Rev.1- 2023

BİLGİ GÜVENLİĞİ EL KİTABI 2023

BİLGİ GÜVENLİĞİ SENİN SORUMLULUĞUNDUR…

İçindekiler

BİLGİ GÜVENLİĞİ POLİTİKASI

Amaç

Bu el kitabı; Bilgi Güvenliğinin ne olduğunu ve Arnavutköy Belediyesi'nin bilgi güvenliğine yaklaşımını anlatan politikayı içerir. Arnavutköy Belediyesi; bilgi kaynaklarını kullanan tüm kullanıcılarına, ilişki içinde olduğu üçüncü taraflara, tedarikçilerine bu politikayı duyuracaktır.

Aynı zamanda Arnavutköy Belediyesi bu politikayla; Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmaktaki amacını, hedeflerini, sistemi nasıl kuracağını, uygulayacağını, izleyeceğini ve raporlayacağını açıklar.

Bu politika; BGYS kapsamı içerisinde kalan tüm sistem ve lokasyonlardaki faaliyetler sırasında uygulanacak Bilgi Güvenliği gereklerini belirler. Arnavutköy Belediyesi'nde kurulan ISO/IEC 27001 standardı uyumlu Bilgi Güvenliği Yönetim Sisteminin kapsamı ise; BGYS.K.01-Bilgi Güvenliği Kapsamı dokümanında belirlenmiştir.

Bilgi Güvenliği

Bilgi güvenliği, bilgi ve bilgiyi kaydeden, erişime vasıta olan, depolayan varlıkların tümünün izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa etme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik unsurundan herhangi biri zarar görürse güvenlik zafiyeti oluşur.

Gizlilik: Bilginin yetkisiz kişilerin eline geçmeme ve yetkisiz erişime karşı korunmasıdır.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

Erişilebilirlik (kullanılabilirlik): Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

BGYS (Bilgi Güvenliği Yönetim Sistemi); kurum kuruluş ve şirketlerin faaliyetleri sürecinde ürettikleri, topladıkları, işledikleri, sakladıkları ve ilettikleri her tür bilginin güvenliğini, bütünlüğünü sağlayan ve gerektiğinde yetkili kişilerin bilgiye kolay hızlı ve doğru biçimde ulaşmasına imkân veren bir sistemdir. Uluslararası ISO/IEC 27001 standardı ile kurallar bütünü haline getirilmiştir.

Arnavutköy Belediyesini doğrudan BGYS kurmaya zorlayan bir yasal düzenleme olmamakla birlikte Üst Yönetim mevcut olan bazı kanunlar, yönetmelikler, stratejiler, eylem planları vb. gereklilikleri yerine getirmek için sistematik bir şekilde BGYS kurulmasını sağlamıştır.

Bilgi Güvenliği yönetimi için izlenen uluslararası standart ISO/IEC 27001'dir. Arnavutköy Belediyesi bu El Kitabı'nda; Kurum olarak tanımlanacaktır.

Yönetimin Taahhüdü

Arnavutköy Belediye Başkanlığı Üst yönetimi, Bilgi Güvenliğine ve bilgi varlıklarına yönelik her türlü riski yönetmek amacıyla;

- Kurumsal bilgileri, personel özlük bilgilerini, vatandaş/mükellef ve tedarikçi bilgilerini (finansal veriler, kişi bilgileri) değerli ve kritik kabul etmekte ve bilgi güvenliği ile ilgili yasaların getirdiği zorunlulukları yerine getirmeyi,

- Kurumsal faaliyetlerinin gerçekleşmesinde kullanılan bilişim hizmetlerinin kesintisiz devam etmesi, kişisel ve özel verilere sadece yetkili kişilerce erişilebilmesi amacıyla gerekli alt yapıyı sağlamayı ve gerekli güvenlik tedbirlerini almayı,
- Bilgi Güvenliği Yönetim Sitemi, ISO/IEC 27001 standardının gereklerini yerine getirecek şekilde dokümante etmeyi ve sürekli iyileştirmeyi,
- Bilgi Güvenliği yönetiminin etkinliğinin sağlanması için kişileri yönlendirmeyi desteklemeyi,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuat ve sözleşmelere uymayı,
- Bilgi Varlıklarına yönelik riskleri sistematik olarak yönetmeyi,
- Bilgi Güvenliği farkındalığını arttırmak amacıyla teknik ve davranışsal yetkinlikleri geliştirecek eğitimleri gerçekleştirmeyi,
- BGYS'yi; uyguladığı diğer yönetim sistemleri ile birlikte bütünleşik bir şekilde yöneterek, yerel yönetimler alanında bilgi güvenliği açısından öncülüğü ile örnek bir kurum olmak için tüm gücüyle çalışmayı taahhüt etmektedir.

BGYS'nin Amaçları ve Hedefleri

Arnavutköy Belediyesi bünyesinde bir BGYS'nin kurulmasıyla, Tüm belediyecilik faaliyetlerinin, bilgi varlıklarının ve bu varlıkları korumak amacıyla kullanılan tüm idari bina ve tesislerin güvenliğini sağlamak ve uygun bir biçimde yönetilmesi amaçlanır. Ayrıca onaylanmış bir BGYS sisteminin bulunması, mevzuattan doğan birçok yükümlülüğün yerine getirilmesine de yardımcı olacaktır.

Bu bağlamda, Bilgi Güvenliği Yönetim Sistemi hedefleri, şu temel maddeler olarak belirlenmiştir;

- Yönetim Sisteminin ISO27001 standardına uygun olarak kalitesini arttırmak, sürekliliğini sağlamak
- Çalışanların BGYS farkındalığını arttırmak,
- BGYS süreçlerine ilişkin yeterlilik ve yetkinliği arttırmak,
- BGYS maliyetlerini belirlemek ve gerekmesi durumunda bütçe kalemlerini oluşturup kurum bütçesine dahil etmek.
- BGYS risklerini kabul edilebilir seviyelere düşürmek,

BGYS nin amaçları ve hedefleri; BGYS.K.01–Bilgi Güvenliği Kapsamında anlatılmış, bu hedeflere ulaşmak için izlenecek yol, yapılacak kontroller ve ölçüm metodları **hedef takip listesinde** detaylandırılmıştır. Bu liste üzerinden takip edilecektir.

Risk Yönetimi

Arnavutköy Belediyesi; Bilgi Güvenliği Yönetim Sisteminin amaçlanan çıktılarının sağlanması, istenmeyen etkilerin önlenmesi veya azaltılması için, varlıklarına yönelik Bilgi güvenliği risklerini belirler ve analiz eder. Risk yönetiminden çıkan uygunsuzlukların doğru değerlendirilerek bir iyileştirme fırsatına dönüştürülmesi için gerekli faaliyetleri tanımlar ve bu faaliyetleri BGYS süreçleri ile bütünleştirerek planlar ve gerçekleştirilmesini sağlar.

Risk işleme, değerlendirme ve önlemlerinin alınması için uygulanacak metot BGYS.PR.03-Risk Yönetim Prosedüründe detayları ile anlatılır.

Bilgi Güvenliğinin Çerçevesi

Arnavutköy belediyesinde uygulanacak olan BGYS Kurumun bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes için;

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kurum bilgilerinin gizliliğini korur
- Bilgi kritiklik seviyesine göre yedeklenir
- Risk düzeylerine göre güvenlik önlemleri alınır
- Bilgi güvenliği ihlalleri raporlanır ve gereken tüm aksiyonlar alınır.
- Kurum içi bilgi kaynakları bağlı bulunduğu mevzuatta veya yaptığı sözleşmelerde açıkça belirlenen haller dışında üçüncü kişilerle hiçbir surette paylaşılmaz

- Kurum bilişim kaynakları T.C. yasalarına, bunlara bağlı kanun ve yönetmeliklere aykırı faaliyetler amacı ile kullanılamaz

Bilgi güvenliği gereklerinin yerine getirilmesi çerçevesinde, kurumun bağlantılı olduğu iç ve dış hususlar, yasal gereklilikler, tarafların ihtiyaç ve beklentileri BGYS.K.01-Bilgi Güvenliği Kapsamı dokümanında detaylarıyla anlatılmıştır.

Kaynakların temini

Arnavutköy Belediyesi; kurumun amacına ve hedeflerine bağlı olarak Bilgi güvenliği gereklerini yerine getirmek ve planladığı hedeflere ulaşmak için gerekli insan, finansal, zaman, altyapı kaynaklarını bağlı bulunduğu mevzuat çerçevesinde tedarik edecektir. BGYS için gerekli kaynakları temin etme süreci BGYS Yönetim Komitesi tarafından yürütülerek kontrol edilecektir.

Roller ve sorumluluklar

Arnavutköy Belediyesi'nde sistemin kurulması, uygulanması, sürdürülmesi, izlenmesi ve sürekli olarak iyileştirilmesi ve işletilmesinin sağlanması için roller ve sorumluluklar belirlenerek, BGYS Yönetim ve Yürütme Komiteleri oluşturulmuştur.

Bu bağlamda, BGYS sürecinde karar ve onay aşamalarını gerçekleştirecek, gerekli işgücü ve bütçeyi sağlayacak olan Yönetim Komitesi'nin üyeleri; Kurum Başkanı, Başkan Yardımcıları, Yönetim Temsilcisidir. Alınan kararların yürütülmesi, sürdürülmesi, izlenmesi ve bilgi güvenliği konusunda muhtemel riskleri belirleyerek alınması gereken önlemlerle ilgili Bilgi Güvenliği Yönetim Komitesine seçenekler sunacak Yürütme Komitesinin üyeleri; Yönetim Temsilcisi, BGYS Sorumlusu ve kapsam dâhilindeki müdürlüklerde belirlenen ekiplerdir.

BGYS organizasyonu, belirlenen roller, rollerin görev, yetki ve yetkinlikleri BGYS.OD.01-Roller ve Sorumluluklar dokümanında anlatılmıştır.

Bilgi Güvenliği Yönetim Sisteminin Yürütülmesi ve Kullanıcı Sorumluluğu

Arnavutköy Belediyesi, BGYS yi kurarken ve yönetirken yapması gereken gereklilikleri iş süreçlerine uygun olarak yazılı prosedürler haline getirmiştir. Dokümante ettiği tüm politika ve prosedürlerini BGYS.PR.01-Dokümanların Kontrolü Prosedüründe tarif edildiği şekilde oluşturur, onaylar, yayınlar, gözden geçirir ve revize eder.

Bilişim sistemlerine erişim ile ilgili standardın belirlediği Mobil cihaz kullanımı, internet, parola, temiz masa temiz ekran uygulamaları ve kontrolleri, ilgili politika ve prosedürlere göre yapılacaktır.

İş sürekliliği ve Acil Durum Planları, Veri Yedekleme, Virüs ve saldırganlardan korunma, fiziksel ve çevresel güvenlik, sistem temini ve bakım gerekleri, haberleşme ve ağ güvenliği, erişim kontrolleri prosedürleri bu politikayı destekler. Bu alanlarla ilgili işleyiş özel olarak dokümante edilmiş politika ve prosedürlerle tanımlanır.

BGYS'de planlanan hedeflerin izlenmesi, ölçülmesi ve değerlendirilmesi BGYS Yönetim Temsilcisi, BGYS Sorumlusu, BGYS Müdürlük Ekipleri tarafından yapılır. İç kontroller ise yılda en az bir defa iç tetkik yapmaya yetkin personel tarafından BGYS.PR.04-İç Tetkik Prosedürü'nde anlatıldığı şekilde yapılacaktır. Üst Yönetim bilgi Güvenliği Yönetim Sisteminin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek için planlı aralıklarla gözden geçirecektir.

Arnavutköy Belediyesi; tedarikçiler vasıtası ile aldığı hizmetin kesintisiz ve kaliteli olarak sağlanmasını güvence altına almak ve isteklilerine iş yaptırma/ihalelere girme bariyeri koyma hususunda Bilgi Güvenliği/İdare Memnuniyetini bir tercih unsuru olarak görmektedir. Bu hususu kendi çalışanlarına, isteklilerine ve yüklenici/ tedarikçilerine açıkça deklare etmektedir. Bu bağlamda Kurum, tedarikçiler/yüklenicileri ile BGYS.PL.08-Tedarikçi İlişkileri Yönetim Politikası çerçevesinde çalışacaktır.

Arnavutköy Belediyesi ISO/IEC 27001 uyumluluğu kapsamında, teknik gerekliliklerin yerine getirilmesinin yanı sıra BGYS organizasyonunda tanımlanan tüm rollerdeki personelin uygun öğrenim, eğitim, beceri ve deneyime sahip olması ve çalışanların görevlerini etkin bir şekilde yerine getirmesinin sağlaması için genel eğitim stratejisi geliştirmiştir. BGYS nin yürütülmesinde ve izlenmesinde görevli personele gerekli iç tetkikçi, baş denetçi eğitimleri aldıracak, son kullanıcı farkındalık eğitimleri düzenleyecektir.

Sürdürülebilir bir BGYS için bütün çalışanların katılım ve farkındalığı önemlidir. Personelin bilgi güvenliği farkındalığını yüksek tutmak için e-posta, SMS mesajları gönderilecek, mümkün olduğu sürece belediye yerleşkelerinde bilgi güvenliğini sağlamayı, ihlal olaylarını bildirmeye teşvik edici afiş, posterler asılacak, broşürler dağıtılacaktır.

Arnavutköy Belediyesi bilgi ve bilgi işleme olanaklarına erişim sağlayabilen tüm personel, Kurumun Bilgi Güvenliği Politikasını ve bu politikada atıf yapılan politika, prosedür ve talimatları bilmekle ve kurum varlıklarını kullanırken belirlenen kurallara uygun hareket etmekle yükümlüdürler. Bu yükümlülük tüm kullanıcılarla (Üst Yönetim dahil bütün personel, memur, işçi, sözleşmeli, hizmet alımı personeli, tedarikçi firma çalışanı ve üçüncü taraflar) yapılan taahhütname ile güvence altına alınacaktır. Varlıkların kullanımında uyulması gereken kurallar BGYS.PL.02-Varlıkların Kabul Edilebilir Kullanımı Politikasında detaylı olarak anlatılmıştır.

Bilgi Güvenliği gereklerinin yerine getirilmediği, politika ve prosedürlerin ihlal edildiği durumlarda disiplin süreci işletilecektir. Güvenlik ihlali gerçekleştirdiği kesinleşen personel için bağlı bulunduğu mevzuat çerçevesinde;

- Uyarı,
- İhtar,
- Para cezası,
- Geçici uzaklaştırma,
- Kesin uzaklaştırma,
- Tazminat davası açma,
- Açılan tazminat davalarının sonuçlarının rücu edilmesi,
- Cezalarının birinin veya birden fazlasının uygulanması yaptırımları uygulanabilecektir.

Sürdürülebilirliği sağlamak için bilgi güvenliği ihlalleri BGYS.PR.18-Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü'nde anlatıldığı metotla kayıt altına alınacak, kayıt altına alınan Bilgi Güvenliği ihlallerine bağlı olarak BGYS.PR.05-Düzeltici ve İyileştirici Faaliyet Prosedürü'nde anlatıldığı şekilde düzeltici-iyileştirici faaliyet planlanarak takip edilecektir. Bu faaliyetlerle BGYS'de sürekli iyileştirme amaçlanır.

BİLGİ GÜVENLİĞİ KAPSAMI

Amaç

Bu metnin amacı; Arnavutköy Belediyesi'nin Bilgi Güvenliği Yönetim Sisteminin kapsam ve sınırlarını organizasyon, yerleşkeler ve altyapı bazında tanımlamaktır. Aynı zamanda bu doküman, kurumun bağlamını, genel yapısını, ilgili tarafların beklentilerini tanımlar.

BGYS Kapsamı, kurulacak sistemlerin değerlendirileceği ve uygun biçimde ele alınacağı alanı ifade eder. Onaylanmasından üst yönetim sorumludur. Kapsam ve sınır ifadelerindeki değişiklikler üst yönetim tarafından gözden geçirilir.

Teknolojik ve yasal değişiklikler ve iş fırsatları sonucu kurumun yapısı zaman içinde değişikliğe uğrayacağından bu doküman her yıl ve majör değişikliklerden sonra (bina, proses değişiklikleri vs.) gözden geçirilecek ve bu değişikliklerin etkilerini karşılamak için BGYS güncellenecektir.

Kapsam

Bu metin, etkin bir yönetim sistemi kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve sürekli iyileştirmek için Arnavutköy Belediyesi sistemlerinin amaçlarını etkileyebilecek iç/dış hususları ve ilgili tarafların ihtiyaç ve beklentilerinin anlaşılması analizlerini kapsamaktadır.

Arnavutköy Belediyesi Bağlamının Anlaşılması

Arnavutköy Belediyesi 1987 yılında kurulmuştur. 2004 yılına kadar Gaziosmanpaşa İlçesi sınırları içinde "belde belediyesi" statüsünde olan Arnavutköy; 5216 sayılı Büyükşehir Belediyesi Kanunu'nun 23 Temmuz 2004 tarihinde "ilk kademe belediyesi" statüsünü almış ve İstanbul Büyükşehir Belediyesi ile organik açıdan ilişkilendirilmiştir. 5747 sayılı Büyükşehir Belediyesi Sınırları İçinde İlçe Kurulması ve Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun ile 22 Mart 2008 tarihinde İlçe Belediyesi statüsü kazanmıştır.

Arnavutköy Belediyesi'nin görevleri, hak, yetki ve imtiyazları 5393 sayılı Belediye Kanunu'nun 14 ve 15. maddelerinde açıklanmıştır.

Organizasyon yapısı

Arnavutköy Belediyesi idarî teşkilatı bir bütün olarak Başkana bağlıdır. Arnavutköy Belediyesi'nde 5 kademeli bir teşkilat yapısı vardır. Bu yapıda, başkan, 5 tane başkan yardımcısı ve 24 müdürlük, 1 Uzmanlık bulunmaktadır.

BELEDİYE BAŞKANI

↓

BAŞKAN YARDIMCILARI

↓

MÜDÜRLER

↓

ŞEFLER

↓

MEMURLAR-SÖZLEŞMELİ PERSONEL-İŞÇİLER

Şekil 2: Arnavutköy Belediyesi'nde Hiyerarşik Kademeler

Arnavutköy Belediyesi; 9 Hizmet Binası, 10 Kültür ve Sanat Merkezi 11 Sosyal Hizmet Alanı, 7 Eğitim ve Gençlik Merkezi, 8 Kütüphane, 8 lokasyonda Spor Kompleksi ve Statlar, 2 iştirak şirketi (ARAŞ A.Ş ve PERAŞ A.Ş), 2022 yılı itibariyle 1406 çalışanı ile hizmet vermektedir.

Arnavutköy Belediyesinin Amaçları ve Hedefleri

Amaçları

Belde sakinlerinin mahallî müşterek nitelikteki ihtiyaçlarını karşılamak, beldede ekonomi ve ticaretin geliştirilmesi ve kayıt altına alınmasını sağlamak, hızlı, etkin ve kaliteli hizmet sunmak için "Kurumsal mükemmeliyeti oluşturmak" Yarının İstanbul'unu, bugünün Arnavutköy'nde inşa etmek.(vizyon)

Hedefleri

Teknolojik ve fiziksel altyapıyı geliştirmek, sosyal imkânları iyileştirmek" ve "Kuruluş imajını güçlendirmek, etkinliği ve görünürlüğü artırmak" Çalışanlarına, sürekli iyileştirmeyi teşvik etmeye yönelik eğitim sağlamak. Arnavutköy Belediyesi stratejik planındaki hedeflere ulaşmak için çalışanlarının kurumsal ciddiyetini canlı tutacak farkındalığını arttırmak, becerilerini ve kabiliyetlerini desteklemek. **"Hizmetlerini, yarının İstanbul'unun ihtiyaçlarına hitap edecek bir perspektifle sunmak"(misyon)**

BGYS Amaçları

Arnavutköy Belediyesi; bünyesinde barındırdığı tüm bilgi valıklarının güvenliğini sağlama ve yönetilmesi amacı doğrultusunda; Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesini benimsemiştir ve mevcut kurumsal sistemlerini bilgi güvenliği yönetim sistemi ile ilişkilendirmeyi, desteklemeyi, kurumsal BGYS' sini ISO/IEC 27001:2013 standartlarına uygun olarak yürütmeyi amaçlamaktadır.

Arnavutköy Belediyesi'nde BGYS kurulması projelendirilirken aşağıda belirtilen maddeler amaçlanmıştır.

- Kurumsal bilgilerinin güvenliğini sağlamak
- Çalışan özlük bilgilerinin güvenliğini sağlamak
- Vatandaş/mükellef bilgilerinin güvenliğini sağlamak
- Hizmet veren sistemlerin sürekli erişilebilir olmasını sağlamak
- Erişim kayıtlarını tutarak suç niteliğinde olabilecek erişimlerin delillerini yasal otoritelere sağlamak
- Sistemlerde kayıtlı üçüncü taraf gerçek-tüzel kişilerin ve Kurum çalışan bilgilerinin yetkisiz kişilerin eline geçmesini engellemek
- Veri bütünlüğünü sağlamak
- Erişim seviyelerini belirlemek
- Yedekleme ve kurtarma stratejisi belirlemek
- Kurum riskleri ve teknik açıklıkları yönetmek
- Bilgi varlıklarını yönetmek
- Bilgi varlıkları üzerinde kullanıcı sorumluluklarını belirlemek
- Fiziksel ve çevresel güvenliği sağlamak
- Tedarikçi ilişkilerinde bilgi güvenliğini sağlamak.

BGYS Hedefleri

Bu amaç bağlamında Bilgi Güvenliği Yönetim Sistemi hedefleri Arnavutköy Belediyesi tarafından şu ana maddeler olarak belirlenmiştir;

- Yönetim Sisteminin ISO27001 satandardına uygun olarak kalitesini arttırmak, sürekliliğini sağlamak
- Çalışanların BGYS farkındalığını arttırmak,
- BGYS süreçlerine ilişkin yeterlilik ve yetkinliği arttırmak,
- BGYS maliyetlerini belirlemek ve gerekmesi durumunda bütçe kalemlerini oluşturup kurum bütçesine dahil etmek,
- BGYS risklerini kabul edilebilir seviyelere düşürmek,

Bilgi Güvenliği Yönetim Sistemi'nin yukarıda belirtilen hedeflerine ulaşmak için, **Ölçüm Yapılacak Kontroller ve Ölçüm Metodu** sayısal ölçeklere bağlanarak detaylandırılmış, BGYS.LS.04-Hedef Takip Listesinde kayıt altına alınmıştır. BGYS Yönetim Temsilcisi ve BGYS Sorumlusu tarafından izlenmektedir.

Listenin güncellenmesinden ve hedeflerin gerçekleşme durumlarının liste üzerinden izlenmesinden BGYS Yönetim Temsilcisi sorumludur. BGYS Yönetim Temsilcisi hedeflerin gerçekleştirilme oranlarına göre takip listesinde ilgili değerleri oluşturur. Hedefler YGG toplantılarında değerlendirilir.

Genel olarak tüm hedeflerin belirlenen başarı hedeflerine ulaşması beklenmektedir. Hedefin ulaşılamadığı durumlarda ulaşılamayan hedefler incelenerek gerekli aksiyonlar alınır.

Hedeflerin kabul edilebilir Başarı oranları Hedef Takip Listesinde verilmiştir. Bu listedeki değerlere ulaşıldığında hedefler başarılmış kabul edilir.

Yasal Gereklilikler

Kurumun BGYS ile ilgili hedeflenen çıktılarına ulaşmasında etkisi olabilecek yasal gereklilikler aşağıda verilmiştir.

Kurumu doğrudan BGYS kurmaya zorlayan bir yasal düzenleme olmamakla birlikte mevcut olan bazı kanunlar, yönetmelikler, stratejiler, eylem planları vb. gerekliliklerini yerine getirmek için BGYS kurulması, sistematik bir şekilde yönetim sağlayacaktır.

1. **TCK (Bilişim Suçları)**

   - Madde 243- Bilişim sistemine girme (Yetkisiz erişim)
   - Madde 244-Sistemi engelleme, bozma, verileri yok etme veya değiştirme (Hacking)
   - Madde 245-Banka veya kredi kartlarının kötüye kullanılması
   - Madde 246-Tüzel kişiler hakkında güvenlik tedbiri uygulanması

2. **TCK (Bilişim Vasıtalı Suçlar)**

   - Madde 124-Haberleşmenin engellenmesi
   - Madde 125-Hakaret
   - Madde 132-Haberleşmenin gizliliğini ihlal
   - Madde 133-Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması
   - Madde 135-Kişisel verilerin kaydedilmesi
   - Madde 136-Verileri hukuka aykırı olarak verme veya ele geçirme
   - Madde 138-Verileri yok etmeme
   - Madde 226-Müstehcenlik

3. **Fikir ve Sanat Eserleri Kanunu**

   - Madde 71- B) Ceza davaları: I – Suçlar: 1. Manevi, mali veya bağlantılı haklara tecavüz
   - Madde 72 – Teknolojik önlemleri etkisiz kılma

4. **Ceza Muhakemesi Kanunu**

   - Madde 134- Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma

5. **5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanununun, İçerik Sağlayıcının Sorumluluğu, Yer Sağlayıcının Yükümlülükleri, Toplu Kullanım Sağlayıcıların Yükümlülükleri**
6. **6698 Sayılı Kişisel Verilerin Korunması Kanunu**

Yukarıda sayılan kanun ve kanun maddeleri ve bunlara bağlı yönetmelik, genelge vs… Kurumun bağlı bulunduğu yükümlülüklerdir. BGYS kanunlarda geçen ve Kurumu ilgilendiren maddeler hakkında kontroller sağlanmasını şart koşmaktadır. Kanunda geçen bu maddelerin gereğinin sistematik bir şekilde sağlanması ve takip edilmesi için BGYS Kuruma katkı sağlayacaktır.

** Yükümlü olduğumuz diğer mevzuatların listesi BGYS.FR.01 Dış Kaynaklı Doküman Listesinde ve BGYS.PR.20 Yasal Gereksinimlere Uyum Ve Kontrol Prosedürü İçerisinde belirtilmiştir.

İlgili Tarafların İhtiyaç ve Beklentilerinin Anlaşılması

Kurumun BGYS ile ilgili tarafları iç ve dış taraflar olmak üzere iki başlık altında ele alınmıştır. Belirlenen iç ve dış taraflar aşağıda verilmiştir.

İç Taraflar

a. Personel (Çalışanlar)
b. Yerine getirilecek politikalar, hedefler ve stratejiler,
c. Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
d. Kurum kültürü,
e. Bilgi sistemleri, bilgi akışı ve karar alma süreçleri (resmi ve gayrı resmî),
f. Kurum tarafından uyarlanan standartlar, kılavuzlar, modeller ve Sözleşmeye ilişkin ilişkilerin biçim ve genişliği.

Dış Taraflar

a. Gerçek-tüzel kişiler
b. Altyapı Sağlayıcı Şirketler (Telekomünikasyon, elektrik, su, doğalgaz vb.)
c. Yasa Koyucular
d. Belediye iştirak şirketi ve Yükleniciler (taşeronlar)
e. Tedarikçiler, Vatandaşlar ve Mükellefler

İlgili Tarafların İhtiyaç ve Beklentileri

İlgili Taraflar / **Beklentiler**	Personel (Çalışanlar)	Gerçek-tüzel kişiler	Altyapı Sağlayıcı Şirketler	Yasa Koyucular	Yükleniciler	Tedarikçiler, Vatandaşlar ve Mükellefler
Personel özlük bilgilerinin	**X**					

güvenliğinin sağlanması						
Elektronik ortamda sunulan hizmetlerin sürekliliğinin sağlanması		X			X	X
Firma bilgilerinin güvenliğinin sağlanması		X		X	X	X
Vatandaş bilgilerinin güvenliğinin sağlanması		X		X		X
Belge ve kayıtların güvenliğinin sağlanması	X	X		X	X	X
Şirketlerin mali bilgilerinin güvenliğinin sağlanması		X		X	X	X
Veri transferi ortamlarının güvenliğinin sağlanması	X	X		X	X	X
Servisler arasındaki bağlantının güvenli bağlantı olmasının sağlanması	X			X	X	
Bilgi varlıklarının güvenliğinin sağlanması	X			X		
Bilgi güvenliğinin sağlanması için uyulması gereken politika ve prosedürlerin sağlanması	X	X	X	X	X	X

Kurum bilgi varlıkları envanteri ayrıca tutulmakta ve bilgi güvenliği riskleri bu varlıklarla ilişkilendirilmektedir.

Bilgi Güvenliği Yönetim Sisteminin Kapsamı

Arnavutköy Belediyesi ve ilgililerin beklentileri göz önünde bulundurulduğunda; BGYS organizasyon, yerleşkeler ve altyapı bazında kurumun tüm varlıklarını kapsamaktadır.

Hariç Tutmalar

Kurum iştiraki olarak çalışan şirket/şirketlerin lokasyonları, bu şirket/şirketlerin çalışmaları ile Arnavutköy Belediyesi bilgi varlıkları ile ilişkili olmayan varlıkları kapsama dahil edilmemektedir.

Bu doküman; her yıl Yönetimi Gözden Geçirme Toplantılarında gözden geçirilecek, organizasyonda bir değişiklik olması halinde yeniden yayınlanacaktır.

VARLIKLARIN KABUL EDİLEBİLİR KULLANIM POLİTİKASI

Amaç

Bu politika; Arnavutköy Belediyesi personelinin ve 3. tarafların kurum varlıklarını kullanırken uyması gereken kuralları tanımlamak amacıyla oluşturulmuştur.

Kapsam

Bu doküman Arnavutköy Belediyesi Bilgi Güvenliği Kapsamı dokümanında belirtilen tüm personeli, geçici görevliler ve Kurumun bilgi varlıklarına erişimine izin verilmiş olan diğer Kurum/kuruluş/şirket çalışanları (üçüncü taraf) bu politika ile belirtilen kurallara uymak zorundadır.

Genel kurallar

1. Kurum bilgi ve haberleşme sistemleri ve donanımların (İnternet, e-posta, telefon, çağrı cihazları, telsiz, faks, bilgisayarlar, tabletler, mobil cihazlar ve cep telefonları da dâhil olmak üzere) kullanımı sadece Kurum hizmet alanı ve ilgili amaçlar doğrultusunda olmalıdır. Bilişim kaynakları sadece Kurum için yapılan çalışmalar ve Kurumun onayladığı alanlarda kullanılabilir. Bu sistemlerin yasa dışı, rahatsız edici, Kurumun diğer politika, standart ve rehberlerine aykırı veya Kuruma zarar verecek herhangi bir şekilde kullanımı bu politikanın ihlal edildiği anlamına gelir.
2. İş süreçlerini engellemeyecek düzeyde ve Bilgi Güvenliği Politikasını ve prosedürlerini ihlal etmeyen kişisel kullanımlar kabul edilebilir kapsamda değerlendirilir.
3. Kullanıcılar Bilişim kaynaklarını aşağıdaki durumlar için kullanamaz:
   - Yetkisiz erişim
   - Diğer kullanıcılara ait varlıklara kasıtlı yetkisiz erişim ve ziyan
   - Diğer kullanıcılara ait varlıkların yetkisiz kullanımı
   - Bilişim kaynaklarında yer alan varlıkların izinsiz (yetkisiz) kopyalama ve kullanımı.
   - Bilgisayar iletişim imkânlarını kasten gereksiz olarak kullanarak, diğer kullanıcıların bilişim faaliyetlerini engelleme. (Rastgele etkileşimli elektronik iletişim veya e-posta değişimi başlatmak, etkileşimli ağ olanaklarının aşırı kullanımı vb.)
   - Arnavutköy Belediyesi'nin kritik bilgisinin ortaya çıkmasını veya Kurum servislerini ulaşılamaz hale getirme.
   - Kurum faaliyetleri ile ilişkisi olmayan, özel iş veya eğlence amacıyla kullanmak.

- Kuruma ait bilgi işlem sistemlerine şifreleme ve parola mekanizmalarını kırmaya yönelik program ve araçları yüklemek ve kullanmak.
- Kuruma ait bilgi sistemleri üzerinde, Kurum bilgisi ve izni olmadan değişiklik, yükseltme, genişletme yapmak.
- Kurum gizli varlıklarına yetkisiz erişim yapmak.
- İşle ilgili olmayan veya telif hakları ile korunan dosyaları (ör. müzik, film, kitap dosyaları, vb.) Kurum bilgisayarlarına ve bilgi sistemlerine indirmek, depolamak, çoğaltmak ve paylaşıma açmak.

4. Kullanıcılar Kurum tarafından kendilerine sağlanmış olan program lisans bilgilerini sadece Kurum faaliyetleri doğrultusunda kullanabilir.
5. USB Disk, CD-ROM gibi taşınabilir cihazlarda Kuruma Özel veya Gizli bilgi yedeklenmesi ve bulundurulması esas olarak kabul edilmemektedir. Zorunlu durumlarda uyulması gereken esaslar "Mobil Cihaz Kullanımı Politikasında belirtilmiştir. Diğer taşınabilir ortamlar için "Mobil Cihaz Kullanımı Politikası" nda belirtilen kurallara uyulmalıdır.
6. Herkese açık sistemler (ör: genel internet sayfaları) hariç tüm bilişim sistemlerine erişim parola korumalıdır. Parolalar "Parola Politikasına uygun şekilde tanımlanmalı ve kullanılmalıdır.
7. Kullanıcılar Kurum kaynaklarına erişimi için kullandığı hesap bilgilerini kimseyle paylaşamaz. Yetkisiz kişilerin ele geçirmesine imkân verecek şekilde söylememeli, yazmamalı, kaydetmemeli ve elektronik ortamda depolamamalıdır. İlgili kullanıcı hesabı ile yapılan tüm işlemlerin sorumluluğu hesap sahibi kullanıcıya aittir.
8. Kurum varlıklarına her türlü erişim için "Erişim Kontrol Politikasın"a uygun hareket edilmelidir.
9. Bilgisayarlar, aktif kullanım dışında iken şifreli ekran koruyucular devreye alınır.
10. Mesai zamanları dışında bilgisayar sistemleri mecbur olmadıkça kapalı tutulurlar
11. Kullanıcılar sorumlu oldukları Kurum varlıklarını yetkisiz kişilerle paylaşamaz. Gerekli özenin gösterilmesi ve yetkisiz erişime karşı dikkatli olunması kullanıcı sorumluluğundadır.
12. Kurum bu sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutar.
13. Çalışma alanlarında, "Temiz Masa ve Temiz Ekran Politikası" prensiplerine uygun şekilde, Açık (GENEL) olarak sınıflandırılmış bilgiler dışında bilgilerin başkalarınca görülmesine imkân verilmeyecek şekilde önlemler alınmalıdır;
    - Açık (GENEL) olmayan belgeler, masalarda bırakılmamalıdır.
    - Açık (GENEL) olmayan dosyalar üzerinde çalışılırken bilgisayar ekranları herkesin görebileceği konumda bırakılmamalıdır.
    - Açık (GENEL) olmayan dokümanlar diğer kişilerce görülmesini engellemek amacıyla, kullanılmadığı zamanlarda masa üstlerinden kaldırılıp gerekli korumaları alınmış çekmece ve dolaplarda saklanmalıdır.
14. Açık (GENEL) olmayan belgeler dışında doğrudan işle ilgili olarak kendisine ulaştırılmayan ya da teslim edilmeyen Kurum belgelerini incelememeli, değiştirmemeli, saklamamalı, kopyalamamalı, silmemeli ve paylaşmamalıdır.
15. Gizlilik dereceli bilgilerin posta, faks, telefon, e-posta ve benzeri elektronik yöntemlerle iletiminde "Bilgi İşleme Prosedürü" 'ne uygun davranılmalıdır.
16. Herkese açık bilgiler dışındaki bilgileri internet üzerinde, haber gruplarında, posta listelerinde ve forumlarda paylaşmamalıdır.
17. Gizlilik dereceli bilgiler içeren belgeleri, elektronik ortamları ve bilgi işlem sistemlerini korumak için gerekli fiziksel önlemleri "Fiziksel Güvenlik Prosedürü" 'ne uygun şekilde yerine getirmelidir.
18. Gizli ve hassas bilgiler elektronik ortamda Kurum içine ve özellikle Kurum dışına gönderilmeden önce sıkıştırılarak şifrelenmelidir. Söz konusu şifreler ayrı bir şekilde bildirilmelidir.
19. Gizlilik dereceli bilgiler elektronik ortamda işlenirken, depolanırken, aktarılırken "Bilgi İşleme Prosedürü" 'ne uygun şekilde davranılmalıdır.
20. Gizlilik dereceli bilgilerin ve bilgi içeren ortamlarının imhasında "Teçhizat Güvenliği Prosedürü" 'ne uygun şekilde davranılmalıdır.
21. Kurum tarafından açıkça belirtilen durum ve yöntemler dışında, 3. taraflar ile Kurum bilgileri paylaşılmamalı, aktarılmamalı, yayınlanmamalı ve internet ortamında paylaşılmamalıdır.
22. 3. Taraflar ile gizlilik sözleşmesi imzalanmadan ve yetkili çalışanınca nezaret edilmeden Kurum bilgi işlem sistemlerine ve donanımlarına bağlanmamalı ve çalışmalarına izin verilmemelidir.
23. Çalışanlar, çalıştıkları ortamdaki masa ve dolap çekmecelerini kilitli tutmalı ve anahtarları sorumlu kişiler haricinde kimseyle paylaşmamalıdır.

24. Başta kullanıcı bilgisayarları ve sunucular olmak üzere olan tüm sistemler, zararlı yazılımlara karşı korunmalı ve uygun şekilde kullanılmalıdır.
25. Kuruma ait bilgi işlem sistemlerini izinsiz olarak kullanım dışı bırakılmamalı, yeri değiştirilmemeli ve Kurum dışına çıkartılmamalıdır.
26. Sunucu sistemleri üzerinde, kişisel bilgisayar uygulamaları (ör; e-posta programları, ofis uygulamaları, yazılım geliştirme araçları, network test araçları, vb.) kurulmamalı ve kullanılmamalıdır.
27. İş süreçleri için gerekmeyen ve kullanılmasına izin verilmeyen sunucu hizmetlerini (ör; HTTP, Telnet, SSH, vb.) bilgi işlem sistemleri üzerinde çalıştırılmamalıdır.
28. Kurum tarafından sağlanan ve kullanım amaç ve biçimleri yazılı olarak bildirilen Kurum ağ bağlantı yöntemleri dışında bir yöntemle (ör; ADSL modem, 3G modem, GPRS, vb.) internete veya başka ağlara bağlanmak için kullanılmamalıdır.
29. Kabul edilebilir internet ve e-posta erişim kuralları için "İnternet ve E-Posta Kullanım Prosedürü" 'ne uygun hareket etmelidir.

Genel Donanım Kullanım Esasları

30. Bilgisayar donanımlarının kullanıcılara verilmesi, ilgili kullanım esaslarının tanımlanması Bilgi İşlem Müdürlüğü tarafından yönetilir.
31. Kullanıcılar donanımlara yeni bileşenler ekleyemez veya çıkartamazlar. Ek bir gereksinimin oluşması durumunda Bilgi İşlem Müdürlüğünden yardım talebinde bulunmalıdır.
32. Kullanıcılar kullandıkları bilgisayarlarına izinsiz BIOS şifresi ekleyemezler.
33. Kullanıcılar kullandıkları bilgisayarların işletim sistemlerinde değişiklik yapamazlar.
34. Bilgisayar donanımları üzerindeki tüm bilgilerin Kurumsal nitelikte olduğu kabul edilir.
35. Kurum bilgisayarları üzerinde tutulan tüm bilgiler Kurum tarafından denetlenebilir. Kullanıcılar bu esasa uymakla yükümlüdürler.
36. Kullanıcılar donanım güvenliğini tehdit edecek eylemlerden sakınmakla yükümlüdürler. Kullanıcılara teslim edilen donanımlar üzerinde ayarların değiştirilmemesi, anti virüs programı gibi makine güvenliği ile ilgili ayarlara müdahale edilmemesi ve ilgili programlarda bir sorun gözlemlendiğinde bağlı olduğu sorumluya bildirmesi gerekmektedir.
37. İstemciden istemciye dosya paylaşım programlarını (P2P) Kurum bilgisayarlarına yüklememeli ve kullanmamalıdır.
38. Güvenlik riski oluşturabilecek internet sitelerine girilmemesi kullanıcı sorumluluğundadır.
39. Kullanıcılar Kurumdan ayrılmadan önce kendilerine zimmetli olan tüm donanımları teslim etmekle yükümlüdürler.
40. Kullanıcılar donanımlar üzerinde kasıtlı yapılan zarar vermeler (makinelere fiziksel zarar verme, vurma, kırma, makine üzerine bir sıvının dökülmesi, makinenin düşürülmesi, yetkisiz donanım eklenmesi/çıkarılması vs.) nedeniyle oluşan donanım sorunlarından sorumludurlar. Cezai yaptırım uygulanır ve verdiği zarar kullanıcıya ödetilir.
41. Faks ve Ses cihazlarını kullanıcılar sadece Kurum işleri için kullanmalı, işle alakasız şahsi işleri için meşgul etmemelidirler.
42. Kullanıcılar çıktı alma işlemi için kendi katlarında bulunan ağ yazıcılarını kullanmalıdırlar. Çok gizli gizlilik derecesindeki çıktılar masaüstü ve genel kullanıma açık olmayan yazıcılardan alınmalıdır.
43. Kurum işi ile alakalı olmayan çıktılar kesinlikle Kurum yazıcılarından çıkarılmamalıdır.
44. Çıktı alınan kritik dokümanlar yazıcıya gönderildikten sonra, yazıcı yanında beklenmeli, tüm dokümanın çıktı işlemi bittikten sonra yazıcının yanından ayrılmak gerekmektedir.
45. Yazıcıya gönderilen ve daha sonra iptal edilen tüm dokümanlar mutlaka kontrol edilmelidir.
46. Kullanılmayan ve yok edilmesi gereken bilgiler ilgili prosedüre göre yok edilmelidir.
47. Mühür kullanma yetkisi verilen kişi tarafından muhafaza edilmelidir.
48. Mühür kullanma yetkisi verilen kişilerden habersiz şekilde kullanılmamalıdır.

MOBİL CİHAZ KULLANIM POLİTİKASI

Amaç

Bu politika, Arnavutköy Belediyesi'nde mobil cihazların kullanımı ile ortaya çıkabilecek risklerin yönetilmesi ve destekleyici güvenlik önlemlerinin belirlenmesi amacı ile oluşturulmuştur.

Kapsam

Bu politika Arnavutköy Belediyesi'nde çalışan tüm personeli kapsamaktadır.

Genel Kurallar

Bilgiyi taşımanın kolay bir yolu olan dizüstü bilgisayarlar (laptop), tabletler, akıllı telefonlar gibi mobil cihazların barındırdıkları hassas bilgilerin güvenliğinin sağlanması için dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır.

1. Mobil cihazlara erişimler mutlaka parola ile olmalıdır.
2. Kullanıcı mobil cihazında sakladığı bilgilerin farkında olmalı ve bilgi sınıfına göre muamele etmelidir.
3. Hassas ve gizli bilgiler mümkün olduğunca mobil cihazlarda saklanmamalıdır.
4. Mobil cihazlarda saklanan bilgilerin önemine göre bilgiler şifrelenerek saklanmalıdır.
5. Kaybolmaya ve çalınmaya karşı mobil cihazlar başıboş bırakılmamalıdır. Kaybolma ve çalınması durumunda Bilgi İşlem Müdürlüğü ile iletişime geçilerek gerekli güvenlik önlemleri alınır.
6. Mobil cihazlar kullanılmadığı durumlarda kablosuz erişimleri (kızılötesi, Bluetooth, Wi-Fi) kapalı konumda olmalıdır.
7. Yetkisiz kullanıcılar kendilerine teslim edilen mobil cihazlara yeni bileşenler ekleyemez ya da mevcut bileşeni çıkartamaz. Ek bir gereksinim olduğunda Bilgi İşlem Müdürlüğü ile irtibata geçilmelidir.
8. Tüm dizüstü bilgisayarlar domain yapısına dâhil edilmelidir. Ayrıcalık durumlarında Bilgi İşlem Müdürlüğüne bilgi verilir ve mutlak suretle Anti virüs yazılımı yüklenmesi sağlanır.
9. Bilgisayar donanımları üzerindeki tüm bilgilerin kurumsal nitelikte olduğu kabul edilir. İlgili donanımlar üzerinde şahsa özel bilgilerin tutulmamalıdır.
10. Kullanıcılar Dizüstü bilgisayarlar üzerinde önemli yedek tutmamalıdır.
11. Dizüstü bilgisayarlar otomobil ile seyahat halindeyken araçların bagaj kısmında, toplu taşıma araçlarında seyahat halindeyken ise kullanıcının yanında taşınmalıdır.
12. Lisanssız ürünler cihazlara kurulmamalıdır.
13. Firma ve/veya cihazın işleviyle ilgisi olmayan ürün ve/veya servisler cihazlara kurulmamalıdır.

Taşınabilir Veri Depolama Ortamı Kullanım Kuralları

Günümüzde çok fazla bilgi çok küçük cihazlar içerisinde taşınabilir hale gelmiştir. Bilgi güvenliğinin sağlanması için taşınabilir ortam kullanımında dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır.

1. Kullanıcılar iş ile ilgili her türlü bilgiyi kurum dışına taşınabilir ortamlarda çıkarırken dikkat etmeli, gerekli olandan daha fazla bilgiyi dışarı göndermemelidir.
2. Kurumun belirlenmiş bilgisayarlar haricinde bilgisayarlar USB bellek takılamaz. Bilginin USB Disk ile Taşınması gerektiği durumlarda USB Diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır.
3. İçerisinde tehdit unsuru olan casus yazılımların bulunması ve USB Disk içindeki verinin silinmesine veya başkalarını eline geçmesine neden olabileceği ihtimali düşünülerek, USB Disk biçimlendirdikten sonra veri kopyalanmalıdır.
4. Taşınacak verinin de tehdit unsuru içeren herhangi bir yazılım içermediğine emin olunmalıdır.
5. Önemli bilgilerin yedekleri hem gizlilik hem de bütünlük açısından taşınabilir ortamlara alınmamalıdır.
6. Kaynağı güvenilir olmayan yerlerden temin edilen yerlerden taşınabilir veri depolama ortamları kullanılmamalıdır.

ERİŞİM KONTROL POLİTİKASI

Amaç

Bu politika, Arnavutköy Belediyesi lokasyonlarında veya uzaktan çalışma alanlarında, bilgi ve bilgi işleme olanaklarına erişim için dikkat edilmesi gereken hususları belirlemek amacıyla oluşturulmuştur.

Kapsam

Bu politika, Arnavutköy Belediyesi çalışanlarının ve 3. tarafların tüm erişim yetkilerini kapsamaktadır.

Politika ve uygulama

Bilgi güvenliğini sağlamanın en temel yolu bilgi varlığına yetkisiz kişilerin erişimlerini engellemek/kısıtlamaktır. Bu erişimler iki şekilde gerçekleşebilir; fiziksel ve mantıksal olarak yetkisiz kişilerin kapsam dâhilindeki erişimlerini engellemek için dikkat etmemiz gereken hususlar bu dokümanda tanımlanmıştır.

Sistem Erişim Kontrolü

1. Sistemlere erişim yetkileri; EBYS üzerinden "Erişim Yetkilendirme Talep Formu" ile ilgili birim tarafından talep edilir ve Bilgi İşlem Müdürlüğü tarafından düzenlenir.
2. Kullanıcıların sistemlere erişim yetkileri görevler ayrılığı ilkesi esas alınarak bağlı oldukları müdür tarafından onaylanır.
3. Sistem erişimlerinde mutlaka tüm erişimlerin kısıtlanması için parola kontrolü kullanılmalıdır.
4. Parolasız erişilebilen sunucu, servis veya sistemler bulunmamalıdır.
5. Sistemlere erişimlerde ortak hesap kullanılmamalıdır. Kişi bazında hesabın açılamadığı durumlarda (kurulumla gelen, domainde bulunmayan vs..) kullanımlar günlük kayıtları tutularak gözden geçirilmelidir.
6. Sistemlere yapılan tüm erişimlerin günlük kayıtları (log) tutulmalı ve bozulmaya karşı korunmalıdır.
7. Erişim yetkileri verilirken "bilmesi gerektiği kadar prensibi" ne göre hareket edilmelidir.
8. Yönetici rolündeki personel sistem, sunucu ve servisler üzerinde her türlü işlem için tam yetkilidir.
9. Sistem Yöneticisi rolündeki personel sistem erişiminde sadece etki alanı sunucusunda bulunmaktadır. Normal kullanıcı ekleme, silme, şifre yenileme gibi yetkileri vardır.
10. Sistemlere uzaktan erişim gerektiren durumlarda Uzaktan erişim yetkisi verilecek firmaların yetkili personellerinden öncelikle statik IP bilgisi ve ilgili firma bilgileri istenecek, daha sonra "Uzaktan Erişim Talep Formu'nun ilgili firma tarafından doldurulup Bilgi İşlem Müdürlüğüne iletilmesi sağlanacaktır.
11. Uzaktan erişim için yetkilendirilmiş kuruluş çalışanları veya kuruluşun bilgisayar ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluklara sahiptirler.
12. Uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir.
13. Mobil VPN ile uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile yapılmalıdır.
14. Kuruluş ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.
15. Kuruluştan ilişiği kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri takip edilmeli ve yetkiler / hesap özellikleri buna göre güncellenmelidir.
16. Uzak erişimde yapılan tüm network hareketlerinin günlük kayıtları tutulmalıdır. (loglanmalıdır)
17. Uzak erişim verilecek olan kullanıcılara sözleşmesine göre belirli süreli izinler verilmelidir.
18. Uzak erişim bağlantısında boşta kalma süresi (Herhangi bir işlem yapılmadığı takdirde connection time out süresi) kurumun ihtiyacına göre sınırlandırılmalıdır.
19. Uzaktaki kullanıcı cihazını VPN bağlantısı dışında başka bir bağlantı yapmak için konfigüre edemez. (split tunnel, dual homing vb.)

20. Yazıcı, fotokopi cihazı, faks cihazı gibi cihazların bulunduğu ağların kritik sistemlerin bulunduğu ağlara erişimi engellenmelidir.
21. Sistemlere erişim için kullanılan parolalar parola politikasına göre belirlenmelidir.

Ağ Erişim Kontrolü

1. Kritik sistemlerin bulunduğu ağ diğer ağlardan ayrılmalıdır ve erişimi kısıtlanmalıdır.
2. Ağ cihazlarının bulunduğu ağ diğer ağlardan ayrılmalıdır ve erişimi kısıtlanmalıdır.
3. Uzaktan erişimler için sadece yetki verilen sistemin bulunduğu ağa ve cihaza erişecek şekilde yetkilendirme yapılmalıdır.
4. Kablosuz ağlar için güçlü bir şifreleme kullanılmalıdır.
5. Kablosuz ağlarda varsayılan SSID isimleri kullanılmamalıdır.

Kablosuz Ağ Cihazlarına Erişim Kontrolü

1. Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.
2. Kurum kullanıcısı olmayan kişiler için misafir ağı tanımlanmalı ve bu ağ diğer tüm ağlardan yalıtılmalıdır.

Ağ Cihazlarına Erişim Kontrolü

1. Ağ cihazları erişimlerinde mutlaka tüm erişimlerin kısıtlanması için şifre kontrolü kullanılmalıdır.
2. Şifresiz erişilebilen ağ cihazı bulunmamalıdır.
3. Sistemlerin dahil olduğu ağ cihazlarına veya portlara erişim yetkisi ağ cihazları yöneticisinde olmalıdır.
4. Ağ cihazlarına yapılan tüm erişimlerin günlük kayıtları (log) tutulmalı ve değiştirilmeye karşı korunmalıdır.

Bilgiye Erişimin Kısıtlanması

Erişim izinlerinde kullanıcıya tanımlanması gerekenden daha fazla erişim izni tanımlanmamalıdır.

1. Uygulama erişiminde sadece ilgili menüler erişime açılmalıdır.
2. Hangi verinin hangi kullanıcı için olduğu belirlenmelidir.
3. Kullanıcıların erişim haklarını okuma, yazma, silme ve yönetme gibi yetkiler olarak düzenlenmelidir.
4. Diğer uygulamaların veriye olan erişimleri gözden geçirilmelidir.
5. Hassas bilgileri içeren sistemler için fiziksel ve mantıksal ek güvenlik önlemleri alınmalıdır.

Güvenli Oturum Açma

Oturum açma işlemleri sırasında bilgisayarı sadece yetkili kullanıcıların kullanabileceğine dair kullanıcılar bilgilendirilmelidir.

1. Oturum açma işlemleri sırasında yetkisiz kullanıcılara yol göstermemesi amacıyla yardım mesajları yayınlanmamalıdır.
2. Oturum açma bilgileri ancak tüm veri girişi yapıldıktan sonra doğrulanmak ve hatalı bir giriş yapıldıysa hangi verinin hatalı olduğu belirtilmemelidir.
3. Başarısız oturum açma girişimi sayısının sınırlanması ve başarısız denemelerin kaydedilmesi, özel bir yetkilendirme yapılmadıkça daha sonraki oturum açma girişimlerinin engellenmesi veya belli bir süre bloke edilmesi sağlanmalıdır.
4. Maksimum oturum açma deneme sayısı aşıldığı zaman sistem konsoluna alarm mesajı gönderilmelidir.
5. Oturum açma işlemi için izin verilen minimum ve maksimum süreler tanımlanmalı ve bu süre aşıldığında oturum açma istemi sonlandırılmalıdır.
6. Parola girilirken ekranda karakterler görüntülenmemelidir.
7. Oturum açma işlemleri sırasında sistem veya uygulamaların kimlikleri işlem başarıyla tamamlanana kadar görüntülenmemelidir.

8. Zaman aşımı süresi, bilginin kritikliği, uygulama özellikleri ve kullanıcı terminalinin taşıdığı risklerin derecesine uygun olarak belirlenmelidir.
9. Kritik uygulamalar için bağlantı süreleri ve sayıları kısıtlanmalıdır.

Kullanıcı Erişim Yönetimi

Yetkili kullanıcı erişimini temin etmek ve sistem ve hizmetlere yetkisiz erişimi engellemek için dikkate alınması gereken hususlar aşağıda belirtildiği gibidir.

Kullanıcı Kaydetme ve Kayıt Silme

1. İstihdam sağlanan her kullanıcı için etki alanında kullanıcı adı ve mail adresi, Bilgi İşlem Müdürlüğüne iletildiğinde oluşturulur. Yazılımlar ile ilgili yetkiler kullanıcının çalıştığı birim tarafından talep edilmekte, Bilgi İşlem Müdürlüğü yetkileri açmaktadır.
2. Oluşturulan kullanıcı hesap bilgileri kullanıcılara görev yapacakları birim amiri yolu ile bildirilmelidir ve ilk oturum açmalarında parola değiştirmeleri zorunlu olmalıdır. 24 saat içinde logon olup şifresini değiştirmeyen hesaplar pasif duruma getirilmelidir.
3. Kullanıcılar kendilerine tahsis edilen kullanıcı hesap bilgileri kişiye özeldir ve hiç kimse ile paylaşmamalıdır.
4. Kuruluşta göreve yeni başlayanlar, kuruluştan ayrılanlar ve birim değişiklikleri Bilgi İşlem Müdürlüğüne iletildikten sonra en kısa sürede erişim yetkileri silinmelidir.
5. Kuruluştan ayrılan kuruluş kullanıcılarının hesapları ayrı bir yer içerisinde yetkileri düşürülerek saklanır.
6. Kullanıcı Erişimlerinin Düzenlenmesi ve Kontrolü
7. Kullanıcılara standart kullanıcı haricinde verilen izinler “Erişim Yetkilendirme Talep Formu” ile bildirilir.
8. Kullanıcılara verilen yetkilerde görevlerin ayrılığı ilkesi göz önünde bulundurulur.
9. Kullanıcılara atanacak tüm yetkiler düzenlenmeden hesap aktif edilmez.
10. Aktif edilen hesaplarda ihtiyaca göre talep edildiğinde erişim yetkileri yeniden düzenlenir.
11. Sistem ve uygulamalarda kullanıcılara verilen haklar kayıt altında tutulmalıdır. Müdür onayı olmadan kimseye ek erişim hakkı verilmemelidir.
12. Kullanıcı yetkileri en yılda 1defa periyodik olarak gözden geçirilir ve 90 gün ve üzeri erişim yapmayan kullanıcılar devre dışı bırakılıp farklı bir alanda erişim bilgileri tutulur.
13. Kullanıcının parolasının 5 defa hatalı girilmesi durumunda hesap pasif duruma getirilir.
14. Ayrıcalıklı kullanıcı yetkileri en az 6 ayda bir gözden geçirilir ve kullanılmayan hesapların veya ayrıcalık süresi dolmuş hesapların yetkileri düşürülür ve 3. Adıma göre işlem yapılır.
15. Kuruluştan ayrılan kuruluş kullanıcılarının hesapları ayrı bir alanda yetkileri düşürülerek saklanır.
16. Ayrıcalıklı erişim hakları için gerekli süreler tanımlanmalıdır.
17. Ayrıcalıklı erişim haklarının iz kayıtları öncelikli incelenmelidir.
18. Ayrıcalıklı erişim hakları tanımlanırken ihtiyacı kadar ilkesi göz önünde bulundurulmalıdır.
19. Düzenli olarak kullanılacak ayrıcalıklı erişim hakları için ayrı bir hesap tanımlanmalıdır.
20. Sistem yapılandırma yetenekleri olan kullanıcı parolaları çok gizli bilgi şartlarına uygun olarak saklanmalıdır.
21. Üçüncü taraf bağlantıları için dış firmalar ile yapılan anlaşmalar ile sorumluluklar iletilmelidir.
22. Esas kural olarak üçüncü taraf bağlantılar için ayrı kullanıcı adları oluşturulmalıdır.
23. Üçüncü taraflar için oluşturulan kullanıcı hesaplarının diğer sistemlere erişimleri kısıtlanmalıdır.
24. Üçüncü tarafların tüm erişimleri kayıt altına alınmalıdır.
25. İşi biten firmaların hesapları kapatılmalıdır.

Kullanıcı Sorumlulukları

1. Kimlik bilgileri kesinlikle paylaşılmamalıdır.
2. Kimlik bilgilerini korunmalıdır buna 3. taraflara verilen geçici / kalıcı kimlikler dâhildir.
3. Gizli kimlik bilgileri için kayıt tutmaktan kaçınılmalı ve kayıt tutulması gerekli durumlar için kayıtlar şifreli olarak saklanmalıdır.
4. Kimlik bilgilerinin ifşa olabileceği durumlarda hemen gerekli değişiklikler yapılmalıdır.
5. Kimlik bilgilerinin parolaları nitelikli olmalıdır. Tahmin edilebilir parolalardan uzak durulması tavsiye edilir. (doğum tarihi, isim gibi)

6. Geçici parolaları ilk sisteme girişte değiştirilmeli
7. Kurumsal parolalar kuruluş dışında kullanılmamalıdır. (özel e-posta hesabı, sosyal medya hesapları)
8. Bilgisayar kullanımına ara veren kullanıcılar bilgisayarlarının başından ayrılırken ekranlarını kilitlemekle sorumludurlar.
9. Kullanıcılar şifrelerinin çalındığından kuşkulandıklarında yetkili birimlere haber vermeli, gereken önlemleri almalı ve bilgi güvenliği ihlal olayı kaydı açmalıdır.

PAROLA POLİTİKASI

Amaç

Bu politika amacı Arnavutköy Belediyesi'nde parola kullanımı için gereken kuralları belirlemektir.

Kapsam

Bu dokümanda belirtilen parola oluşturma kuralları, kapsam dâhilinde yer alan kullanıcılara Kurumsal erişim için verilen kullanıcı adı ve şifreler mutlak şekilde uygulanması gereken kuralları içermektedir. Kurumsal erişim harici kalan özel ve Kurumsal uygulamalar için aynı kurallar tavsiye niteliğindedir.

Genel kurallar

1. Kurum kullanıcıları, kendilerine verilmiş olan kullanıcı adı ve parolaların sadece kendileri tarafından kullanılması ilkesini koruma sorumluluğuna uymalıdırlar. Bu ilkenin ihlali durumda kullanıcı sorumlu olacaktır.
2. Tüm kullanıcılar sistem yöneticilerinin ve Bilgi İşlem Müdürlüğü tarafından sağlanan hizmetlerden faydalanmak için sistemde oturum açmak zorundadır. Tüm kullanıcıların kullanıcı-kimliği (user-ID) ve sadece kullanıcının bildiği parola ile kimlik doğrulamasının yapılması zorunludur.
3. Kullanıcı etki alanı parolaları 90 gün süreyle geçerli olup geçerlilik süresi dolduğu zaman veya parolanın güvenlikte olmadığına dair bir gösterge olduğu zaman (ör: saldırılar, çalınma şüphesi, Truva atı bulunması, vs.) değiştirilmelidir.
4. Parolalar aşağıdaki özelliklere uygun olmalıdır.
    a. Kullanıcılarının etki alanı parolaları en az 8 karakterli olmalıdır, büyük harf, küçük harf, noktalama işareti ve rakam özelliklerinden en az üçünü içeren karmaşık şifreler belirlenmelidir.
    b. Parolalar çalışanların, ailesinin ve arkadaşının sahip olduğu bir hayvanın veya bir sanatçının ismine sahip olmamalıdır.
    c. "Arnavutköy", "zetacad","istanbul", "ankara" gibi isimler içermemelidir.
    d. Doğum tarihi veya adres ve telefon numaraları gibi kişisel bilgiler içermemelidir.
    e. Aaabbb, qwerty, zyxwuts, 123321 vs. gibi sıralı harf veya rakamlar içermemelidir.
    f. Yukardaki herhangi bir kelimenin geri yazılış şekli olmamalıdır.
    g. Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek, gizli1, gizli2) olmamalıdır.
5. Kullanıcıya verilen ilk etki alanı parolasını unuttuğu zaman verilen parolalar "geçici parola" olarak düşünülmeli ve ilk oturum açılışında sistem tarafından değiştirmeye zorlanmalıdır.
6. Kurum personeli şahsi parolalarını özel kontrol altında tutmalı, parolalarını sistem yöneticisi de dahil olmak üzere hiç kimseyle paylaşmamalıdır.
7. Kullanıcılar parolalarının çalındığından kuşkulandıklarında yetkili birimlere haber vermeli, gereken önlemleri almalı ve bilgi güvenliği ihlal olayı kaydı açmalıdır.
8. Kullanıcılar, kurum servisleri için kullandıkları parolalarını, Internet üzerinde başka amaçlar için (örneğin tartışma gruplarına üyelik, Yahoo, gmail vb. gibi bedava e-posta hesapları için) kullanmamalıdır.

9. Parolalar, dosya, otomatik komut dosyası (log-in script), yazılım makrosu, erişim kontrolü olmayan bilgisayarlar ve yetkisiz personelin fark edebileceği yerlere (kâğıt üzerine yazarak bilgisayarın yanına bırakmak gibi) yazılmamalıdır.
10. Kullanıcılar şahsi işleri için kullanmış oldukları parolaları kesinlikle sistemde kullanmamalıdır.
11. Kullanıcılar ihtiyaç duydukları zaman Ctrl+Alt+Del tuşlarına basarak parolalarını değiştirebilmelidir.
12. Kritik sistemlere ve ağ cihazlarına erişim için sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır.
13. Oturum açma sırasında parola kısmı **** olarak gizlenmelidir.
14. Sistemler kullanılan güvenlik yazılımlarıyla hatalı ve başarısız logonlar kaydedilmelidir.
15. Herhangi bir denetim sırasında kullanıcı adları tespiti kolay ve anlaşılır olmalıdır.

TEMİZ MASA VE TEMİZ EKRAN POLİTİKASI

Amaç

Bu politika, Arnavutköy Belediyesi'nde kullanıcıların çalışma esnasında masa ve ekranlarının kullanımında uyması gereken kuralları belirtmek amacıyla oluşturulmuştur.

Kapsam

Bu politika; Arnavutköy Belediyesinde bilgisayar ve masa başında çalışan, bilgi varlığına doğrudan ulaşma imkanı olan tüm personeli kapsamaktadır.

Genel kurallar

1. Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgeler kilitli yerlerde muhafaza edilmelidir.
2. Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir.
3. Personelin kullandığı masaüstü veya dizüstü bilgisayarlar ekran açık terkedildi ise; 10 dakika içerisinde ekran kararmalı, mesai saatleri içerisinde ekran otomatik olarak 30 dakika sonra kapanmalı 60 dakika sonra bilgisayar uyku moduna geçmeli, mesai saatleri dışında 5 dakika sonra ekran kapanmalı 6 dakika sonra da bilgisayar uyku moduna geçmelidir.
4. Personel kendileri veya birimleri için kritik belgeleri, Kuruluşa Özel ve Gizli etiketli dokümanları mutlaka kilitli çekmece veya dolaplarda bulundurmalıdırlar.
5. Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır.
6. Ekranlar yetkisiz kişilerin görmesi engelleyecek şekilde yerleştirilmelidir. Cama veya koridora dönük şekilde yerleştirilmemelidir.
7. Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler kâğıt öğütücü, disk/disket kıyıcı, yırtma, yakma vb. metotlarla imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir.
8. İçerisinde Kuruluşa ait bilgi bulunan CD, DVD, USB vb. depolama ortamları masa üzerlerinde bırakılmamalıdır.
9. CD, sarf malzemesi, sarf donanımlar vb. malzemeler mutlaka kilitli ortamlarda bulunmalıdır.
10. Yazıcı ve Faks makineleri sürekli kontrol edilmeli ve bu cihazlarda gizlilik önemi arz eden bilgiler bırakılmamalıdır.
11. Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PC'ler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.
12. Şifrelerin ve erişim kartlarının kişiye özel olduğu bilinmeli ve paylaşılmamalıdır.
13. Temiz masa ve ekran politikası içeriği her yıl farkındalık eğitimlerinde çalışanlara tekrarlanmalıdır.

TEDARİKÇİ İLİŞKİLERİ YÖNETİMİ POLİTİKASI

Amaç

Bu politikanın amacı, Bilgi Güvenliği Yönetim Sistemi çerçevesinde çalışılan tedarikçilerin verdiği hizmetin kesintisiz ve kaliteli olarak sağlanmasını güvence altına almak ve yürütme yöntemlerini açıklamaktır.

Kapsam

Bu politika, Arnavutköy Belediyesinin çalıştığı tüm tedarikçileri kapsar.

Genel kurallar

Arnavutköy Belediyesi Resmi kamu kurumu olarak yaptığı işlerde, verdiği hizmetlerde devamlılığı ve kaliteyi sağlamak için tedarikçilerle çalışmaktadır. Bu çalışmaların şartları mevzuata bağlı olarak hizmet anlaşmaları, ihale ve satın alma dosyaları ile kayıt altında tutulur.

Bu politikanın genel amacı kurumla çalışan tedarikçiler tarafından erişilen varlıkların korunmasını sağlamak, tedarikçinin kuruluşun varlıklarına erişimi ile ilgili riskleri azaltmak, bilgi güvenliği gereklerini yerine getirmek ve yapılan çalışmaların kalitesini arttırmaktır.

Tedarikçi ilişkilerini yönetmek için hizmet alan her birim risk profiline göre değerlendirme yapmalı, çalışacağı tedarikçinin türüne göre tedarik sürecini planlamalı, süreç dâhilinde bilgi varlıklarına erişim türünü belirlemeli, verilen erişim izinlerini izlemeli, kurum politika ve prosedürlerine uymasını sağlamalı ve farkındalığını arttırmalıdır.
Bilgi güvenliği gereksinimlerini karşılamak amacıyla; tedarikçinin hangi sınıftaki bilgilere erişebileceği, sözleşme süresince çalıştıracağı personelin niteliği, yetkinliği ve erişim yetkileri, bilgi güvenliği farkındalığı ve uyumu, sözleşmenin bitiminden itibaren gizliliğin korunmasına yönelik tedbirler tanımlanmalı ve anlaşmalara dahil edilmelidir

Tedarik sürecinde Kurum bünyesinde çalışacak personele bilgi güvenliği farkındalık eğitimi verilmesi zorunludur. Bu eğitimlerde Kurum ile iletişim halinde bulunan tedarikçi personelin bilgi güvenliğine uygun çalışma ve davranma kuralları konusunda bilgilendirme yapılır.

Kurum tedarikçileri ile çalışması süresince Bilgi Güvenliği gereklerini teminat altına almak için bazı ek önlemler geliştirmiştir.

- "Paydaş Personel Gizlilik Taahhütnamesi": Tedarikçi firmalara bağlı olarak Arnavutköy Belediyesinin lokayonlarında çalışan, kurum kaynaklarına erişim sağlayan personelin imzalaması istenen taahhütnamedir.
- "Gizlilik Sözleşmesi": tedarikçi firmaların Arnavutköy Belediyesi ile çalıştıkları süre içinde vakıf oldukları, eriştikleri her türlü kurumsal bilginin korunmasını temin etmek için imzalanan sözleşme.
- 'Uzaktan erişim talep formu': Verilen hizmet kapsamında kurum sistemlerine uzaktan erişim sağlaması gereken tedarikçilerden alınan form. Formla uzaktan erişimi sağlayacak cihazın IP si ve sistemlere giriş yolu formla kayıt altına alınır ve bu verilere göre form onaylanır.

İNTERNET VE E-POSTA KULLANIMI POLİTİKASI

Amaç

Bu politika; Arnavutköy Belediyesi e-posta ve internet hizmetinin uygun olmayan kullanımını engelleyerek; Kurumun yasal yükümlülüklerini, kapasite kullanımını ve Kurumsal imajını korumak amacı ile dikkat edilmesi gereken hususları ve belirlemek için oluşturulmuştur.

Kapsam

Bu politika; Arnavutköy Belediyesinde istihdam edilmiş olan tüm personeli kapsamaktadır.

Kısaltmalar ve Tanımlar

Anti virüs Gateway: Ağ Geçidinde virüs ve zararlı programları tarama teknolojisi

Spam: İstenmeyen e-posta.

Phishing: Dolandırıcıların rastgele kullanıcı hesaplarına e-mail gönderdikleri bir çevrimiçi saldırı türüdür.

GB: Gigabyte (Bilgisayarlarda kullanılan 1024 megabayt anlamına gelen ölçü birimidir)

MB: Megabyte (Bilgisayarlarda kullanılan 1.000.000 byte anlamına gelen ölçü birimidir)

Genel kurallar

İnternet Kullanım Esasları

Her türlü bilgiye erişilebilen ve her türlü bilginin paylaşılabileceği internet kullanımında dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır.

1. Kurum bilgisayar ağı erişim ve içerik denetimi yapan bir güvenlik duvarı (firewall) üzerinden geçtikten sonra internete çıkacaktır.
2. Kurumun ihtiyacı ve yasal gereklilikler doğrultusunda Kurum içerik filtrelemesi yapabilmelidir, istenilmeyen sitelere (oyun, kumar, şiddet, pornografi vb.) erişim yasaklanabilmelidir.
3. Kurumun ihtiyacı doğrultusunda saldırı tespit ve önleme cihazları kullanılmalıdır.
4. Antivirüs gateway sistemleri kullanılarak internete giden veya internetten gelen bütün trafik virüslere karşı korunmalıdır.
5. Yetkilendirilmiş sistem yöneticileri internete çıkarken ihtiyaçları doğrultusunda bütün servisleri kullanabilmelidir.
6. Multimedya streaming yapılmamalıdır.
7. Kişisel internet kullanımı işin üretkenliğini etkilemediği ve işin önceliğinin önüne geçmediği sürece kabul edilebilirdir.
8. İş ile ilgili olmayan yüksek hacimli dosyalar (müzik, video vb.) yüklenmemeli ve indirilmemelidir.
9. Kurum tarafından onaylanmamış yazılımlar internet üzerinden indirilmemelidir ve Kurum sistemlerine yüklenmemelidir.
10. Üçüncü tarafların interneti kullanımı Bilgi İşlem Müdürlüğü'nün izni ile sağlanmalıdır ve üçüncü tarafların kullandıkları ağ ile Kurum sistemlerinin bulunduğu ağ birbirinden farklı olmalı ve birbirileri ile haberleşmeleri engellenmelidir.
11. İnternet ortamında, Bilgi İşlem Müdürlüğü'nden yazılı izin alınmaksızın herhangi bir biçimde Kurum adına beyanda ya da taahhütlerde bulunulmamalıdır.
12. Kurum içerisinden yapılan Internet erişimlerinde Kurum güvenliğini tehlikeye sokacak veya Türkiye Cumhuriyeti yasalarında yasadışı kabul edilen sitelere girilmemesi kullanıcı sorumluluğundadır.
13. Kurum içerisinden yapılan internet erişimi, Kurum tarafından denetlenmeli ve kayıt altına alınmalıdır. 5651 sayılı kanun gereği Kurum ilgili erişim bilgilerini tutmak ve devletin ilgili mercileri tarafından istenmesi durumunda bu bilgiyi sağlamakla yükümlüdür. Bu kanun doğrultusunda kullanıcıların yasadışı kabul edilen sitelere girmesi durumunda Kurun yetkilileri tarafından gerekli cezai işlem uygulanabileceği ya da savcılık tarafından haklarında suç duyurusunda bulunulabileceğini bilmekle yükümlüdür. Kurum, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü taraflarla, emniyet kuvvetleriyle veya yargıyla kullanıcının izni olmadan paylaşma hakkını saklı tutar.
14. Kullanıcılar kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bunun için kullanıcılar kimlik bilgilerini uygun şekilde saklamalı ve başkaları ile paylaşmamalıdır.

E-Posta Kullanım Esasları

1. Kullanıcı kendisine tanımlanan e-posta hesabının özelliklerinde değişiklik yapılmasını talep ederse bu talebini EBYS sistemi üzerinden "Erişim Yetkilendirme Talep Formu" ile Bilgi İşlem Müdürlüğü'ne iletmelidir.
2. Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz
3. Kurum e-posta kaynakları Kurum işlerinin gerçekleştirilmesi için kullanılmalıdır.
4. İş dışı konulardaki haber grupları Kurum e-posta adres defterine eklenemez.
5. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez.
6. Kurumun e-posta sunucusu, Kurum içi ve dışı başka kullanıcılara zincir e-postalar, reklam, karalama SPAM veya Phishing mesajlar göndermek için kullanılamaz.
7. Kurumun e-posta sistemi ücretsiz veya ticari yazılımın alınması, gönderilmesi veya saklanması için kullanılamaz.
8. Kullanıcı hesapları, doğrudan ya da dolaylı olarak ticari ve kâr amaçlı olarak kullanılamaz. Diğer kullanıcılara bu amaçla e-posta gönderilemez.
9. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz
10. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı, e-posta Bilgi İşlem Müdürlüğüne iletilmelidir
11. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" vb. uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (ZIP veya RAR formatında) mesaja eklenmelidir.
12. Kurum ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Gönderilmesi zorunlu durumlarda ise içerik şifrelenmelidir ve mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
13. Zincir mesajlar, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, Bilgi İşlem Müdürlüğü'ne haber verilmelidir. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılmalıdır.
14. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul etmektedir. Suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların içeriğinden kullanıcı sorumludur.
15. Kullanıcı, gelen ve/veya giden mesajlarının Kurum içi veya dışındaki yetkisiz kişiler tarafından okunmasını engellemelidir.
16. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın Bilgi İşlem Müdürlüğü'ne haber verilmelidir. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılmalıdır.
17. Kullanıcı, Kurumsal mesajlarına, Kurum iş akışının aksamaması için zamanında yanıt vermelidir.
18. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda Bilgi işlem Müdürlüğü'ne haber verilmelidir. Durum değerlendirildikten sonra gerekli ise bilgi güvenliği ihlal olayı başlatılmalıdır.
19. Kullanıcı, e-posta vasıtasıyla bulaşabilecek virüs gibi zararlı içerikten korunmak amacıyla, tanımadığı kişilerden gelen ve şüpheli eklentiler içerdiği görülen mesajları gerekmediği sürece açmamalıdır. Tüm e-posta içerikleri ve eklentileri açılmadan önce zararlı kodlara ve virüslere karşı taramadan geçirilmelidir.
20. Kuruluşa ait olmayan e-posta hizmetleri ile (Gmail, Hotmail, Yahoo, vb.) Kurumsal bilgiler paylaşılmamalıdır.
21. Çalışanlar düzenli olarak posta kutularını gözden geçirmelidir ve gerekmeyen e-postaları silmelidirler.
22. Kullanıcı, elektronik posta sistemlerini, önemli bilgilerin arşiv deposu için kullanmamalı.
23. Kurum personeli kişisel mesajlaşmaları için Kurumsal e-posta hesabını kullanmamalıdır, gönderdiği, aldığı e-postalarda kişisellik aramamalıdır. Bu yüzden yetkili kişiler önceden haber vermeksizin e-postaları denetleyebilirler.
24. Elektronik haberleşmenin içeriğinin düzenli olarak izlenmesi Kurumun politikasının bir parçası değildir. Ancak Kurum şüphelenilen mesajların incelenme hakkına ve yetkisine sahiptir. Bununla birlikte Internet üzerinden yapılan elektronik haberleşmenin içeriği izlenebilir ve elektronik haberleşme sistemlerinin kullanımı işlevsel, bakım, teftiş, güvenlik, araştırma faaliyetlerini desteklemek için izlenebilir. Çalışanlar

elektronik haberleşmenin içeriğini Kuruluşun zaman zaman kontrol edeceği gerçeğini kabul ederek kullanmalıdırlar.

BİLGİ İŞLEME

Amaç

Bu prosedür; Kurum içerisinde ve herhangi bir dış varlık arasında transfer edilen bilginin güvenliğini sağlamak amacıyla oluşturulmuştur.

Kapsam

Bu prosedür; Arnavutköy Belediyesi ne ait tüm bilgi varlıklarının transferini kapsamaktadır.

Kısaltmalar ve Tanımlar

USB: Universal Serial Bus (Evrensel Seri Veriyolu)

CD: Compact Disc (Yoğun Disk)

DVD: Digital Versatile Disc (Çok Amaçlı Sayısal Disk)

SSH: Secure Shell (güvenli veri iletimi için kriptografik ağ protokolüdür)

Genel kurallar

Gizlilik dereceli bilgilerin aktarımından önce, bilgiyi talep edenin bu bilgiye erişim yetkisi bulunduğundan emin olunur. Erişim yetkisinin bulunduğunu belgelendirme sorumluluğu bilgiyi talep eden taraftadır. Şifahi olarak gizlilik dereceli bilgilerin Kuruluş içinde ve dışında aktarımı söz konusu olamaz.

Elektronik ortamda bilgi transferi

1. Elektronik ortamda gizli dosyaların transferi yapılmamaktadır.
2. Elektronik postalar yetkisiz erişime değiştirilmeye ve hizmet kesintisine karşı korunur.
3. Sistemlere yönetim amaçlı erişimler SSH gibi güvenli yöntemlerle yapılır.
4. Sistemlere yönetim amaçlı yapılan uzaktan erişimler VPN gibi güvenli metotlar ile yapılır.
5. Sistem yönetiminin farklı bir iletişim kanalından (farklı bir porttan) yapılması sağlanmalıdır.

Fiziksel ortamda bilgi transferi

1. Kurumdan yapılacak bilgi transferi (arşiv dosyası devri) karşı kurumla yapılan yazışmadan sonra gerçekleştirilir.
2. Transferi yapılacak bilginin miktarı, türü, içeriği kayıt altına alınır.
3. Karşılıklı imza altına alınan tutanakla karşı kuruma elden teslim edilir.
4. Kurye ile gönderilen bilgi için, yetkili kuryeler onaylanmış olmalıdır.
5. Gönderilen ortam fiziksel ve çevresel değişkenlerden etkilenmeyecek şekilde özenle paketlenir.
6. Gönderen taraf, aktarılan varlığın alıcının eline geçip geçmediğini kontrol eder. (örneğin telefon ile teyit alınır)
7. Bilgi varlığı, zarf içine sığabilecek boyutlarda ise (CD, Kâğıt gibi), zarfa konularak yapıştırılmak suretiyle kapatılır. Gönderen kişi, zarf kapağını imzalayarak kuryeye teslim eder.
8. Bilgi varlığı, disk, bilgisayar gibi zarf içine sığmayacak boyutlarda ise, uygun şekilde paketlenir. Paketler, gönderilen varlığa zarar gelmesini önleyecek nitelikte ve sağlamlıkta olmalıdır. Paketlerin yolda açılmadığından emin olmak için kapak bölümü imzalanır.
9. Alıcı taraf, aktarım esnasında gönderilen paketin açılmadığından emin olmalıdır.
10. Aktarımların dolaylı yollarla, elden ele teslimat şeklinde değil, bir seferde gönderenden alıcıya ulaşacak şekilde gerçekleşmesi esastır.

Sözlü ve Görsel Bilgi Transferi

1. Elektronik ve fiziksel ortamlarda bilginin aktarımı konusunda olduğu gibi, sözlü iletişimde de bilgi güvenliğinin korunması sağlanır.
2. Kuruluşa özel konular hakkında, kamuya açık alanlarda yüksek sesle konuşulmaz.
3. Telefon görüşmelerinde, toplantılarda, vb. sözlü iletişimin sağlandığı ortamlarda karşı tarafın (telefonla görüşülen kişi, toplantı katılımcıları gibi) gizlilik dereceli bilgiye erişim yetkisi yoksa veya erişim yetkisinden emin olunamıyorsa, gizlilik dereceli bilgiler paylaşılmaz.
4. Çalışanlar "sosyal mühendislik" yöntemi konusunda bilgilendirilir ve yetkisiz kişilere bilgi vermez.
5. Kurumun kamuoyundaki imajını oluşturan, reklam, web sitesi, afiş, tanıtım videosu gibi tanıtım materyalleri bir bilgi güvenliği ihlali olup olmadığı (gizlilik dereceli bilgilerin dâhil edilmiş olması, teknik altyapıya ilişkin detaylı bilgilerin bulunması vb.) kontrol edilerek kamuoyuna sunulur.
6. Yapılan toplantılar veya çalışma gruplarında hazırlanan görseller (Kâğıt üzerinde veya yazı tahtasında bulunan topolojiler) saklanır ya da yok edilir.

FİZİKSEL GÜVENLİK

Amaç

Bu prosedür, Kurumun bilgi varlıklarına yetkisiz fiziksel erişimi, bilgi ve bilgi işleme olanaklarına hasar verilmesini ve müdahale edilmesini engellemek için dikkat edilmesi gereken hususları belirlemek amacıyla oluşturulmuştur.

Kapsam

Bu prosedür; Arnavutköy Belediyesi Bilgi Güvenliği gereklerinin uygulanacağı tüm fiziksel lokasyonları kapsamaktadır.

Genel kurallar

1. Bina girişleri kartlı geçiş ve özel güvenlik ile korunur.
2. Sistem odası diğer ortamlardan yalıtılır ve ayrı erişim kontrolleri (kartlı geçiş, parmak okuma, kilitli kabinler vb. sistemler) bulunur.
3. Kritik bilgi işleme tesisleri
4. girişleri sürekli kapalı tutulur.
5. Kritik bilgi işleme tesisleri gerekli görüldüğünde birden fazla önlem ile korunur.
6. Fiziksel güvenlik sınırı tedbirleri alanın içerisinde bulundurduğu bilgi varlığının güvenlik ihtiyaçlarına göre belirlenir.
7. Yönetim Merkezi binasında ziyaretçilerin giriş çıkış kayıtları saklanmalıdır.
8. Kurum içerisinde yetkilendirilmemiş kişilerin bilgi ve fiziksel varlıklara erişimi engellenmeli, kişilerin sadece erişmesi gereken alanlara ulaşması sağlanmalıdır.
9. Gizli alanlara girişler ilgili müdürlük sorumluları / yöneticileri tarafından onaylanmalıdır.
10. Ziyaretçilere fiziksel güvenlik ve acil durumlar hakkında bilgi verilmelidir.
11. Ziyaretçiler kimlik kartları ile erişim sağlamalı, gizli alanlarda yetkisiz kişilerin görülmesi durumunda uyarı yapılmalıdır.
12. Gizli alanlara girişler ilgili müdürlük sorumluları tarafında liste yapılmalı, yöneticileri tarafından onaylanmalıdır.
13. Kritik odalara erişimler kontrollü olmalıdır ve yalnızca yetkili kişiler girebilmelidir.
14. Hassas odaların tabela ve işaretleyiciler ile yerleri belirlenmemelidir.
15. Diğer Kurum çalışanları ve üçüncü tarafların gerekli durumlarda personel çalışma alanına erişimleri sırasında yetkili çalışanlar refakat etmelidir.
16. Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.
17. Kritik bilgi içeren ofisler ve odalar ile ilgili aşağıdaki hususlara ayrıca dikkat edilmelidir;
    - Kritik bilgi içeren ofisler ve odalar kolay erişilebilir yerlerde konumlandırılmamalıdır.

- Kritik bilgi içeren odalara erişimlerde mümkünse ayrıca giriş kontrolleri (parmak izi, damar okuyucu, kartlı geçiş vb.) uygulanmalıdır ve bu erişim kayıtları saklanmalıdır ve değiştirilmeye karşı korunmalıdır.
- Kritik bilgi içeren ofisler ve odalarda kolay tutuşabilir malzemeler bulundurulmamalıdır.
- Kritik bilgi içeren ofisler ve odalarda yangın, su baskını, deprem, patlama, sivil gösteri ve hareketler ve diğer doğal veya insan kaynaklı felaketlerin muhtemel sonuçlan değerlendirilmelidir ve gerekli önlemler alınmalıdır.

18. Kurumsal güvenliği sağlamak Destek Hizmetleri Müdürlüğü sorumluluğundadır.
19. Kurumsal güvenliği sağlamak amacıyla kuruluş girişinde 24 saat güvenlik bulunmalıdır.
20. Tüm katlarda kritik noktalar kameralar ile izlenmeli ve kayıt edilmelidir.
21. Kurum personeli geçiş kartlarını imza karşılığında İnsan Kaynakları Müdürlüğünden teslim almalıdır.
22. Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karsı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.
23. Komşu tesislerden kaynaklanan potansiyel tehditler göz önünde bulundurulmalıdır.
24. Kayıt cihazlarının güvenli alanlara sokulmasına engel olunmalıdır.
25. Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.
26. Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.
27. Güvenli bölgelere örneğin sistem odasına yapılan girişler kayıt altına alınmalıdır.
28. Teslimat ve yükleme alanları güvenlik ve kamera ile kontrol altında tutulmalıdır.
29. Yönetim Merkezi binasında ziyaretçilerin giriş çıkış kayıtları saklanmalıdır.
30. Ziyaretçilere fiziksel güvenlik ve acil durumlar hakkında bilgi verilmelidir.

YASAL GEREKSİNİMLERE UYUM VE KONTROL

Amaç

Bu prosedürün amacı; Arnavutköy Belediyesinde uygulanmakta olan Bilgi güvenliği gereklerinin yasal altyapısını açıklamak ve yasalara uyumu kontrol etmek için bir çerçeve sunmaktır.

Kapsam

Bu prosedür; Arnavutköy Belediyesi Bilgi Güvenliği Kapsamına dahil edilen tüm varlıkları kapsar.

Genel esaslar

1. Kurum Bilgi Güvenliği Kapsamı dokümanında yer alan her şahıs, hizmet alımı olarak firmalar tarafından Kurum kaynaklarını kullanmakta olan üçüncü taraflar, tedarikçiler Kurum Bilgi Güvenlik politikası ve konu ile ilgili düzenlenmiş her türlü yasal kurallara uyma zorunluluğundadırlar. Aykırı durumlar söz konusu olduğu hallerde Kurum içi ya da hukuki cezalandırmaya tabi tutulacaklarını bilmekte ve bu prosedürü okuyarak taahhüt etmektedirler.
2. Yukarıdaki maddede adı geçen tüm şahıs ve grupların sorumlulukları kapsam dâhilindeki müdürlüklerde belirlenmiş ve kişilere tebliğ edilmiş aynı zamanda BGYS kapsamında tüm çalışanlarla "Kullanıcı Taahhütnamesi" imzalanmıştır.
3. BGYS kapsamında yapılan organizasyondaki roller ve sorumluluklar ise "Roller ve Sorumluluklar" organizasyon dokümanında, ihtiyaç halinde veya acil bir durumda kimin kimlerle bağlantı kuracağı "İletişim Kılavuzu" dokümanında tanımlanmıştır.
4. Kurum kaynaklarının kullanımı esnasında oluşacak yasal veya Kurum içi düzenlemelere aykırı faaliyetlerin kayıtlarının tutulması ve gerektiğinde delil olarak yetkili makamlara verilmesi Kurum sorumluluğundadır.
5. Kurumda uygulanan bilgi güvenliği politikaları, kaynakların oluşturulması ve sunumu ve kullanımı fikri mülkiyet hakları, personel yasaları ve diğer ilgili yasalara uygun olacaktır.
6. Şifreleme için kısıtlamalar belirlenmeli ve yasal zorunluluklar için istenen belgeler yazılım ve donanımlar ile şifrelenmesi durumunda erişilebilir oluğu kontrol edilecektir.

7. Ağ üzerinde yapılan her türlü erişim ve hareketler kayıt altına alınmalı yetkisiz erişim ve kural dışı kullanım tespit edilen durumlarda "Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürü" uygulanmalıdır.
8. Herhangi bir bilişim suçu işlediği saptanan çalışan, yasalara uygun olarak cezai işlem görür.
9. Bilgi güvenliği olayı için kanıt oluşturabilecek (yazışmalar, internet erişim kayıtları, DHCP kayıtları) herhangi bir veri, yetkililer gelene kadar değişime uğramayacak ve kanıt özelliğini kaybetmeyecek şekilde saklanacaktır.

Bu genel esasların yanında ISO 27001 Kapsamlı BGYS Politikası, Prosedürleri ve yazılı belge haline getirilmiş tüm bilgiler ilgili personelin yetkisine açık şekilde, Kurum İçi Kalite ve Bilgi Güvenliği Yönetimi için kullanılan uygulama üzerinde yayınlanmaktadır. Aynı zamanda, üçüncü taraflara ve tedarikçilere bildirilmesi gereken Taahhüt, Politika belgeleri web sitesinde yayınlanmaktadır.

Kurumun üst yönetimi dâhil olmak üzere tüm Kurum çalışanları ve 3. taraflar, Kurum tarafından belirlenmiş ve dokümante edilmiş ISO 27001 Kapsamlı BGYS Politikası ve Prosedürlerine uygun hareket etmek zorundadır. Uygunsuz hareketler ve aykırılık sebepli suç kapsamında olan her eylem disiplin hükümleri ve / veya yasal yaptırımlarla cezai işlem göreceklerdir.

BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

Amaç

Bu prosedürün amacı; Arnavutköy Belediyesi'nde bilgi güvenliği ihlal olayları tespitinde ve yönetiminde dikkat edilmesi gereken noktaları açıklamaktır.

Kapsam

Bu doküman Arnavutköy Belediyesi Bilgi Güvenliği Kapsamında yer alan tüm bilgi varlıkları içerir.

Genel esaslar

Bilgi güvenliği ihlal olayı tespiti konusunda tüm çalışanlar öncelikli ve gerçek sorumludurlar. Bununla birlikte tüm kullanıcılar sistemde ve fiziksel ortamda oluşan olağan dışı durumları BGYS Sorumlusuna bildirmekle sorumludurlar. Olay ihlalleri kurumsal portal üzerindeki İHLAL/BİLDİRİ sekmesinden de yapılabilir.

BGYS Sorumlusu olayların tespitinden sonraki süreçler olan delil toplama, önlem alma, deneyim edinme ve disiplin yönetimi konularında ilgili birimlerle çalışma gerçekleştirecektir. İhlal olayları ile ilgili oluşturulan kayıtlar bilgi güvenliği toplantılarında BGYS Yürütme Komitesi ile paylaşılacaktır.

BGYS Yürütme Komitesi tekrar edebilecek ihlal olaylarını engellemek veya gerçekleşmesi durumunda müdahale edebilmek için İhlal olayları ile ilgili oluşturulan kayıtları incelemek ile sorumludur.

Bilgi güvenliği olaylarına hızlı etkili ve düzenli şekilde cevap verebilmek için bilgi güvenliği ihlal olayları karşısında BGYS Sorumlusu öncelikli ve gerçek sorumludur. Tespiti yapılan olay ile ilgili Kuruluş dışı birim ya da firmadan destek alınması gereken durumlarda iletişimi kurmak ve sağlamak konusunda öncelikli sorumluluk müdahaleyi yapacak olan ilgili müdürlük ve BGYS Yönetim Temsilcisidir.

Kuruluş çalışanlarının şüpheli buldukları durumlarda normal şartlarda mail, telefon veya yazılım üzerinden görev kaydı açarak iletişime geçmeleri gereklidir. ***İstem dışı kaybolan veya ortaya çıkan dosyalar, anti-virüs ajanının çalışmasında çıkan sorunlar, bilgisayarların aşırı yavaşlaması, istemsiz çalışan programlar ve istemsiz açılan pencereler, yetkisiz personelin güvenli alanlarda bulunması, gizli dosyaların dış müdahaleye açık olması, sadece Kuruluş içerisinde bilinmesi veya işlenmesi gereken bilginin kuruluş dışında veya sosyal medyada paylaşılması gibi çok özel durumlarda sözlü veya telefonla yapılan bildirimler kayıt altına alınacaktır.***

BGYS Yönetim Temsilcisi, BGYS Sorumlusuna gelen olay bildirimlerini veya Kuruluş güvenlik yazılımları aracılığıyla tespit edilen bilgi güvenliği ihlal olayları olarak tespit ettikleri her şüpheli durumu yönetmekle sorumludur.

BGYS Sorumlusu düzenli bir şekilde bilgi güvenliği ihlal olayı oluşup oluşmadığını kontrol etmelidir.

Bilgi İşlem Fiziksel olarak sistem ve servislerde açıklıkların bulunup bulunmadığı kontrol edilmelidir. Raporlama müdahale için gerekli bilgileri kapsayacak detayda olmalı ve kayıtlar içermelidir.

Yaptırım

Bu el kitabında çerçevesini çizilen; Arnavutköy Belediyesi Bilgi Güvenliği Politikalarını ve uygulanacak kuralları; tüm personel bilme, kabul etme ve gereklerini yerine getirme yükümlülüğündedir. Yükümlülüğünü yerine getirmeyenler hakkında olayın meydana geliş şekline göre disiplin süreci işletilecektir.