | Olay toplama ayarları. Koruma ve İnceleme | Kuruluşun altyapısını saldırılardan korumaktan sorumlu çalışanlar |
| Yazılım Politikası | Yazılım satın alma, yazılım kaydı, kurulum ve kaldırma, şirket içi yazılım geliştirme ve bulutta yazılım kullanımı. | Tüm çalışanlar |
| Teknik Güvenlik Açığı Yönetimi Politikası | Güvenlik açığı tanımı, bilgi kaynakları, yamalar ve güncellemeler, güvenlik açığı değerlendirmesi, sağlamlaştırma, farkındalık eğitimi ve güvenlik açığı ifşası. | Kuruluşun altyapısını kötü amaçlı yazılımlardan korumaktan sorumlu çalışanlar |
| Ağ Güvenliği Politikası | Ağ ayrımı, çevre güvenliği, kablosuz ağlar ve uzaktan erişim dahil olmak üzere ağ güvenliği tasarımı; Roller ve sorumluluklar, günlüğe kaydetme ve izleme ve değişiklikler dahil olmak üzere ağ güvenliği yönetimi. | Ağların tasarlanmasından, uygulanmasından ve yönetilmesinden sorumlu çalışanlar |
| Elektronik İleti Politikası | Elektronik mesaj gönderme ve alma, elektronik mesajlaşma olanaklarının izlenmesi ve e-posta kullanımı. | Elektronik mesajlaşma olanaklarının kullanıcıları |
| Güvenli Kalkınma Politikası | İş gereksinimleri belirleme, sistem tasarımı, geliştirme ve test etme ve dış kaynaklı yazılım geliştirme. | Ismarlama yazılım geliştirmeleri için kod tasarlamaktan, yönetmekten ve yazmaktan sorumlu çalışanlar |
| Tedarikçi İlişkileri için Bilgi Güvenliği Politikası | Durum tespiti, tedarikçi sözleşmeleri, hizmetlerin izlenmesi ve gözden geçirilmesi, değişiklikler, anlaşmazlıklar ve sözleşmenin sona ermesi. | Tedarikçi ilişkilerinin kurulması ve yönetilmesinde yer alan çalışanlar |
| Kullanılabilirlik Yönetimi Politikası | Kullanılabilirlik gereksinimleri ve tasarımı, izleme ve raporlama, kullanılabilirlik olmaması, kullanılabilirlik planlarını test etme ve değişiklikleri yönetme. | Sistemlerin tasarlanmasından ve hizmet sunumunun yönetilmesinden sorumlu çalışanlar |
| Fikri Mülkiyet ve Telif Hakları Uyum Politikası | Fikri mülkiyetin, yasaların, cezaların ve yazılım lisansı uyumluluğunun korunması. | Tüm çalışanlar |
| Kayıt Saklama ve Koruma Politikası | Belirli kayıt türleri için saklama süresi, kriptografi kullanımı, ortam seçimi, kayıt alma, imha etme ve gözden geçirme. | Kayıtların oluşturulmasından ve yönetiminden sorumlu çalışanlar |
| Gizlilik ve Kişisel Verilerin Korunması Politikası | Uygulanabilir veri koruma mevzuatı, tanımlar ve gereklilikler.  | Kişisel verileri kullanarak sistemleri tasarlamaktan ve yönetmekten sorumlu çalışanlar |
| Clear Desk ve Clear Screen Politikası | Ekranlarda gösterilen, çıktısı alınan ve çıkarılabilir ortamlarda tutulan bilgilerin güvenliği. | Tüm çalışanlar |
| Sosyal Medya Politikası | Kuruluşu temsil ederken ve kuruluşla ilgili konuları tartışırken sosyal medyanın nasıl kullanılması gerektiğine ilişkin yönergeler. | Tüm çalışanlar |
| İK Güvenlik Politikası | İşe alım, iş sözleşmeleri, politikaya uyum, disiplin süreci, fesih | Tüm çalışanlar |
| Kabul Edilebilir Kullanım Politikası | Çalışanların kurumsal bilgi güvenliği politikalarına bağlılığı. | Tüm çalışanlar |
| Varlık Yönetimi Politikası | Bu belge, varlıkların bilgi güvenliği perspektifinden nasıl yönetilmesi gerektiğine ilişkin kuralları ortaya koymaktadır. | Tüm çalışanlar |

Tablo 1: Politikalar

## Bilgi güvenliği politikasının uygulanması

Bu belgede ve Tablo 1'de listelenen destekleyici politikalar kümesinde yapılan politika beyanları, Yukato üst yönetimi tarafından gözden geçirilmiş ve onaylanmıştır ve bunlara uyulmalıdır. Bir çalışanın bu politikalara uymaması, kuruluşun Çalışan Disiplin Sürecine uygun olarak disiplin cezası alınmasına neden olabilir.

Herhangi bir Yukato politikasıyla ilgili sorular, ilk etapta çalışanın en yakın bölüm yöneticisine yöneltilmelidir.