ERZURUM BÜYÜKŞEHİR BELEDİYESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI

BİLGİ GÜVENLİĞİ POLİTİKASI

(Versiyon 1.0)

2022

Doküman Detayları

Hazırlanma Tarihi	12.12.2022	**Yayın**	Final
Hazırlayan	Olcay Ozan DİKBAŞ – Ersin YILDIZ		
Doküman Numarası	EBB-POL-01		

Revizyon Geçmişi

Revizyon Tarihi	Önceki Revizyon Tarihi	Yapılan Değişikliklerin Özeti
12.12.2022		İlk Yayın

Onay

Onaylayan	İmza	Görevi	Tarih	Versiyon
Zafer AYNALI		Genel Sekreter	12.12.2022	1.0
Murat ALTUNDAĞ		Genel Sekreter Yardımcısı	12.12.2022	1.0
Serkan ÇEKİÇ		Bilgi İşlem Daire Başkanı	12.12.2022	1.0

İçindekiler

1 Amaç

Bilgi Güvenliği Politikasının amacı, Erzurum Büyükşehir Belediyesi'nde uygulanan süreç ve faaliyetlerde, süreç ve bilgilerin gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla üst yönetimin kurumsal güvenlik yönünü tayin etmek ve gereksinimleri tanımlamaktır.

2 Kısaltmalar ve Tanımlar

Tanım	Açıklama
Bilgi	Çalışmalar sonucu ortaya çıkan karar verme aşamasında kullanılan, anlam taşıyan işlenmiş veri.
Bilgi Güvenliği	Bilgi güvenliği, bilgi varlıklarının ortamdaki olası tehditlerden zarar görmeden kullanılabilmesidir. Bilgi Güvenliği, "Gizlilik", "Bütünlük" ve "Erişilebilirlik" olarak isimlendirilen üç unsurdan oluşur.
Gizlilik	Bilginin sadece izin verilenler tarafından erişilmesidir.
Bütünlük	Bilginin sahibi tarafından yaratılmasından sonra yetkisiz değiştirilmemesinin sağlanması
Erişilebilirlik	Bilginin istendiğinde hizmet verilecek konumda olmasının sağlanması
Bilgi Güvenlik Yönetim Sistemi (BGYS)	Bilgi Güvenliğini iyileştirmek, yönetmek, gözden geçirmek, uygulamak için iş riski temelli toplam yönetim sistemi
BGYS dokümantasyonu	BGYS'yi yönetmek için oluşturulan Bilgi Güvenliği Politika, Prosedür, Talimat ve Kılavuzları
Spam	Büyük adetlerde özellikle reklam amacıyla gönderilen, istenmeyen, teklifsiz veya uygun olmayan e-posta mesajlarıdır.
Oltalama (Phishing)	E-posta/web sayfalar üzerinden bir kişinin erişim bilgilerini, özellikle internet bankacılığı bilgilerini, yetkisiz olarak ele geçirmek için yapılan kandırma yöntemidir.
İş Etki Analizi	Özel bir felaketin etkilerini ve iş fonksiyonlarının süreçlerini analiz etme işlemi.
İş Sürekliliği	Kuruluşun olaylara karşılık verme ve bunun planlamasını yapma konusunda stratejik ve taktiksel becerisi ve iş kesintileri için önceden tanımlanmış kabul edilebilir seviyede iş uygulamalarına devam etme becerisidir.
Görevler Ayrılığı	Hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile mali karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi görevlerinin çalışanlar arasında paylaştırılmasıdır.

Risk Analizi	Risklerin hesaplanması ve kaynakların tespiti için bilginin sistematik kullanımı.

3 Sorumlular

BGYS koordinasyonu ve yönetiminden, hizmetler için süreç alanlarının tanımlanmasından, süreçlerin uygulanmasından ve raporlama faaliyetlerinin yerine getirilmesinden sorumlu bir Yönetim Temsilcisi ataması yapılmıştır.

BGYS Temsilcisi : Bilgi ve İletişim Teknolojileri Direktörü

BGYS Sorumlusu : Bilgi Güvenliği ve Sistem Yönetimi Uzmanı

3.1 BGYS Temsilcisi

Erzurum Büyükşehir Belediyesi'nin BGYS yöneticisi, Bilgi İşlem Daire Başkanı'dır ve sorumlulukları aşağıdaki gibidir:

- BGYS faaliyetlerini geliştirmek ve güvenlik ihtiyaçlarını karşılamak üzere yapılan plan ve programların uygulanması için kaynakların atamasını gerçekleştirmek.
- Yönetimi BGYS'de gerçekleştirilen faaliyetler ve önemli güvenlik konuları hakkında bilgilendirmek.
- Bilgi güvenliği aktivitelerine ve güvenlik programlarına yön vermek ve onaylamak
- Bilgi güvenliğinin kurumsal olarak yaygınlaşmasını sağlamak için gerekli görev ve sorumlulukları delege etmek.
- Büyükşehir Belediyesi Bilgi Güvenliği Politikası ve Prosedürlerini gözden geçirmek ve gerekli değişiklikler için önerilerde bulunmak.
- Bilgi güvenliği risk değerlendirme raporlarını, aksiyon planlarını, güvenlik kontrollerini gözden geçirmek ve bilgi güvenliği risk yönetimi faaliyetleri ve artık risklerin kabulünü gerçekleştirmek.
- Erzurum Büyükşehir Belediyesi'nde acil durumlarda ve önemli güvenlik ihlallerinde güvenlik tehditlerini ve tekrarlanmaması için alınan önlemleri gözden geçirmek.
- BGYS iç denetim raporlarını gözden geçirmek ve değerlendirmek.
- Farkındalık eğitimlerinin etkinliğinin ölçülmesi ve sonuçların değerlendirmek.
- Kapsam içerisindeki süreç ve birimleri tanımlayan ve zaman planını içeren İç Tetkik Planı'nı onaylamak ve tetkiklerin gerçekleşmesini sağlamak.
- İlgili otorite ve çalışma grupları ile iletişim ve koordinasyonun sağlamak.
- Dış taraflara ve belgelendirme kuruluşlarına karşı kurumu temsil etmek ve ilgili faaliyetlerde koordinasyonu sağlamak.
- BGYS dokümantasyonu içerisinde yer alan politika, prosedür, form, şablon, liste vb. dokümanları hazırlamak ve/veya hazırlanması için koordinasyonu sağlamak.
- BGYS şartlarına uyum sağlanması için koordinasyonu sağlamak.
- BGYS kapsamında karşılaşılabilecek bilgi güvenliği risk analizinin gerçekleştirilmiş ve gerekli önlemlerin alınmış olmasını sağlamak için ilgili ekipleri koordine etmek.
- BGYS Temsilcisi Üniversite Mezunu olmalı, Bilgi Güvenliği konularında tecrübe sahibi olmalı ve en az bir sistemin kurulma aşamasında görev almış olmalı.

3.2 Büyükşehir Belediyesi Çalışanları

Büyükşehir Belediyesi çalışanlarının rol ve sorumlulukları aşağıdaki gibidir:

BGYS dokümantasyonuna uymak.

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

BGYS Politikalarına uyumun sağlanmadığı veya bilgi güvenliği ihlal olayına şahit olduğu durumlarda ihlal olayın some@erzurum.bel.tr bildirimde bulunmak.

Büyükşehir Belediyesi bilgi sistemlerinin uygun şekilde çalışmasını olumsuz etkileyebilecek veya bilgi güvenliğini tehlikeye atacak faaliyetlerde bulunmamak.

BGYS dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi İşlem Daire Başkanlığı'na bildirmek.

Bilgi ve kurumsal kaynaklara erişim/bağlantılarında yetkilerinin iş ihtiyaçları kadar olmasını sağlamak.

3.3 Büyükşehir Belediyesi Yöneticileri

Büyükşehir Belediyesi yöneticilerinin rol ve sorumlulukları aşağıdaki gibidir:

BGYS kurallarına uymak ve ekibi içerisinde uyumu sağlamak üzere gerekli aksiyonların koordinasyonunu ve takibini gerçekleştirmek.

Kendilerine bağlı çalışanlarının sistem ve uygulama yetkilerini gözden geçirmek ve görevi dışında olan yetkilerin iptalini sağlamak.

Kendilerine bağlı çalışanların nakil, terfi ve ayrılmalarında bilgi erişim yetkilerini gözden geçirmek ve ihtiyaç kalmayan yetkilerin iptal edilmesini sağlamak.

3.4 Bilgi Varlık Sahipleri ve Operasyon Sahipleri

Bilgi Varlık Sahipleri'nin ve Operasyon Sorumluları'nın rol ve sorumlulukları aşağıdaki gibidir:

Sahibi olunan bilgi varlığın erişim haklarını ve kimlerin yönetici ve kullanıcı bazında hangi ayrıcalıkla erişilebileceğini tayin etmek.

Varlık envanterinin güncelliğini sağlamak.

Sahibi olunan varlıkların gizlilik sınıflarını belirlenen kritere göre tayin etmek, gizlilik sınıfı değişen varlıkları güncellemek ve BGYS Yöneticisi'nin onayına sunmak.

3.5 Siber Olaylara Müdahele Ekibi (SOME)

SOME'nin rol ve sorumlulukları aşağıdaki gibidir:

Çalışan, teknik ekip, yardım masası veya üçüncü partilerden ve dış müşterilerden gelen bilgi güvenlik olaylarını analiz ederek bunları önceliklendirmek ve gerekli aksiyonların alınması için koordinasyonu sağlamak

Tekrarlayan olaylar için kalıcı çözümler üretmek ve aksiyon almak/aldırmak

Bilgi sistemlerine ait güvenlik olaylarına ve zafiyetlerine, zamanında düzeltici aksiyonların alınmasını sağlamak için Üniversite içinde iletişimi ve koordinasyonu sağlamak

Bilgi Güvenliği Olay Yönetimi Politikası belirtilen aktivitelere uygun hareket etmek.

Gerçekleşen olaylarda; çalışanlar, müşteri, hizmet sağlayan veya yasal düzenleyici kurumlara bilgi verilmesi gerekiyorsa, bilginin gönderilmesini sağlamak/koordine etmek.

3.6 Tedarikciler ve iş ortakları

Tedarikciler ve iş ortakları rol ve sorumlulukları aşağıdaki gibidir:

BGYS Yöneticisi tarafından belirlenen ve sözleşmeler veya güvenlik protokolü vasıtasıyla firmasına/kendisine bildirilen bilgi güvenliği/gizlilik kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen BGYS dokümantasyonuna uymak.

- Büyükşehir Belediyesi'ne ait bilgi ve varlıkları Büyükşehir Belediyesi'nin onayı ve izni olmadan başkaları ile paylaşmamak
- Büyükşehir Belediyesi tarafından kendilerine verilen kimlikleri sözleşmelere, BGYS politika ve prosedürlere uygun şekilde kullanmak.
- Büyükşehir Belediyesinde çalışmakta olan çalışanlarının kendi firmasından ayrılması/görev değiştirmesi söz konusu ise, bu durumu aynı gün içerisinde Büyükşehir Belediyesi 'ne bildirmek ve yetkilerinin iptal olmasını sağlamak.
- Büyükşehir Belediyesi'nin onay ve izni olmadan, Büyükşehir Belediyesi'nin cihazlarındaki veri ve yazılımı kopyalamamak, ortamın resmini/videosunu çekmemek, Büyükşehir Belediyesi veri güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak.

4 Uygulama

4.1 Yönetimin Taahhüdü

Bilgi, Büyükşehir Belediyesi'nin en önemli varlıklarından biridir ve herkes bilgi güvenliğinden sorumludur. Yöneticiler, tedarikçiler, iş ortakları ve çalışanlar hakkındaki bilgiler, süreçler, faaliyetler ve sistemler başarımız için önemlidir. Bu nedenle, bilgi varlıklarının gizliliğinin uygun şekilde sağlanması, içeriğinin doğru ve tam olması ve gerektiğinde ulaşılabilir olması, Büyükşehir Belediyesi'nin kurumsal yönetiminin ana unsurlarındandır. Ayrıca Büyükşehir Belediyesi'nin yasal şartlara uyumluluğunu temin etmek için bilginin güvenliliğinin sağlanması zorunlu bir koşuldur.

Sahip olunan bilgi varlıkları; bilgiyi üretme, işleme ve sunma imkanları, Büyükşehir Belediyesi'nin vizyonuna ulaşmak için en önemli değerleridir. Büyükşehir Belediyesi, kurumsal işlevlerini yerine getirmek için birçok bilgiye ve bilgi varlıklarına gereksinim duymaktadır. Bu bilgilerin gizliliğinin uygun şekilde sağlanması, içeriğinin doğru ve tam olması ve gerek duyulduğunda ulaşılması Büyükşehir Belediyesi'nin ana hedefleri arasındadır.

Bu amaçla;

- BGYS kapsamında bilgi ve süreçler tespit edilir. Karşılaşılabilecek riskler değerlendirilir ve önemli riskleri azaltmak için gerekli önlemler alınır,
- Büyükşehir Belediyesi, yasa ve sözleşmelerden kaynaklanan gereksinimlere uyum için kişisel ve kurumsal bilgilerinin güvenliğini taahhüt eder.
- BGYS' nin devamlılığını sağlamak için gerekli kaynaklar temin edilir ve sistemin sürekli gelişmesi desteklenir,
- Bu amaçların gerçekleştirilebilmesi için ortaya çıkan gereksinimleri karşılamak ve bilgi güvenliğini yönlendirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ile sürekli olarak iyileştirmek için toplantılara yönetim olarak katılır ve BGYS Yönetim Temsilcisi ataması yapılır.

4.2 Bilgi Güvenliği Organizasyonu

a) Büyükşehir Belediyesi içinde bilgi güvenliğinin etkin yönetimi için; TS ISO/IEC 27001 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulur.
b) BGYS'nin devamlılığını sağlamak için gerekli kaynaklar sağlanır ve sistemin sürekli gelişmesi desteklenir.
c) Bu politikanın Sorumluluklar başlığı altında yer alan Bilgi Güvenliği Yönetim Yapısı işletilir.

4.3 İnsan Kaynakları Güvenliği

a) Büyükşehir Belediyesi çalışanları ve yüklenicilerinin kendi sorumluluklarını anlamalarını ve düşünüldükleri roller için uygun olmalarını sağlamak için istihdam öncesi kontroller tesis edilir.
b) Büyükşehir Belediyesi çalışanları ve yüklenicilerinin bilgi güvenliği sorumluluklarının farkında olmaları ve yerine getirmeleri için bilgilendirmeler ve farkındalık eğitimleri yapılır. Bu eğitimlere katılmak ve güncel bilgilere sahip olmak herkesin görevidir.
c) Büyükşehir Belediyesi ait gizli bilgiler asansör, kafeterya vb. umuma açık mekanlarda tartışılmaz.
ç) Verilen iş ilanlarında açıklamalar, Büyükşehir Belediyesi'nin gelecek planları veya BT ihtiyaçları, hassas bilgileri içermeyecek şekilde yapılır.

4.3.1 Bilgi Güvenliği Farkındalığı

a) Çalışanların bilgi güvenliği farkındalığını arttırmak, güncel tehditler ve alınması gereken önlemler konusunda uyarmak amacı ile her sene çeşitli faaliyetler (bilgi güvenliği duyuruları, bilgi güvenliği seminerleri, eğitimler vb.) yürütülür.
b) İşe yeni alınan çalışana oryantasyon çalışmasında İK Daire Başkanlığı tarafından bilgi güvenliği politika ve prosedürlerine ilişkin bilgi verilir.
c) Tüm çalışanlara zorunlu olarak yılda en az bir kez olmak üzere Bilgi Güvenliği Farkındalık Eğitimi seminer veya e-eğitim olarak verilir. Bu eğitimlerin içeriğinin oluşturulmasından Bilgi İşlem Daire Başkanlığı, çalışanların katılımının sağlanmasından IK Daire Başkanlığı sorumludur. Ayrıca bilgi güvenliği ile ilgili özel sorumluluğu bulunan çalışanlara bu konudaki yeterlilik ve etkinliğini arttırmak üzere eğitimler atanır.
ç) Bilgi Güvenliği Farkındalık Eğitimi'nde aşağıdaki konular işlenir:
    - Güncel Güvenlik Tehditleri
    - Sosyal Mühendislik
    - Bilgi Güvenliği Politika ve Prosedürleri
    - Bilgi Güvenliği Olay Bildirimi
    - Bilgi Güvenliği Yönetim Sistemi
    - Bilgi güvenliğine ilişkin çalışan sorumlulukları
d) Büyükşehir Belediyesi tarafından organize edilecek bilgi güvenliği program ve eğitimlerine iştirak etmek bütün Büyükşehir Belediyesi çalışanlarının görevleri arasındadır. Verilen farkındalık eğitimlerinin etkinliğinin ölçülebilir olması esastır. Eğitimler sonrasında verimliliğinin ölçülmesi amacıyla katılımcılardan anket, sınav gibi yollar ile geri bildirimler alınır.
e) Yöneticiler, kendilerine raporlayan çalışanın eğer var ise rol ve sorumluluğu kapsamında yer alan sistem ve uygulamaların vb. süreçlerin işletilmesine ilişkin eğitimlerin alınmasından ve bu eğitimlerin planlanarak temin edilmesinden sorumludur.

4.4 Bilgi Varlığı Yönetimi

a) Bilgi ve bilgi işleme tesisleri ile ilgili varlıklar belirlenir ve bu varlıkların bir envanteri tutulur. Her bir varlık için Varlık Sahibi belirlenir ve bu varlıklara ilişkin bilgilerin güncel tutulması Varlık Sahibi' nin görevidir.
b) Varlık Sahibi, aksi belirtilmediği sürece o bilgiyi hazırlayan ve üreten bölümün veya birimin başındaki kişi olarak varsayılır. Varlık Sahibi; bilginin korunması için delege edilmiş operasyon sahibine, varlığın hassasiyeti, önemi, kontrolü ve izleme ihtiyaçları konusunda bilgi verir.
c) Varlıkların kabul edilebilir kullanımına ilişkin kurallar Kabul Edilebilir Kullanım Politikası içinde listelenmiştir ve herkes bu politikayı anlayıp uygular.
ç) Varlık Sahipleri, Varlık Yönetimi ve Sınıflandırma Politikası' nı göz önüne alarak, varlıkların gizlilik sınıflarını tanımlar ve gerekli etiketlemeleri belirler. Sınıflamanın doğru yapılması varlık sahibinin sorumluluğudur. Varlık sınıflandırılması işlemi için son onay BGYS Yöneticisi tarafından gerçekleştirilir.
d) Bilgi işlenirken, iletilirken ve muhafaza edilirken Gizlilik, Bütünlük ve Erişilebilirlik esas alınarak korunur.

4.5 Erişim Kontrolü

a) Bilgi ve kurumsal kaynaklara erişim/bağlantı yetkileri, "gerekli olan en az yetki" prensibine göre verilir.
b) Erişim/bağlantı yetkileri ve sorumluluklar, "görevler ayrılığı ilkesine" göre verilir.
c) Kaynaklara erişim özellikle tahsis edilmediği sürece, yasak olarak kabul edilir.
ç) Varlık Sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirir.
d) Parola yönetim sistemleri etkileşimli olur ve yeterli güvenlik seviyesine sahip parolaları temin etmektedir. Tüm taşınabilir bilgisayar ve cihazlar insansız durumdayken parola ile kilitlenerek koruma altına alınır.
e) Hesap verilebilirlik ortamını sağlamak adına, her kullanıcı kendi kimlik doğrulama bilgilerinin korunmasından sorumludur. Erişim bilgileri kişiye özeldir ve paylaşılmaz.

4.6 Kriptografi

a) Büyükşehir Belediyesi'in sahip olduğu bilgilerin gizliliğini ve bütünlüğünü güvence altına almak için kurum dışına aktarılan veriler üzerinde kriptografik (ssl) kontroller uygulanır.
b) Kullanılan ssl sertifikası her yıl yenilenmektedir.
c) Kullanıcı parolaları sha-256 algoritmasına göre şifrelenir.

4.7 Fiziksel ve Çevresel Güvenlik

a) Bilgi ve bilgi işleme tesislerini/sistemlerini barındıran alanları korumak için; güvenlik sınırları belirlenir, bu alanlarda taşıdığı riskle doğru orantılı olarak fiziksel güvenlik tesis edilir.
b) Güvenlik önlemleri alınırken doğal felaketler, kötü niyetli saldırılar veya kazalar göz önünde bulundurulur.
c) Taşınabilir cihazın kaybolması veya yetkisiz kişilerin eline geçmesi riski durumunda, zaman kaybetmeden Siber Olaylara Müdahale Ekibi (SOME)'ne haber verilir.
ç) Giriş çıkış kapıları, ofis odaları ve malzeme teslim alma/verme alanları (depolar, giriş kapıları vb.) güvenli konuma getirilir ve Fiziksel Güvenlik Politikası'na uygun hareket edilir.
d) Ömrünü doldurmuş depolama ortamları formatlanarak üzerinde bilgi olmadığından emin olunur ve demirbaş birimine hurda olarak gönderilir.

e) Ortak kullanılan yazıcılardan alınan çıktılar göndereni tarafından takip edilerek alınır. Kritik ve üstü sınıfındaki belgeler ortak yazıcılardan alınmaz.

4.8 İşletim Güvenliği

a) Bilgi güvenliğini etkileyen önemli değişiklikler gerçekleştirilmeden önce planlanır, test edilir ve kayıt edilir.
b) Zararlı kodlardan ve teknik güvenlik açıklıklarından kaynaklı veri kaybı yaşamamak için düzenli olarak ağ, uygulama ve sistem seviyelerinde zafiyet taraması ve sızma testleri gerçekleştirilir. Bununla beraber anti-virüs yazılımları kullanılır. Bu yazılımlarla düzenli olarak tarama gerçekleştirilir.
c) Veri kaybını en aza indirmek ve/veya tamamen önlemek için yedekleme mekanizmaları kullanılır ve bu yedek verilerin bütünlüğü düzenli olarak test edilir.
ç) Sistemler üzerinde gerçekleştirilen önemli değişiklikler denetlenebilir ve izlenebilir şekilde yapılandırılır. Günlük raporları gizli bilgi içeren ara yüzlere erişim ve erişim kurallarında yapılan değişiklikler için sorumluyu belirleyebilme olanağını sağlayabilecek niteliktedir.
d) Uygunsuz davranışları engellemek, kullanıcı sorumluluğunu teşvik etmek ve güçlü sistem yönetimi sağlamak için üretim ortamları verisini etkileyen tüm kullanıcı aktiviteleri takip edilebilir olmalıdır. Günlük raporlarının bütünlüğü güvence altına alınarak, iş ihtiyaçları ve yasal zorunluluklara göre belirlenen sürelerde saklanmaklıdır.
e) Büyükşehir Belediyesi ağları ve bilgisayarları aşağıda belirtilmiş tüm yasal amaçlarla izlenir:
    - Kullanımın yetkili bir şekilde olduğunun sağlanması.
    - Güvenlik prosedürlerinin doğrulanması.
    - Sistem ve operasyonel güvenlik.
    - Büyükşehir Belediyesi politikaları ve regülasyonlara uygunluk.
    - Yasadışı aktivitelerin tespiti ve engellenmesi.

4.9 Haberleşme Güvenliği

a) İletişim ağı üzerinde bulunan sistemler kritiklik ve erişim ihtiyacına göre bölümlenir ve uygun güvenlik önlemleri alınır.
b) Bilişim ağının sınırları uygun donanım ve yazılım kullanılarak koruma altına alınır ve bilişim ağı sınırları ve iç ağ düzenli olarak uygun bir şekilde izlenir.
c) Bilgilerin elektronik olarak transferi esnasında transfer edilen bilginin Varlık Yönetimi ve Sınıflandırma Politikası'nda belirlenen gizlilik sınıfına göre güvenlik ihtiyaçları sağlanır.
ç) Herhangi bir Büyükşehir Belediyesi çalışanı; halka açık mekanlarda, resmi konferanslarda sunum veya tanıtım yaptığında Büyükşehir Belediyesi ile ilgili bir bilgi/resim vb. paylaşacak ise aşağıdaki kurallara uyar:
    - Paylaşılacak materyal ile ilgili; Bilgi Güvenliği Birimine ve konusu ile alakalı birime bilgi verir.
    - En az direktör veya koordinatör seviyesi olmak üzere yöneticisinden onay alır.
    - Paylaşılacak materyali İletişim ve Yazı İşleri Koordinatörlüğü ile paylaşır.

4.10 Sistem Temini, Geliştirme ve Bakımı

a) Bilgi güvenliğinin, bilgi sistemlerinin tüm yaşam döngüsü boyunca dahili bir parçası olmasını sağlamak için bilgi güvenliğini ilgilendiren bütün projelerde Bilgi İşlem Daire Başkanlığı'nın görüşü alınır.

b) Bilgi güvenliğinin bilgi sistemleri geliştirme yaşam döngüsü içerisinde tasarlanıp uygulanmasını güvence altına almak için bütün sistem geliştirme faaliyetleri Güvenli Sistem ve Yazılım Geliştirme Prosedürü' ne uygun olarak yapılır.
c) Kritik sistemler için güvenlik sıkılaştırma kılavuzları oluşturulur. Sistemlerin bu kılavuzlarda belirlenen kurallara uyumu takip edilir.
ç) Geliştirme, test ve işletim ortamları iş verileri ve işletim yazılımlarına yetkisiz erişimi engellemek veya kazara değiştirme riskini azaltmak için ayrılır.

4.11 Tedarikçi İlişkileri

a) Tüm Üçüncü Parti'ler, Büyükşehir Belediyesi'nin uymakla zorunlu olduğu yasa ve yönetmelik kurallarına uygun hizmet verirler.
b) Büyükşehir Belediyesi'nin bilgi varlıklarına erişim hakkı olan üçüncü partilerin uyması gereken kurallar imzalanan sözleşmelerde veya dokümanlarda tanımlanmıştır. Bu politika erişim yetkisi verilen bütün üçüncü partilerle paylaşılır, üçüncü parti tarafından protokol olarak imzalanır ve politikaya uymamaları durumunda söz konusu olacak yaptırım sözleşme veya ek protokol ile güvence altına alınır.
c) Büyükşehir Belediyesi ağına bağlanacak tüm firmalar ile Gizlilik Anlaşması imzalanır.

4.12 Bilgi Güvenliği İlkeleri

a) Taraflar, özellikle kişisel bilgilerini içeren ve bununla sınırlı olmaksızın bu Sözleşme konusu işlemlerin yapılması ile ilgili tüm bilgileri, Büyükşehir Belediyesi'nin uymakla zorunlu olduğu mevcut ve yeni çıkacak mevzuatlara uyacak şekilde korumak için gerekli kontrol ve tedbirleri almakla yükümlü olduğunu, aksi halde doğabilecek her türlü zarardan sorumlu olduğunu beyan ve kabul eder.
b) Büyükşehir Belediyesi ile ilgili her türlü bilgiyi içeren materyal, dokuman ve/veya benzeri kayıtlar taraflar arasındaki işbu ticari ilişkinin nihayet bulması ve/veya bu sözleşmenin sona ermesi halinde ve/veya karşı tarafın yazılı ihtarı üzerine Büyükşehir Belediyesi'ne iade veya imha edilir. İade veya imhaya ilişkin kanıtlar talep halinde gösterilmek üzere saklanır.
c) Büyükşehir Belediyesi, hizmet sunumu ile ilgili konularda söz sahibi olacak ve gerekirse hizmet sunum süreçlerinde bilgi güvenliği ile ilgili değişiklik yapılmasını isteyebilecektir. Bu durumda yüklenici firma Büyükşehir Belediyesi'nin isteğini ivedilikle yerine getirecektir.
ç) Büyükşehir Belediyesi işbu sözleşmede yer alan güvenlik maddelerinin yerine getirildiğini kontrol etmek amacıyla Yükleniciyi denetleyebilir. Yüklenici Kişisel Verilerin Korunması Kanununa göre "Veri İşleyen" durumunda ise denetleme kişisel verilerin korunması kapsamında yapılır. Bu denetleme Yüklenicinin ofisinde, veri merkezinde veya Büyükşehir Belediyesi ile ilgili bilgileri kapsayacak yerlerde, bilgisayar, sunucu ve diğer elektronik ve basılı dokuman üzerinde inceleme yapmayı içerebilir. Yüklenici, bu denetimlerde gerekli bilgileri ve ortamı sağlamakla yükümlüdür.
d) Yüklenici, Büyükşehir Belediyesi projelerinde çalışan personel değişikliklerini (işe giriş, işten çıkış, görev tanımı değişikliği) derhal Büyükşehir Belediyesi'ne bildirecek ve Büyükşehir Belediyesi bünyesinde verilmiş olan yetkilerin kaldırılmasını talep edecektir.
e) Yüklenici'nin, alt yüklenici başka bir firma ile anlaşması durumunda bu firmanın sözleşmede belirtilen tüm hükümleri karşılaması gerekmektedir. Alt yüklenici firmanın işbu hükümleri karşılamaması halinde oluşacak zararlardan Yüklenici sorumludur.
f) Sistem/Uygulama/Veritabanı erişimlerinde her Yüklenici Personeli farklı hesap kullanacaktır. Yüklenici firma Büyükşehir Belediyesi'ne hizmet vermekte kullandığı sistemlerde denetim izlerini açık tutmakla yükümlüdür. Bağlantı yapılan IP/Terminal bilgisi, tarih, zaman, kullanıcı adı, işlem detayı içermelidir. Büyükşehir Belediyesi gerekli gördüğü hallerde yapılan işlemler hakkında rapor ve

denetim izlerini talep etme hakkını saklı tutar. Bu nedenle Yüklenici firma denetim izlerini yasal süre boyunca saklamakla yükümlüdür.

g) Yüklenici firma personeli Büyükşehir Belediyesi'nin izni olmadan Büyükşehir Belediyesi'nin mülkiyetindeki sistem/ağ erişime teşebbüs etmeyecektir. Erişim esnasında da Büyükşehir Belediyesi'nin kendine bildirdiği kurallara aynen uyacak, verilen yetkileri arttırmaya yönelik bir teşebbüste bulunmayacaktır.

ğ) Büyükşehir Belediyesi verileri Yöneticilerin yazılı onayı olmaksızın hiç bir şekilde CD, DVD, USB gibi taşınabilir medyalarda ve kişisel bilgisayarlarda veya bilgi kaçağına neden olabilecek herhangi bir ortamda saklanamaz, transfer edilemez, işlenemez, kullanılamaz. Büyükşehir Belediyesi ile Yüklenici Firma arasında gizli bilgilerin paylaşımı söz konusu olduğunda bu işlem şifreli olarak ve güvenli kanallar ile yapılacaktır.

h) Cep telefonu, fotoğraf makinası, kamera, kayıt cihazı gibi elektronik cihazlar bilgi güvenliğini tehlikeye sokacak şekilde izinsiz olarak çalışma ortamında kullanılmayacaktır.

ı) Yüklenici Firma kendi bünyesinde Büyükşehir Belediyesi'ne ait bilgilerin bulunduğu sistemlerin fiziksel ortamlarını yetkisiz erişimlerden korumak üzere giriş-çıkış kartları, güvenlik kameraları vb. gerekli güvenlik önemlerini yerine getirmekle yükümlüdür.

i) Yüklenici kendi sorumluluğu altındaki bilgi ve verilerin uygun biçimde yedeğinin alınmakta olduğundan, güvenli olarak saklandığından ve kurtarma süreçleri için gerekebilecek düzenlemeleri yapmakta olduğundan ve böylece bir problemin ortaya çıkması durumunda Büyükşehir Belediyesi'nin işine olan etkisinin en aza indirgendiğinden emin olunmalıdır. Yüklenici, beklenmeyen yıkıcı faaliyetlerin söz konusu olması durumunda servis sunumunun devamlılığını sağlayabilmek için uygun ölçütlerin oluşturulmuş olduğundan emin olmalıdır. Bu ölçütler, resmi felaket kurtarma ve iş devamlılığının Yüklenici işinin kapsamında planlanması, uygulanması ve önceden test edilmesini içermelidir.

j) Büyükşehir Belediyesi'nden alınan veriler Büyükşehir Belediyesi'nin yazılı izni olmadan üçüncü kişilerin veri merkezinde saklanamaz, yönetimi üçüncü kişilere devredilemez.

k) Yüklenici firma çalışanları, gördüğü bir bilgi güvenliği ihlal olayını vakit kaybetmeden kendisine refakat eden Üniversite çalışanına yüz yüze, eposta veya telefon kanalıyla bildirir. Refakatçi Büyükşehir Belediyesi çalışanı bu bilgi güvenliği olayını değerlendirerek SOME' ye (some@erzurum.bel.tr) bildirir.

l) Yüklenici, Büyükşehir Belediyesi ile ilişkili çalışanlarını, asgari olarak yılda bir kere olmak koşulu ile periyodik olarak bilgi güvenliği farkındalığı konusunda eğitmeli ve bu eğitimlere ilişkin kayıtları istenildiği takdirde Büyükşehir Belediyesi ile paylaşabilmelidir.

m) Yüklenici firma, geliştirdiği yazılım ve/veya ürettiği donanımlarına arka-kapı (backdoor) zararlı yazılımların eklenmediğini garanti etmeli ve bunun için ilgili kontrolleri kendisi Büyükşehir Belediyesi'ne teslimattan önce gerçekleştirmelidir.

n) Yüklenici firma, geliştirdiği ve geliştirttiği yazılımların uzaktan izinsiz erişim, kod çalıştırma, veri sızıntısı ve manipülasyonu, servis dışı bırakma vb. bilinen uygulama güvenliği risklerini içermemesini sağlamak için bünyesinde güvenli geliştirme süreçleri oluşturmalı ve geliştiricilere güvenli kodlama eğitimleri, sızma testleri, kaynak kod analizi güvenlik testleri gibi güvenlik aktivitelerini Büyükşehir Belediyesi'ne teslimattan önce kendisi gerçekleştirmelidir. Yüklenici firmanın test senaryoları, elde edilen sonuçları ve güvenlik açıklıklarının giderildiğine ilişkin kanıtları Büyükşehir Belediyesi ile paylaşması gerekmektedir.

o) Büyükşehir Belediyesi gerçekleştireceği ürün/yazılım kabul testleri kapsamında bilgi güvenliği testlerini yapabilir veya üçüncü bir partiye yaptırabilir. Bu testler sırasında çıkabilecek problemlerin çözümünün gecikmesi ve de ürünün sorunlarının giderilmemesi nedeniyle Sözleşme'nin ifası gecikir ise Sözleşme'de belirtilen cezai şartlar uygulanacaktır.

ö) Yüklenici Firma, Büyükşehir Belediyesi'nin onaylı izni olmadan Büyükşehir Belediyesi bilişim ortamlarında Sızma ve Zafiyet Analizi Testleri yapamaz.
p) Yüklenici Firma çalışanları sağlanan giriş kartları görünür bir şekilde taşınacak, başkaları ile paylaşılmayacak, kaybolması durumunda ilgililere vakit kaybetmeden bildirilecektir.
r) Arızalı veya bakım gerektirien bilgi varlıkları Büyükşehir Belediyesi'ne ait bilgiler veya kişisel veriler içermesi durumunda hafıza birimleri çıkarılarak veya özel disk sıfırlama yazılımları kullanılarak diskleri sıfırlandıktan sonra dışına çıkarılacaktır.
s) Yükenici Firma, Büyükşehir Belediyesi'nin yasakladığı fiziksel alanlara giremez.
ş) Yüklenici, Büyükşehir Belediyesi'nde çalıştırdığı her personeline işbu sözleşmenin ekinde bulunan Bilgi Güvenliği Taahhütnamesini imzalatmakla yükümlüdür.

4.13 Bilgi Güvenliği İhlal Olayı Yönetimi

a) Bilgi güvenliği ihlal olaylarının yönetimi için güvenlik olayları ve açıklıkları üzerindeki bağlantısını içeren, tutarlı ve etkili bir yaklaşımın sağlanması amacı ile yönetim sorumlulukları ve prosedürler belirlenir.
b) Tüm bilgi güvenlik ihlalleri Siber Olaylara Müdahale Ekibi'ne (SOME) bildirilir. Siber Olaylara Müdahale Ekibi, bu güvenlik ihlallerinin gelecekte tekrar oluşmaması ve kısa zamanda çözümlenmesi için gerekli tedbirleri alır veya ilgili paydaşları yönlendirerek gerekli tedbirlerin alınmasını sağlar.
c) Bilgi güvenliği ihlal olaylarına müdahale Bilgi Güvenliği Olay Yönetimi Prosedürü'ne göre gerçekleştirilir.
ç) Bilgi güvenliği ihlal olaylarının analizi ve çözümlemesinden kazanılan bilgi birikimi kullanılarak, gelecekteki ihlal olaylarının gerçekleşme olasılığını veya etkilerini azaltmak için gerekli aksiyonlar alınır.

4.14 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları

a) Tüm kritik sistemler için, İş-Etki Analizi ve Risk Değerlendirmesi gerçekleştirilir.
b) Kriz ve felaket gibi olumsuz durumlarda bilgi güvenliği ve bilgi güvenliği yönetimi sürekliliğinin sağlanması için iş sürekliliği ve felaket kurtarma için planlama çalışmaları yapılır. Bu çalışmaların uygulanabilirliği ve yeterliliği düzenli olarak test edilir ve raporlanır.
c) Oluşturulan kurtarma ve süreklilik planları, iş-etki analizi sonucunda çıkan ihtiyaçları karşılayacak şekilde geliştirilir.

4.15 Uyum

a) Yasal, meşru, düzenleyici veya sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek adına gerekli özel kontroller ve bireysel sorumlulukları karşılayan gereksinimler yazılı olarak saklanır ve güncelliği takip edilir.
b) Fikri mülkiyet hakları ve tescilli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalardan doğan gereksinimlere uyum sağlamak için Büyükşehir Belediyesi'nin onaylamadığı ve lisanssız yazılımlar kullanılmaz.
c) Bilgi güvenliğinin kurumsal politika ve prosedürler uyarınca gerçekleştirilmesini ve yürütülmesini sağlayabilmek için düzenli olarak bilgi güvenliği bağımsız bir şekilde gözden geçirilir.
ç) Büyükşehir Belediyesi, T.C. Devleti kanunlarının tanımladığı tüm yasal hükümlere uymak zorunda olup, hiçbir Büyükşehir Belediyesi çalışanı, T.C. Devleti'nin kabul ettiği bilgi güvenliği ile ilgili ulusal ve uluslararası kanunların dışındaki bir aktivitede bulunamaz.

d) BGYS kapsamında Bilgi Güvenliği Risk Analizi gerçekleştirilir ve tespit edilen risklere yönelik gerekli önlemler alınır. Bu çalışma yılda en az bir defa bütünsel olmak üzere, önemli değişiklikler sonrasında da sadece değişiklik kapsamı için tekrar yapılır.

5 Yaptırım

Çalışanların yukarıda belirtilen hususlara uymamaları halinde, haklarında Büyükşehir Belediyesi Disiplin Esaslarında düzenlenen disiplin cezaları uygulanır.

6 İlgili Dokümanlar

No	Doküman	Kodu
1	Güvenli Sistem ve Yazılım Geliştirme Prosedürü	EBB-PR-02
2	Bilgi Güvenliği Olay Yönetim Prosedürü	EBB-PR-03
3	Kabul Edilebilir Kullanım Politikası	EBB-POL-04
4	Varlık Yönetimi ve Sınıflandırma Politikası	EBB-POL-05
5	Erişim Denetimi Prosedürü	EBB-PR-04
6	Fiziksel Güvenlik Politikası	EBB-POL-06