T.C.
ESKİŞEHİR
ODUNPAZARI BELEDİYESİ
BİLİŞİM SİSTEMLERİ KULLANIM VE BİLGİ GÜVENLİĞİ YÖNERGESİ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönergenin amacı; Odunpazarı Belediyesi bünyesinde bulunan tüm bilişim sistemlerinin, ağ altyapısının, donanım, yazılım, güvenli elektronik imza (e-imza), kurumsal sabit ve mobil iletişim hatları, toplu SMS servisleri ve bilgi varlıklarının güvenli, etkin, verimli ve ilgili mevzuata uygun olarak kullanılmasını sağlamak; bilgi güvenliği risklerini en aza indirmek ve kullanıcıların yetki ile sorumluluklarını belirlemektir.

Kapsam ve kapsam dışı sistemler

MADDE 2- (1) Bu Yönerge; Odunpazarı Belediyesi'nin tüm birimlerini, tam veya yarı zamanlı çalışan tüm personelini (memur, sözleşmeli personel, işçi, şirket personeli), stajyerleri ve belediye bilişim sistemlerine fiziksel veya uzaktan erişim sağlayan dış kaynaklı hizmet sağlayıcıları (yüklenici, danışman vb.) kapsar.

(2) Görev ve Sorumluluk Bakımından Kapsam Dışı Sistemler ve Süreçler:

a) Belediyenin kurumsal resmi web sitesinin (www.odunpazari.bel.tr) içerik yönetimi, güncellenmesi, yayın politikası ve idari sorumluluğu Basın, Yayın ve Halkla İlişkiler Müdürlüğüne aittir. Ancak, kurumsal iş süreçlerine ve vatandaş hizmetlerine yönelik oluşturulan alt alan adları (ebelediye.odunpazari.bel.tr vb.) ile bu adreslerde çalışan kurumsal web uygulamalarının teknik altyapı ve güvenlik sorumluluğu Bilgi İşlem Müdürlüğündedir.

b) Belediye hizmet binaları, tesisler ve sahadaki güvenlik kamera sistemleri (CCTV) ile telsiz haberleşme sistemlerinin kurulum, işletim, bakım, onarım ve kayıt yönetimi süreçleri Bilgi İşlem Müdürlüğünün görev ve sorumluluk alanı dışındadır. (Kamera sistemlerinin sadece kurumsal yerel ağ üzerinden yaptığı veri trafiği ve ağ port güvenliği Bilgi İşlem Müdürlüğü tarafından denetlenir.)

c) Birimlerin kullanımında bulunan bilgisayar, monitör, masaüstü yazıcı ve benzeri son kullanıcı bilişim ekipmanlarının Taşınır Mal Yönetmeliği kapsamındaki demirbaş kaydı, takibi, personele zimmetlenmesi ve müdürlükler arası devir işlemleri Bilgi İşlem Müdürlüğünün görev alanı dışında olup ilgili harcama biriminin (Müdürlüğün) sorumluluğundadır.

Dayanak

MADDE 3- (1) Bu yönergenin hazırlanması ve yönergedeki hükümlerin uygulanması ile ilgili yasal dayanaklar şunlardır;

a) 5393 sayılı Belediye Kanunu,

b) 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu ile Taşınır Mal Yönetmeliği,

c) 7545 sayılı Siber Güvenlik Kanunu ve 177 sayılı Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi,

ç) 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve 5490 sayılı Nüfus Hizmetleri Kanunu (KPS mevzuatı),

d) 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve 5809 sayılı Elektronik Haberleşme Kanunu,

e) 5070 sayılı Elektronik İmza Kanunu,

f) 5846 sayılı Fikir ve Sanat Eserleri Kanunu,

g) 6100 sayılı Hukuk Muhakemeleri Kanunu (HMK Madde 193),

ğ) 2019/12 sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve T.C. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı "Bilgi ve İletişim Güvenliği Rehberi",

h) Odunpazarı Belediyesi Bilgi İşlem Müdürlüğü Görev ve Çalışma Yönetmeliği.

Tanımlar

MADDE 4- (1) Bu Yönergede geçen;

a) Belediye: T.C. Odunpazarı Belediyesini,

b) Başkanlık: Odunpazarı Belediye Başkanlığını,

c) Müdürlük: Odunpazarı Belediyesi Bilgi İşlem Müdürlüğünü,

ç) Bilişim Sistemleri: Kapsam dışı tutulan sistemler (telsiz, güvenlik kameraları vb.) hariç olmak üzere; Belediye bünyesindeki tüm sunucular, bilgisayarlar, mobil cihazlar, telefon santralleri ve sabit/IP telefonlar, kurumsal mobil hatlar (Ses, Data, M2M), toplu SMS servisleri, e-imza donanımları, ağ cihazları, yazıcılar, veri depolama üniteleri, işletim sistemleri, kurum içi geliştirilen veya dışarıdan temin edilen kurumsal yazılımlar (EBYS, MIS/ERP, CBS/GIS, CAD, portal ve iş takip yazılımları vb.), e-posta sistemleri ve internet altyapısını,

d) Bilgi Varlığı: Belediye faaliyetlerinin yürütülmesi esnasında üretilen, işlenen, depolanan ve paylaşılan her türlü basılı veya dijital veriyi,

e) E-İmza (Güvenli Elektronik İmza): 5070 sayılı Kanun kapsamında elle atılan (ıslak) imza ile aynı hukuki sonucu doğuran, Nitelikli Elektronik Sertifika (akıllı SIM kart) ve kart okuyucu donanımdan oluşan elektronik veriyi,

f) Kullanıcı: Belediye bilişim sistemlerine erişim yetkisi verilmiş veya kendisine kurumsal bilişim/iletişim ekipmanı, e-imza ve hattı tahsis edilmiş tüm gerçek veya tüzel kişileri,

g) KVKK: 6698 sayılı Kişisel Verilerin Korunması Kanununu,

ğ) M2M (Makineden Makineye İletişim) Hatları: Araç takip sistemleri, saha otomasyonları, akıllı sayaçlar, POS cihazları, güvenlik/kamera üniteleri gibi cihazlar arası veri iletişimi sağlamak amacıyla kullanılan SIM kartları ve abonelikleri,

h) USOM / SOME: Ulusal Siber Olaylara Müdahale Merkezi ve Kurumsal Siber Olaylara Müdahale Ekibini ifade eder.

İKİNCİ BÖLÜM
Genel İlkeler, Yetki ve Sorumluluklar

Genel ilkeler

MADDE 5- (1) Belediyeye ait tüm bilişim sistemleri, sabit ve mobil iletişim hatları, toplu SMS sistemleri ve bilgi varlıkları Odunpazarı Belediyesi'nin mülkiyetindedir ve sadece kurumsal faaliyetlerin yürütülmesi amacıyla kullanılır; özel işler, ticari faaliyetler, siyasi propaganda veya kişisel reklam amaçlı çalışmalarda kesinlikle kullanılmamaktadır.

(2) Bilgi güvenliği; bilginin Gizlilik (yetkisiz erişimlerin engellenmesi), Bütünlük (bilginin doğruluğunun ve tamlığının korunması) ve Erişilebilirlik (yetkili kişilerin ihtiyaç duyduğunda bilgiye ulaşabilmesi) ilkeleri çerçevesinde sağlanır.

(3) "En Az Yetki" ve "Bilmesi Gerektiği Kadar" prensipleri esastır. Kullanıcılara sadece görevlerini yerine getirmeleri için gereken asgari düzeyde erişim yetkisi verilir.

Bilgi İşlem Müdürlüğünün yetki ve sorumlulukları

MADDE 6- (1) Görev alanı kapsamındaki belediye bilişim ve iletişim altyapısını (sunucu, ağ, telefon santrali, kurumsal yazılımlar vb.) kurmak, geliştirmek, işletmek, güncel tutmak ve güvenliğini sağlamak,

(2) 5651 sayılı Kanun kapsamında internet erişim kayıtlarını (log) tutmak ve zaman damgası ile imzalayarak yasal süresince saklamak,

(3) Kurumsal verilerin periyodik yedeklemesini yapmak ve felaket kurtarma senaryolarını hazırlamak.

(4) Siber güvenlik önlemlerini (Güvenlik Duvarı, Antivirüs/EDR, Saldırı Tespit/Önleme Sistemleri vb.) almak, USOM bildirimlerini takip etmek, sistemleri izlemek ve siber olaylara müdahale etmek,

(5) odunpazari.bel.tr alan adının (domain) DNS yönetimini yapmak ve Bilgi İşlem Müdürlüğü sorumluluğundaki alt alan adlarının (ebelediye.odunpazari.bel.tr vb.) barındırma, işletim ve güvenliğini sağlamak,

(6) Bu yönergeye aykırı hareket eden veya sistem güvenliğini tehlikeye atan kullanıcıların erişimlerini veya tahsis edilen mobil hatlarını geçici olarak askıya almak ve durumu ilgili birim amirine / Başkanlığa raporlamak müdürlüğüm yetki ve sorumluluklarıdır.

Birim müdürlüklerinin ve kullanıcıların sorumlulukları

MADDE 7- (1) Birim Müdürleri, kendi birimlerinde görev yapan personelin bu yönerge kurallarına uymasından ve personel görev hareketlerinin (işe giriş, işten ayrılış, emeklilik, müdürlük veya birim değişikliği) yetkisiz erişimlerin ve kamu zararının önüne geçilmesi amacıyla derhal ve EBYS üzerinden resmi yazı ile Bilgi İşlem Müdürlüğüne bildirilmesinden sorumludur.

(2) Başka bir müdürlüğün görev ve sorumluluğunda bulunan özel sistemlerin (resmi web sitesi www.odunpazari.bel.tr içerik ve yönetimi, güvenlik kameraları, telsiz sistemleri vb.) işletilmesi, güvenliği, yedeklenmesi ve 6698 sayılı KVKK dahil ilgili mevzuata uygunluğunun sağlanması ilgili birim müdürlüklerinin sorumluluğundadır.

(3) Birim Müdürlükleri; kendi birimlerinde bulunan bilgisayar, tablet, monitör ve masaüstü (kişisel kullanıma tahsis edilmiş) yazıcı gibi bilişim donanımlarının demirbaş takibini ve zimmet işlemlerini yürütmekle yükümlüdür. Cihazlara özgü yetkilendirmelerin, ağ (network) erişimlerinin, Active Directory (Etki Alanı) oturum açma izinlerinin ve müdürlük bazlı bilgisayar isimlendirmelerinin yeniden düzenlenebilmesi ve yetkisiz erişimlerin önlenebilmesi amacıyla; cihazların kullanıcı değişiklikleri veya müdürlükler/birimler arası devir işlemleri eş zamanlı olarak Bilgi İşlem Müdürlüğüne bildirilmek zorundadır.

(4) Kullanıcılar, kendilerine tahsis edilen donanım, yazılım, e-imza, kurumsal iletişim hatları (Sabit/IP telefon, Ses, Data, M2M), toplu SMS hesapları ve kullanıcı hesaplarının güvenliğinden ve amacına uygun kullanımından doğrudan sorumludur.

(5) Kullanıcılar, bilgi güvenliği ihlallerini, yetki aşımı durumlarını, e-imza/SIM kart/cihaz kayıplarını veya şüpheli durumları derhal Bilgi İşlem Müdürlüğüne bildirmekle yükümlüdür.

ÜÇÜNCÜ BÖLÜM
Talep Yönetimi, Kullanıcı Hesapları, Active Directory, Parola, E-İmza ve Erişim Yönetimi

Talep yönetimi, satın alma ve yetkilendirme usulleri

MADDE 8- (1) Teknik Destek ve İş Takip Sistemi: Bilgi İşlem Müdürlüğünden talep edilecek tüm rutin teknik destek, arıza, bakım, parola sıfırlama, mevcut lisans havuzundan standart yazılım kurulumu ve güncelleme işlemleri kurumsal İş Takip Programı üzerinden yapılır. Telefonla veya şifahen yapılan talepler işleme alınmaz. Kullanıcının kendi bilgisayarına erişemediği durumlarda

(donanım arızası, ağ bağlantısı kesintisi, parolanın unutulması/hesabın kilitlenmesi vb.), İş Takip talepleri kullanıcının bizzat kendisi tarafından mobil uygulama üzerinden veya görev yaptığı birimdeki diğer personeller/birim amiri aracılığıyla oluşturulabilir.

(2) EBYS Üzerinden Yapılması Zorunlu Talepler: Maliyet ve satın alma gerektiren donanım/yazılım/lisans/e-imza/mobil hat talepleri ile her türlü kullanıcı hesap açılışı, toplu SMS ve sistem yetkilendirme taleplerinin Elektronik Belge Yönetim Sistemi (EBYS) üzerinden resmi yazı ile yapılması zorunludur.

(3) Satın Alma ve Hat/E-İmza Tahsis Talepleri: Donanım, yazılım, bilişim ekipmanı, e-imza veya kurumsal mobil hat (Ses, Veri, M2M) taleplerinde; talep edilen ürünün/hattın hangi personel (adı, unvanı, görev tanımı) veya cihaz için istendiği, hangi kurumsal iş ve işlemleri yerine getirmek amacıyla kullanılacağı veya ekonomik ömrünü tamamlayarak hurdaya (HEK) ayrılan/arızalanan hangi demirbaş/seri numaralı cihazın ikamesi olarak talep edildiği gibi gerekçelerin EBYS yazısında açık ve net bir şekilde belirtilmesi şarttır.

(4) Yetkilendirme Esasları ve Denetim: Active Directory (Etki Alanı), EBYS, kurumsal otomasyon, veritabanı, toplu SMS, kurumsal bulut ve dosya sunucuları dahil olmak üzere tüm sistemler için yetki tanımlamaları sadece EBYS üzerinden gelen resmi talep yazısı ile yapılır. Bu resmi yazılar; KVKK, Sayıştay, iç ve dış bilgi güvenliği denetimleri ile adli/idari soruşturmalarda ibraz edilmek üzere kayıt altında tutulduğundan; yazışmalarda anlam karmaşası yaşanmaması ve bürokrasiyi azaltmak amacıyla, talep yazısı yazılmadan önce ilgili Bilgi İşlem personeli ile görüşülerek talep metninin içeriği konusunda mutabık kalınması esastır.

(5) Mevcut Yetkilerin Durumu ve Görev Devri:

a) Bir personel için yeni yetki talep edildiğinde, personelin üzerindeki mevcut yetkilerin korunup korunmayacağı veya hangi yetkilerin kapatılacağı (son durum) yazıda açıkça belirtilmelidir. Sadece "aşağıdaki yetkilerin verilmesi" şeklinde yapılan ve mevcut yetkilerin durumu belirtilmeyen taleplerde, güvenlik ilkesi gereği personelin önceki yetkileri kaldırılarak sadece yeni talep edilen yetkiler tanımlanır.

b) Müdürlük bünyesinde bir göreve yeni bir personel getirildiğinde ve kendisi için yetki talep edildiğinde, o görevi daha önce yürüten eski personelin yetkilerinin kaldırılması da aynı yazıda açıkça talep edilmelidir. Aksi takdirde eski görevlinin yetkileri kendiliğinden kaldırılmaz ve bu durumdan doğacak yetkisiz erişim sorumluluğu ilgili Birim Müdürlüğüne aittir.

(6) İşten Ayrılma, Emeklilik ve Müdürlük Değişikliği:

a) Emeklilik, istifa, görevden ayrılma veya müdürlük/birim değişikliği durumlarında ilgili müdürlük (veya İnsan Kaynakları ve Eğitim Müdürlüğü / ilgili şirket yönetimi), yetkisiz erişimlerin önüne geçmek adına durumu derhal EBYS üzerinden Bilgi İşlem Müdürlüğüne bildirir; varsa personelin üzerindeki kurumsal mobil hatların (SIM kartların) ve e-imza kart okuyucu donanımlarının Bilgi İşlem Müdürlüğüne iadesini veya devrini sağlar.

b) Emeklilik, işten ayrılma veya müdürlük değişikliği bildirimlerinde personelin tüm sistemlerdeki mevcut erişim yetkileri derhal kapatılır. Yetkiler kapatıldıktan sonra "yarım kalan işlerin tamamlanması, eski evraklara erişilmesi" gibi gerekçelerle yapılacak geçici erişim talepleri şifahen kabul edilmez; bu durumlar için ilgili müdürlük tarafından gerekçesi belirtilerek EBYS üzerinden yeniden resmi yetki talebinde bulunulması zorunludur.

c) Müdürlük değiştiren personelin yeni görev yerindeki sistem ve ağ yetkilendirmeleri, eski müdürlüğü tarafından değil, yeni başladığı müdürlük tarafından EBYS üzerinden talep edilmelidir.

(7) Tekil Hesap ve KPS/İletişim Bilgileri: Her kullanıcıya sadece kendisinin kullanacağı tekil bir kullanıcı hesabı tanımlanır, ortak hesap açılamaz. Kullanıcılara kendi bilgisayarlarında "Yerel Yönetici" (Local Admin) yetkisi verilmez. Kullanıcı hesaplarının tanımlanması, Kimlik Paylaşımı Sistemi (KPS) entegrasyonlu yazılımlarda kimlik doğrulaması yapılabilmesi ve kurumsal e-posta

parola sıfırlama/kurtarma işlemlerinin yürütülebilmesi için personelden T.C. Kimlik Numarası, doğum tarihi, cep telefonu ve kişisel e-posta adresi bilgileri talep edilir. Kullanıcının cep telefonu numarası veya iletişim bilgileri değiştiğinde, görev yaptığı müdürlük tarafından Bilgi İşlem Müdürlüğüne bilgilendirme yapılması zorunludur.
(8) Cihaz Yetkilendirmeleri, Ağ Erişimleri ve Bilgisayar İsimlendirmeleri: Kurumsal bilişim cihazlarının (bilgisayar, tablet vb.) ağ (network) erişim kuralları, cihaza özgü sistem yetkilendirmeleri ile Active Directory (Etki Alanı) üzerindeki müdürlük esaslı bilgisayar isimlendirmeleri ve oturum açma izinleri cihazın kayıtlı olduğu birime ve kullanıcıya göre yapılandırılır. Müdürlükler veya birimler arası personel ya da cihaz değişikliklerinde Bilgi İşlem Müdürlüğüne bilgi verilmemesi nedeniyle yaşanacak ağ erişim kısıtlamalarından, oturum açamama sorunlarından, yetki uyuşmazlıklarından ve cihaza tanımlı özel izinler sebebiyle oluşabilecek yetkisiz erişim ile veri güvenliği ihlallerinden ilgili birim ve kullanıcı sorumludur.
(9) Yetki Aşımı Bildirim Yükümlülüğü: Personel; sistemsel bir hata, yazılım açığı veya hatalı yetkilendirme neticesinde kendi görevi ve yetki alanı dışındaki verilere veya ekranlara erişebildiğini fark ettiği anda, bu verileri incelemeksizin, kaydetmeksizin ve paylaşmaksızın durumu derhal bağlı olduğu birim amirliği aracılığıyla EBYS üzerinden Bilgi İşlem Müdürlüğüne bildirmekle yükümlüdür.

Genel parola güvenliği ilkeleri
MADDE 9- (1) Kurumsal yazılım ve sistemlerde (Active Directory özel kuralları saklı kalmak kaydıyla) kullanılan tüm kullanıcı parolaları en az 8 (tercihen 12) karakter uzunluğunda olmalı; sistemin desteklediği ölçüde büyük harf, küçük harf, rakam ve özel karakter içermelidir.
(2) Parolalar ardışık sayılar veya kolay tahmin edilebilir kişisel bilgiler (doğum tarihi, isim-soyisim vb.) içermemelidir.
(3) Parolalar en fazla 90 günde bir değiştirilmelidir.
(4) Parolalar kişiye özeldir; hiçbir koşulda çalışma arkadaşları veya yöneticiler dahil üçüncü kişilerle paylaşılamaz, kağıda yazılarak masa/monitör üzerine yapıştırılamaz. Başka bir personelin kullanıcı adı ve parolası ile sisteme girmek veya giriş denemesinde bulunmak kesinlikle yasaktır.
(5) Kullanıcı hesabı ile yapılan tüm işlemlerden ilgili personelin kendisi sorumludur.

Active Directory (etki alanı) kullanım, oturum ve parola politikaları
MADDE 10- (1) Kullanıcı Adı Standardı ve İsim Değişikliği: Active Directory (AD) kullanıcı hesap adları ad.soyad standardında oluşturulur. Birden fazla isim veya soyisim bulunması halinde, ilk isim veya soyismin baş harfi diğer isim/soyisimle birleşik olacak şekilde tanımlama yapılır. Evlilik, mahkeme kararı vb. nedenlerle personelin ad veya soyadında değişiklik olması durumunda; kullanıcı adının güncellenebilmesi için İnsan Kaynakları ve Eğitim Müdürlüğü veya Odunpazarı A.Ş. tarafından Bilgi İşlem Müdürlüğüne bilgilendirme yapılmalıdır.
(2) Müdürlük Bazlı ve Ortak Bilgisayarlarda Oturum Açma: Kullanıcılar yalnızca kendi görev yaptıkları müdürlük envanterindeki bilgisayarlarda oturum açabilirler. Birden fazla müdürlük personelinin ortak kullandığı bilgisayarlar için; cihazın demirbaşının kayıtlı olduğu müdürlük, o bilgisayarda oturum açmasına izin verilecek diğer müdürlüklerin kullanıcı personelini EBYS üzerinden Bilgi İşlem Müdürlüğüne bildirir.
(3) Mesai Saatleri Oturum Kısıtlaması: Kullanıcılar, varsayılan olarak sadece hafta içi mesai günlerinde 07:00-19:00 saatleri arasında oturum açabilecek şekilde yapılandırılır. Mesai saatleri dışında (özellikle hafta sonu) çalışması gereken kullanıcı ve bilgisayar bilgileri, ilgili birim tarafından bir önceki mesai günü öğlen saat 12:00'ye kadar Bilgi İşlem Müdürlüğüne bildirilmelidir.
(4) Otomatik Oturum Kilitleme: Bilgisayarlarda 15 dakika boyunca hiçbir işlem yapılmadığında

bilgisayardaki açık oturum sistem tarafından otomatik olarak kilitlenir.
(5) İşletim Sistemi ve Grup İlkesi (GPO) Kısıtlamaları: Bilgisayarlardaki Windows işletim sistemlerinde kullanıcılar; Denetim Masası, kayıt defteri (Registry), yazılım kurma ve kaldırma, Çalıştır menüsü, komut satırı uygulaması (CMD/PowerShell), saat ve tarih değişimi, bölgesel ayarlar vb. bazı uygulamaları güvenlik gerekçesi ile kullanamazlar. Bilgi İşlem Müdürlüğü bu uygulamalarda değişiklik yapabilir; bu ayarlamalar kişiye özel değiştirilemez.
(6) Active Directory Parola Politikası ve Sıfırlama Süreci: Active Directory (Etki Alanı) ve AD kimlik doğrulaması ile çalışan sistemlerde aşağıdaki özel parola kuralları uygulanır:

a) Karakter Uzunluğu: Kullanıcı bilişim ağına giriş parolası standart kullanıcılarda en az 10 karakter (büyük-küçük harf, rakam ve alfanümerik/özel karakter karışık), kurum ana bilgisayarlarına (sunucu, veri tabanı ve kritik sistemlere) erişimi olan ayrıcalıklı kullanıcılarda ise en az 14 karakter olmalıdır.

b) Değişim Süresi ve Parola Geçmişi: Kullanıcı parolaları 90 gün sonunda değişime zorlanır ve sürenin dolmasına 7 gün kala oturum açma anında kullanıcıya bilgilendirme mesajı çıkar. Kullanıcı daha önce kullandığı son 5 şifresini tekrar kullanamaz.

c) Hesap Kilitlenmesi: Parola bilgisi 5 kez üst üste yanlış girilirse kullanıcı hesabı kilitlenir. Yanlış giriş sayısı 4 olduğunda, hesabın kilitlenmemesi için 15 dakika geçmeden tekrar parola denemesi yapılmamalıdır.

ç) Parola Sıfırlama ve SMS Bildirimi: Parolasını hatırlamayan ya da hesabını kilitleyen kullanıcı için Madde 8/1'de belirtilen usulle İş Takip Programı üzerinden Bilgi İşlem Müdürlüğüne parola sıfırlama talebi iletilir. Kullanıcı, sistemde kayıtlı cep telefonuna gelen SMS içeriğinde yazan geçici parola bilgisi ile sisteme giriş yapar; güvenlik gereği SMS içeriğinde kullanıcı adı bilgisi yer almaz.
(7) Kimlik İlişkisi ve İz Kayıtları (Log): Kullanıcı; Active Directory (AD) ve AD ile ilişkili tüm sistemlerde oturum açabilmek için kendisine tahsis edilen kullanıcı adı ve parola ikilisinin T.C. Kimlik Numarası ve cep telefonu kaydı ile ilişkili olduğunu, bilişim ağındaki ve bu sistemlerdeki kullanımının gerektiğinde yetkili mercilere teslim edilmek üzere iz kayıtlarının (log) tutulabileceğini bilir ve kabul eder.
(8) Etki Alanına (Domain) Dâhil Edilmeyen Bilgisayarlar: Teknik gereksinimler veya özel iş süreçleri nedeniyle Active Directory (Etki Alanı) yapısına dâhil edilmeyen bilgisayarlar; Belediyenin yerel kurumsal iç ağına (LAN), sunucularına ve veri tabanlarına doğrudan erişemeyecek şekilde izole edilir ve internete yalnızca kontrollü hotspot (izole misafir ağı) üzerinden çıkartılır. Bu cihazların internet erişim logları da 5651 sayılı Kanun kapsamında kayıt altına alınır.

Güvenli elektronik imza (e-imza) tahsisi, kullanımı ve iadesi
MADDE 11- (1) Temin ve Tahsis: EBYS ve diğer resmi iş süreçlerinde kullanılmak üzere personelin ihtiyaç duyduğu Güvenli Elektronik İmza (Nitelikli Elektronik Sertifika / Akıllı SIM Kart ve Kart Okuyucu Donanım), ilgili müdürlüğün EBYS üzerinden resmi talebi doğrultusunda Bilgi İşlem Müdürlüğü tarafından temin edilerek personele tahsis ve zimmet edilir.
(2) Güvenlik ve Hukuki Sorumluluk: 5070 sayılı Elektronik İmza Kanunu uyarınca güvenli elektronik imza, elle atılan (ıslak) imza ile aynı hukuki sonucu doğurur. E-imza donanımının (kart ve okuyucu) muhafazası ile PIN/PUK şifrelerinin gizliliği tamamen personelin şahsi sorumluluğundadır. E-imza ve şifresinin ast-üst ilişkisi veya vekâlet dahil hiçbir gerekçeyle üçüncü kişilerle paylaşılmaması esastır; paylaşılması veya cihazın bilgisayarda takılı ve unutulmuş bırakılması sonucu yapılacak her türlü işlemden sertifika sahibi personel doğrudan sorumludur. E-imza aracını kaybeden veya çaldıran personel, sertifikanın yetkisiz kişilerce kullanımını engellemek amacıyla derhal Bilgi İşlem Müdürlüğüne bilgi vermekle yükümlüdür.
(3) Kullanıcı Kusuru, Kamu Zararı ve Yenileme Ücreti: Sertifika kullanım süresi devam ettiği halde;

personelin kendi kasıt, kusur, ihmal veya dikkatsizliği nedeniyle e-imza SIM kartının veya kart okuyucu donanımın kaybolması, çalınması, kırılması, sıvı teması/fiziksel hasar görmesi ya da PIN/PUK kodlarının tamamen bloke edilerek kartın kullanılamaz hale gelmesi durumlarında; 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun 71. maddesi (Kamu Zararı) ve 657 sayılı Kanun'un 12. maddesi hükümleri gereğince, yeni e-imza sertifikası ve/veya kart okuyucu donanım temini için oluşacak yenileme bedeli ilgili personelden tahsil edilir (veya yenileme bedeli personel tarafından karşılanır).

(4) Emeklilik ve Kurumdan Ayrılma Durumunda İade Süreci: Emeklilik, istifa, nakil veya görevden ayrılma gibi nedenlerle belediyedeki görevi sona eren personelden, kuruma ait demirbaş niteliğindeki kart okuyucu donanım (USB Token / Akıllı Kart Okuyucu) tutanak karşılığında eksiksiz ve çalışır vaziyette Bilgi İşlem Müdürlüğü tarafından geri teslim alınır. Ancak, Nitelikli Elektronik Sertifika (akıllı SIM kart) kişiye özel üretilmiş olduğundan ve personelin farklı bir kurumda veya bireysel işlemlerinde kullanmaya devam edebilmesi sebebiyle personelden geri alınmaz ve sertifika iptal edilmez. (Sadece personelin belediye EBYS ve kurumsal sistemlerindeki imza/erişim yetkileri kapatılır.

Uzaktan erişim

MADDE 12- (1) Belediye dışından kurumsal ağa erişim (VPN vb.) sadece iş gereksinimleri doğrultusunda, ilgili Birim Müdürünün EBYS üzerinden resmi talebi ve Bilgi İşlem Müdürlüğünün onayı ile sağlanır.

(2) Uzaktan erişimlerde Çok Faktörlü Kimlik Doğrulama (MFA/2FA) kullanılması zorunludur.

DÖRDÜNCÜ BÖLÜM
Donanım, İletişim Hatları, Yazılım, İnternet, E-Posta ve Toplu SMS Kullanımı

Donanım, zimmet/devir, yer değişikliği ve taşınabilir medya kullanımı

MADDE 13- (1) Kullanıcılara zimmetlenen bilişim ve iletişim ekipmanları (bilgisayar, monitör, masaüstü yazıcı, tablet, sabit/IP telefon vb.) özenle kullanılmalı, donanımların kasaları açılmamalı ve fiziksel müdahalede bulunulmamalı, arıza durumunda İş Takip Programı üzerinden Bilgi İşlem Müdürlüğüne bildirim yapılmalıdır.

(2) Bilgisayar, monitör, tablet ve masaüstü (kişisel kullanıma tahsis edilmiş) yazıcıların demirbaş takibi, personele zimmetlenmesi ve müdürlükler arası devir işlemleri ilgili müdürlükler (harcama birimleri) tarafından yürütülür. Ancak; cihazlara (bilgisayar, tablet vb.) özgü sistem yetkilendirmelerinin, ağ (network) erişimlerinin, Active Directory (Etki Alanı) üzerindeki müdürlük bazlı bilgisayar isimlendirmelerinin ve oturum açma izinlerinin ilgili cihaza/birime göre yeniden düzenlenebilmesi ve önceki kullanımdan kalan ayrıcalıklar sebebiyle yetkisiz erişimlerin oluşmaması için, yapılan tüm zimmet değişimi ve müdürlükler/birimler arası donanım devir işlemlerinde Bilgi İşlem Müdürlüğüne derhal bilgi verilmesi zorunludur. Sistem tarafından müdürlük standardına göre verilen bilgisayar adları (Computer Name) müdahale edilerek değiştirilemez.

(3) Bilgisayarların Yer Değişikliği Yasağı ve Görevden Ayrılışta Cihaz Teslimi/Formatlama:

a) Bilgisayarlarda ve çevre birimlerinde herhangi bir sebep ile izinsiz yer değişikliği yapılamaz. Zorunlu durumlarda gerekçesi ile beraber Bilgi İşlem Müdürlüğüne EBYS üzerinden bilgilendirme yapılmalıdır. Kullanıcılar görev yeri veya birim değişikliği sebebi ile kullanmakta oldukları masaüstü bilgisayarları yanlarında götüremezler; cihaz demirbaşın kayıtlı olduğu birimde kalır. Kullanıcının yeni görev yerindeki bilgisayarda oturum açabilmesi ve ağ/sistem erişimlerinin düzenlenebilmesi için Bilgi İşlem Müdürlüğüne EBYS üzerinden bilgilendirme yapılması şarttır.

b) İstifa, emeklilik, kurum değişikliği veya görevden ayrılma hallerinde personel; kendisine

zimmetlenmiş olan tüm bilişim donanımlarını (bilgisayar, tablet, çevre birimleri vb.) demirbaşın kayıtlı olduğu kendi birimine (İlgili Müdürlük Taşınır Kayıt Yetkilisine) eksiksiz ve çalışır vaziyette tutanakla teslim etmek zorundadır. İlgili birim, teslim alınan bilgisayar veya taşınabilir cihazı başka bir personele tahsis etmeden önce, cihazın teknik kontrolü ve önceki kullanıcıya ait verilerin temizlenmesi/işletim sistemi formatlaması için İş Takip Programı üzerinden Bilgi İşlem Müdürlüğünden talepte bulunmakla yükümlüdür.
(4) Mesai bitiminde veya bilgisayar başından ayrılmalarda oturum kilitlenmeli (Win + L), mesai sonunda bilgisayarlar kapatılmalıdır (güncelleme veya yedekleme planlamaları hariç).
(5) Temiz Masa ve Temiz Ekran İlkeleri: Çalışma masalarında gizli veya kişisel veri içeren evraklar açıkta bırakılmamalı, bilgisayar ekranları yetkisiz kişilerin göremeyeceği şekilde konumlandırılmalıdır.
(6) USB Port Kısıtlaması ve Veri Aktarımı: Güvenlik politikaları gereği kurumsal bilgisayarların USB depolama giriş portları kapalı tutulur. Dış ortamla veri alışverişi için kullanıcılar yalnızca kurumsal e-posta sistemini ya da Bilgi İşlem Müdürlüğü tarafından sağlanan kurumsal bulut/dosya paylaşım yazılımını kullanabilirler.

Kurumsal mobil hatların (ses, veri ve M2M) ve sabit telefonların tahsisi ve kullanımı
MADDE 14- (1) Tahsis, Zimmet ve Cihaz Temini: Kurumsal faaliyetlerin yürütülmesi amacıyla personele veya otomasyon/saha sistemlerine tahsis edilecek Ses, Mobil Veri (Data) ve M2M (Makineden Makineye İletişim) hatları, ilgili müdürlüğün EBYS üzerinden gerekçeli talebi ve üst yönetim onayı ile Bilgi İşlem Müdürlüğü tarafından temin edilir. Bilgi İşlem Müdürlüğü tarafından ses veya mobil veri hatları ile birlikte cep telefonu donanımı tahsis edilmez; sadece SIM kart (abonelik) ve/veya kurumsal ihtiyaç halinde hücresel bağlantılı tablet tahsisi gerçekleştirilir. Tahsis edilen tüm SIM kartlar tutanak/taahhütname ile ilgili personele zimmetlenir ve SIM kartın takıldığı kişisel veya birim bütçesiyle temin edilmiş cihazların donanımsal arıza, bakım ve güvenliğinden Bilgi İşlem Müdürlüğü sorumlu değildir.
(2) M2M (Cihaz) Hatlarının Yönetimi ve Sorumluluğu: Araç takip sistemleri, uzaktan sulama/aydınlatma otomasyonları, POS cihazları, saha kameraları veya ölçüm cihazları gibi ekipmanlarda kullanılan M2M hatlarının; ilgili müdürlük bünyesinde sorumlu bir personele zimmetlenmesi ve hattın takılı olduğu cihaz bilgilerinin (araç plakası, cihaz seri numarası, kurulum lokasyonu ve kullanım amacı) Bilgi İşlem Müdürlüğüne bildirilmesi zorunludur. M2M SIM kartları, tanımlandığı saha/otomasyon ekipmanı dışında başka hiçbir cihaza (cep telefonu, tablet, taşınabilir modem vb.) kesinlikle takılamaz. M2M hattının takılı olduğu cihazın arızalanması, hurdaya ayrılması, yerinin değişmesi veya hizmetin sona ermesi durumunda, atıl abonelik ve kamu zararı oluşmaması için ilgili müdürlük derhal EBYS üzerinden Bilgi İşlem Müdürlüğüne bildirimde bulunarak hattın iptalini veya devrini talep etmekle yükümlüdür.
(3) Amacına Uygun Kullanım, Kişisel Hotspot Yasağı ve Yasal Sorumluluk: Tahsis edilen sabit/IP telefonlar ile kurumsal ses, veri (data) ve M2M hatları yalnızca belediye iş ve işlemlerinde kullanılabilir; üçüncü kişilere devredilemez, ödünç verilemez ve kullandırılamaz. Tahsis edilen kurumsal SIM kartlar, görevin gerektirdiği meşru kamu işleri dışında kişisel internet paylaşımına (hotspot/tethering) dönüştürülerek kurum dışı cihazların kontrolsüz veri tüketimine açılamaz. Kurumsal mobil hatlar üzerinden gerçekleştirilen her türlü iletişim, veri trafiği, internet erişimi ve paylaşımlardan 5651 sayılı Kanun, 5809 sayılı Kanun ve Türk Ceza Kanunu kapsamında hattın zimmetli olduğu personel doğrudan sorumludur.
(4) Paket Limitleri, Fatura Aşımı ve Mali Sorumluluk: Kurumsal hatlar, tanımlanan tarife ve kota sınırları dahilinde kullanılır ve uluslararası (yurt dışı) aramalara kapalı tutulur. Resmi görevlendirmeler ve kurumsal onaylar haricinde; yurt dışı dolaşım (roaming) kullanımları, katma

değerli özel ücretli servis numaraları (yarışma, şans oyunları, eğlence, bağış servisleri vb.), mobil ödeme işlemleri, toplu/spam SMS gönderimleri veya kişisel kullanım kaynaklı oluşan her türlü tarife/paket aşım bedeli ve ek vergiler ilgili personelden (veya zamanında bildirim yapmayan ilgili birim sorumlusundan) tahsil (rücu) edilir.
(5) Kayıp, Çalıntı ve Görevden Ayrılma: SIM kartın (veya SIM kartın takılı olduğu cihazın) kaybolması ya da çalınması halinde, hattın derhal iletişime kapatılması/dondurulması ve olası maddi/hukuki zararların önlenmesi için durum vakit kaybetmeksizin (önce şifahen/İş Takip üzerinden, akabinde derhal EBYS ile) Bilgi İşlem Müdürlüğüne bildirilmelidir. Bildirim yapılmamasından doğacak tüm mali ve hukuki sorumluluk kullanıcıya aittir. İşten ayrılma, emeklilik, ücretsiz izin veya birim değişikliği durumlarında personele zimmetli kurumsal SIM kartlar tutanakla doğrudan Bilgi İşlem Müdürlüğüne iade edilir veya yeni sorumlu personele resmi yazı ile devredilir.

Yazılım kullanımı, güncellemeler ve lisanslama
MADDE 15- (1) Belediye bilgisayarlarına Bilgi İşlem Müdürlüğünün bilgisi ve onayı dışında hiçbir yazılım, oyun, eklenti veya uygulama kurulamaz.
(2) 5846 sayılı Fikir ve Sanat Eserleri Kanunu uyarınca, belediye sistemlerinde lisanssız (korsan / kırılmış) yazılım bulundurulması ve kullanılması kesinlikle yasaktır. Tespit edilmesi halinde hukuki ve cezai sorumluluk ilgili kullanıcıya aittir.
(3) Merkezi Güncelleme, Güvenlik Ajanları ve Uzaktan Kurulum: Bilgi İşlem Müdürlüğü; kurumsal siber güvenliği sağlamak amacıyla bilgisayarlara uzaktan bağlantı sağlama, merkezi antivirüs/EDR (Uç Nokta Tehdit Algılama ve Yanıt) ajanları yükleme, periyodik tarama yapma, işletim sistemi ve yazılım güvenlik yamalarını otomatik dağıtma, uzaktan program kurulumu, masaüstüne kısayol ekleme ve sistem ilkelerini güncelleme yetkisine sahiptir. Bu güvenlik mekanizmaları ve ajan yazılımlar hiçbir surette personel tarafından kapatılamaz veya devre dışı bırakılamaz.

İnternet kullanımı ve yasaklanan faaliyetler
MADDE 16- (1) Belediye internet altyapısı kurumsal işlerin yürütülmesi amacıyla tahsis edilmiştir.
(2) İnternet erişimleri 5651 sayılı Kanun gereğince kayıt altına alınmakta ve içerik filtreleme sistemleri ile denetlenmektedir.
(3) Kullanılan erişim yöntemine bakılmaksızın (kablolu yerel ağ, kablosuz/hotspot veya kurumsal mobil veri hatları dâhil) kurumsal ağ üzerinden;
a) Türk Ceza Kanunu ve 5651 sayılı Kanun uyarınca suç teşkil eden (yasa dışı bahis, kumar, terör propagandası, müstehcenlik, şiddet veya nefret söylemi içeren) sitelere girilmesi, bu tür içeriklerin indirilmesi, barındırılması veya yayılması,
b) Telif hakları mevzuatına aykırı biçimde müzik, film, oyun veya lisanssız yazılım indirilmesi, paylaşılması veya Torrent/P2P dosya paylaşım araçlarının kullanılması,
c) Güvenlik duvarını ve filtreleme sistemlerini aşmaya yönelik yazılımların (Proxy, VPN eklentileri vb.) kullanılması,
ç) Kurum içi veya kurum dışı ağlarda dinleme (sniffing), yetki yükseltme, parola kırma, güvenlik açığı tarama (port tarama vb.) veya ağ trafiğini aksatıcı saldırı araçlarının çalıştırılması,
d) Sistemlere ve kurumsal ağa zararlı yazılımların (virüs, fidye yazılımı vb.) bulaşmasına zemin hazırlayacak güvenli olmayan internet sitelerine girilmesi, kesinlikle yasaktır.
(4) Misafirlerin ve etki alanına (domain) dâhil edilmeyen izole cihazların internet erişimi, kurumsal yerel ağdan (LAN) tamamen izole edilmiş özel "Misafir Ağı / Kontrollü Hotspot" üzerinden kimlik doğrulaması yapılarak sağlanır ve 5651 sayılı Kanun kapsamında kayıt altına alınır.

Kurumsal e-posta ve toplu SMS kullanımı

MADDE 17- (1) @odunpazari.bel.tr uzantılı kurumsal e-posta adresleri ve kurumsal Toplu SMS servisleri sadece resmi ve kurumsal iletişim/bilgilendirme amacıyla kullanılır.

(2) Kurumsal e-posta adresi ve Toplu SMS altyapısı; kişisel sosyal medya hesapları, alışveriş siteleri, forumlar, kurum dışı özel abonelikler veya zincirleme mesaj, spam, siyasi propaganda, kişisel reklam/tanıtım ve özel kutlama gönderimleri için kullanılamaz.

(3) Toplu SMS Yetkilendirmesi ve Sorumluluk: Kurumsal Toplu SMS arayüzü veya yazılım entegrasyonları üzerinden mesaj gönderim yetkisi, ilgili müdürlüğün EBYS üzerinden resmi talebi ile tanımlanır. Toplu SMS gönderimlerinde 6698 sayılı KVKK hükümlerine uyulmasından ve gönderilen mesaj içeriğinin hukuki/idari doğruluğundan doğrudan gönderimi yapan kullanıcı ve ilgili birim müdürlüğü sorumludur.

(4) Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ve Bilgi ve İletişim Güvenliği Rehberi uyarınca, kurumsal gizlilik içeren verilerin ve resmi yazışmaların yerli olmayan (Gmail, Hotmail, Yahoo vb.) harici e-posta servisleri veya mesajlaşma uygulamaları (WhatsApp vb.) üzerinden paylaşılması yasaktır.

(5) Kullanıcılar, kimlik avı (phishing / oltalama) saldırılarına karşı dikkatli olmalı; tanımadıkları kişilerden gelen şüpheli e-postaları ve eklerini açmadan Bilgi İşlem Müdürlüğüne bildirmelidir.

BEŞİNCİ BÖLÜM
Kişisel Verilerin Korunması, Yedekleme ve Sistem Güvenliği

Kişisel verilerin korunması (KVKK) ve gizlilik

MADDE 18- (1) Kullanıcılar; görevleri gereği erişilen ve işlenen vatandaşlara, mükelleflere veya personele ait kişisel verileri, nüfus/adres kayıtlarını, tapu/mülkiyet bilgilerini, mali verileri ve kurumsal sırları 6698 sayılı KVKK, 5490 sayılı Nüfus Hizmetleri Kanunu (KPS), Vergi Usul Kanunu ve ilgili gizlilik mevzuatına uygun olarak işlemek, saklamak ve yetkisiz kişilerle, sosyal medyada veya harici platformlarda paylaşmamakla yükümlüdür. Bu gizlilik ve sır saklama yükümlülüğü, personelin belediyedeki görevi sona erdikten sonra da süresiz olarak devam eder.

(2) Kişisel veri içeren dosyalar, yetkisiz erişime açık ortak ağ klasörlerinde veya masaüstünde şifresiz olarak bulundurulmamalıdır.

(3) Kurumsal verilerin izinsiz harici bulut depolama servislerine (Google Drive, Dropbox, WeTransfer vb.) yüklenmesi yasaktır. Büyük boyutlu dosya paylaşımları için Bilgi İşlem Müdürlüğü tarafından sağlanan kurumsal bulut/dosya paylaşım altyapısı kullanılır.

Veri yedekleme ve şahsi verilerin sorumluluğu

MADDE 19- (1) Merkezi sunucularda, veri tabanlarında ve kurumsal yazılımlarda bulunan verilerin periyodik yedeklemesi Bilgi İşlem Müdürlüğü tarafından yapılır.

(2) Kullanıcıların kendi masaüstü veya dizüstü bilgisayarlarının yerel disklerinde (C:, D: sürücüleri, Masaüstü vb.) tuttukları verilerin yedekleme sorumluluğu kullanıcıya aittir. Kurumsal öneme sahip dosyaların merkezi dosya sunucularında (File Server) veya kurumsal bulut sisteminde kendilerine tahsis edilen alanlarda saklanması zorunludur.

(3) Kurumsal bilişim cihazlarında, ağ depolama alanlarında veya kurumsal e-posta hesaplarında kullanıcıların kendilerine veya yakınlarına ait şahsi veri, özel fotoğraf, video, müzik, kişisel belge veya finansal döküman bulundurması yasaktır. Bu kurala aykırı olarak kurumsal sistemlerde barındırılan şahsi verilerin; donanım arızası, bakım/onarım, formatlama, sistem sıfırlama, siber saldırı (fidye yazılımı vb.) nedeniyle silinmesi, kaybolması, zarar görmesi ya da teknik müdahale ve denetimler esnasında üçüncü kişilerce görülmesi/erişilmesi durumlarından Odunpazarı Belediyesi ve

Bilgi İşlem Müdürlüğü hiçbir şekilde sorumlu tutulamaz.

Veri merkezi (sistem odası) ve fiziksel güvenlik
MADDE 20- (1) Bilgi İşlem Müdürlüğüne bağlı Sistem Odası (Veri Merkezi) ve katlardaki sistem kabinetleri yüksek güvenlikli alanlardır.
(2) Sistem odasına sadece yetkilendirilmiş Bilgi İşlem personeli girebilir. Bakım veya onarım amacıyla gelen dış firma personeli, yalnızca yetkili Bilgi İşlem personeli refakatinde içeri alınır.
(3) Sistem odasında iklimlendirme, kesintisiz güç kaynağı (UPS), yangın algılama/söndürme ve 7/24 kamera izleme sistemleri çalışır durumda tutulur.

Siber olaylara müdahale
MADDE 21- (1) Kullanıcılar; bilgisayarlarında anormal bir yavaşlama, fidye yazılımı (ransomware) uyarısı, izinsiz erişim şüphesi veya virüs bulaşması gibi durumlarda bilgisayarı kapatmadan derhal ağ kablosunu çekmeli (veya Wi-Fi bağlantısını kesmeli) ve vakit kaybetmeden Bilgi İşlem Müdürlüğüne haber vermelidir.

ALTINCI BÖLÜM
Denetim, İz Kayıtları (Log), İhlal ve Yaptırımlar

Denetim, izleme, log yönetimi, delil niteliği ve sorumluluk reddi
MADDE 22- (1) İki Kademeli Denetim Esası: Kurumsal bilişim sistemlerinin ve donanımlarının denetimi iki kademeli olarak yürütülür:

a) Teknik Denetim: Bilgi İşlem Müdürlüğü tarafından yürütülür. Odunpazarı Belediyesi, bilgi güvenliğini sağlamak, yasal yükümlülükleri yerine getirmek, maliyetleri kontrol altında tutmak ve sistem performansını korumak amacıyla; bilişim sistemleri üzerindeki tüm trafikleri, e-posta ve toplu SMS iletişimini, internet erişimlerini, kurumsal mobil hat (Ses, Veri, M2M) kota ve kullanım detaylarını, e-imza süreçlerini ve kullanıcı aktivitelerini izleme, kaydetme ve denetleme hakkını saklı tutar. Kullanıcılar, kurumsal sistemlerde ve hatlarda kişisel gizlilik beklentisi içinde olamazlar.

b) İdari ve Taşınır Denetimi: Birim Müdürleri ve harcama birimi taşınır kayıt yetkilileri; kendi birimlerindeki personelin bilişim donanımlarını, kurumsal hatları ve e-imza araçlarını amaca uygun, verimli ve bu Yönergeye uygun kullanıp kullanmadığını, demirbaş zimmetlerinin usulüne uygun tutulup tutulmadığını denetlemekle ve tespit edilen usulsüzlükleri derhal Bilgi İşlem Müdürlüğüne ve Başkanlık Makamına bildirmekle yükümlüdür.

(2) Log Yönetimi ve Yasal Delil Niteliği: 5651 ve 5809 sayılı Kanunlar uyarınca; kullanıcıların kablolu yerel ağ (LAN), kablosuz misafir ağları (hotspot) ve kurumsal mobil hatlar üzerinden gerçekleştirdikleri tüm internet erişimleri, ziyaret ettikleri adresler, oturum saatleri ve sistem hareketleri zaman damgalı olarak kayıt altına (log) alınır. Kullanıcı kimliği; T.C. Kimlik Numarası, tahsisli bilgisayar adı, kurumsal mobil hat ve IP/MAC adresi ile eşleştirilmiş durumdadır. Bu kayıtlar yasal yükümlülükler gereği yetkili adli ve idari mercilere sunulmak üzere mevzuatta öngörülen süreler boyunca saklanır. Söz konusu zaman damgalı iz kayıtları; 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 193. maddesi uyarınca bağlayıcı yasal delil (delil sözleşmesi) niteliğinde olup idari soruşturma, disiplin kovuşturması ve adli süreçlerde taraflar nezdinde münhasır ve muteber delil teşkil eder.

(3) Teknik Müdahale ve Sorumluluk Reddi: Bilgi İşlem Müdürlüğü, teknik destek, arıza giderme, sistem bakımı veya güvenlik taraması amacıyla kullanıcı bilgisayarlarına önceden haber vermeksizin uzaktan veya fiziksel olarak müdahale edebilir, disk sıfırlama (format) işlemi uygulayabilir. Bu işlemler sırasında cihazda izinsiz olarak bulundurulan şahsi dosyaların silinmesinden veya ifşa olmasından dolayı kurum ve Müdürlük hiçbir hukuki, idari veya mali mesuliyet kabul etmez

Yönerge ihlalleri ve yaptırımlar
MADDE 23- (1) Bu Yönergede belirtilen kurallara uyulmaması, güvenlik önlemlerinin devre dışı bırakılmaya çalışılması veya kurumsal bilişim ve iletişim kaynaklarının kötüye kullanılması durumunda; ihlalin niteliğine göre ilgili personel hakkında 657 sayılı Devlet Memurları Kanunu, 4857 sayılı İş Kanunu, Toplu İş Sözleşmesi hükümleri ve ilgili diğer mevzuat uyarınca idari ve disiplin işlemleri uygulanır.
(2) İhlalin aynı zamanda Türk Ceza Kanunu, 7545 sayılı Siber Güvenlik Kanunu veya ilgili diğer kanunlar kapsamında suç teşkil etmesi halinde, Başkanlık Makamı onayıyla adli mercilere suç duyurusunda bulunulur ve kasıt, kusur veya ihmal neticesinde kurumun uğradığı doğrudan ve dolaylı tüm maddi/manevi zararlar ile 5018 sayılı Kanun kapsamında oluşan kamu zararları (paket aşım ücretleri, e-imza yenileme bedelleri, idari para cezaları vb. dahil) ilgili personelden tazmin (rücu) edilir.

YEDİNCİ BÖLÜM
Çeşitli Hükümler, Yükümlülükler, Yürürlük ve Yürütme

Taahhütname ve erişim ön şartı
MADDE 24- (1) Tüm belediye personeli ve sistemlere erişim sağlayacak üçüncü taraf çalışanları, bu Yönergeyi okuduğunu, anladığını ve kurallara uyacağını belirten "Personel Bilişim Sistemleri Kullanım ve Bilgi Güvenliği Taahhütnamesi"ni (Ek-1) imzalamakla yükümlüdür. Ek-1 Taahhütnamesini imzalamayan hiçbir kullanıcıya belediye bilişim sistemlerinde kullanıcı hesabı ve erişim yetkisi tanımlanamaz; bilgisayar, e-imza veya kurumsal mobil hat tahsis edilemez. İmzalanan taahhütnameler Bilgi İşlem Müdürlüğü tarafından fiziksel veya elektronik ortamda muhafaza edilir.

Güncelleme ve gözden geçirme
MADDE 25- (1) Bu Yönerge, gelişen teknolojiler, yeni siber tehditler ve değişen yasal mevzuatlar doğrultusunda Bilgi İşlem Müdürlüğü tarafından yılda en az bir kez gözden geçirilir ve gerekirse güncellenerek Başkanlık Olur'una sunulur.

Yürürlükten kaldırılan hükümler
MADDE 26- (1) Bu Yönergenin yürürlüğe girmesiyle birlikte, Belediye bünyesinde daha önce yürürlükte olan bilişim sistemleri, Active Directory ve bilgisayar kullanımına dair tüm eski yönerge, politika, düzenleme ve ilkeler yürürlükten kalkar.

Yürürlük
MADDE 27- (1) Bu Yönerge, Belediye Başkanı tarafından imzalandıktan sonra Odunpazarı Belediyesi'nin www.odunpazari.bel.tr kurumsal internet adresinde yayınlandığı tarihte yürürlüğe girer.

Yürütme
MADDE 28- (1) 28 (yirmi sekiz) maddeden oluşan bu Yönerge Odunpazarı Belediye Başkanı tarafından yürütülür.

ONAY
20.12.2026
Av. Kazım KURT
Belediye Başkanı

EK-1: PERSONEL BİLİŞİM SİSTEMLERİ KULLANIM VE BİLGİ GÜVENLİĞİ TAAHHÜTNAMESİ

T.C.

ODUNPAZARI BELEDİYE BAŞKANLIĞINA

Odunpazarı Belediyesi bünyesinde yürüttüğüm görevim süresince ve görevim sona erdikten sonra;

1. "Odunpazarı Belediyesi Bilişim Sistemleri Kullanım ve Bilgi Güvenliği Yönergesi"ni okuduğumu, anladığımı ve bu yönergede belirtilen tüm kurallara eksiksiz uyacağımı; kurumsal bilişim ve iletişim kaynaklarını şahsi, ticari veya siyasi amaçlarla kullanmayacağımı,

2. İşbu taahhütnamenin imza bloğunda beyan ettiğim ve şahsıma tahsis edilen Active Directory (AD) kullanıcı adı (isim.soyisim), kullanıcı kodu, parola, Güvenli Elektronik İmza (E-İmza) ve diğer erişim bilgilerini gizli tutacağımı, amirlerim dâhil hiçbir gerekçeyle üçüncü kişilerle paylaşmayacağımı; Active Directory (AD) ve AD ile ilişkili/entegre tüm sistemlerde oturum açabilmek için kullanılan bu kullanıcı adının T.C. Kimlik Numaram, cep telefonu kaydım, bilgisayar adım ve IP/MAC adresim ile doğrudan yasal zeminde eşleştirildiğini bildiğimi; bilişim ağındaki ve bu sistemlerdeki kullanımımın gerektiğinde yetkili mercilere teslim edilmek üzere zaman damgalı iz kayıtlarının (log) tutulabileceğini ve bu kayıtların 6100 sayılı HMK Madde 193 uyarınca münhasır ve bağlayıcı yasal delil teşkil ettiğini kabul ettiğimi; bu kullanıcı adı ve hesabım/e-imzam üzerinden yapılan tüm iş ve işlemlerin hukuki, idari ve cezai sorumluluğunun bizzat şahsıma ait olduğunu; kusurum, ihmalim veya dikkatsizliğim nedeniyle (kaybolma, kırılma, çalınma, PIN/PUK bloke olması vb.) kullanılamaz hale gelen e-imza kartı ve/veya kart okuyucu donanımın yenileme ücretini 5018 ve 657 sayılı Kanunlar uyarınca kamu zararı doğmaması adına ödeyeceğimi; emeklilik veya kurumdan ayrılmam durumunda kuruma ait e-imza kart okuyucu donanımı (USB Token) Bilgi İşlem Müdürlüğüne sağlam olarak tutanakla iade edeceğimi (kişiye özel üretilen e-imza SIM kartının ise iade alınmayacağını ve iptal edilmeyeceğini bildiğimi),

3. Tarafıma zimmetlenen bilişim donanımlarını (bilgisayar, tablet, çevre birimleri vb.) ve kurumsal yazılımları sadece belediye iş ve işlemleri için kullanacağımı, Bilgi İşlem Müdürlüğünün onayı olmadan bilgisayarıma hiçbir lisanssız yazılım veya donanım kurmayacağımı, kasa açma/parça değiştirme gibi fiziksel müdahalede bulunmayacağımı, merkezi olarak kurulan anti virüs/EDR güvenlik ajanlarını hiçbir surette kapatmayacağımı veya devre dışı bırakmayacağımı; görev yeri veya birim değişikliği sebebiyle kullanmakta olduğum masaüstü bilgisayarı yanımda götürmeyeceğimi ve bilgisayarlarda izinsiz yer değişikliği yapmayacağımı; görevden ayrılmam halinde zimmetli bilişim donanımlarını kendi birimimin Taşınır Kayıt Yetkilisine eksiksiz teslim edeceğimi; bilgisayar, tablet, monitör ve masaüstü (kişisel kullanıma tahsis edilmiş) yazıcı gibi donanımların zimmet veya birim/kullanıcı değişikliği durumlarında cihaza özgü sistem yetkilendirmelerinin, ağ (network) erişimlerinin, Active Directory (Etki Alanı) oturum açma izinlerinin ve bilgisayar isimlendirmelerinin yeniden düzenlenebilmesi ve yetkisiz erişimlerin önlenebilmesi için Bilgi İşlem Müdürlüğüne bilgi verilmesi gerektiğini; ayrıca kurumsal bilgisayarlarda, depolama alanlarında veya e-posta hesabında şahsıma ait özel veri/dosya (fotoğraf, belge vb.) bulundurmayacağımı, bulundurmam halinde donanım arızası, bakım, formatlama veya siber saldırı gibi nedenlerle bu verilerin silinmesi, kaybolması ya da teknik müdahale/denetim esnasında görülmesi durumlarından Odunpazarı Belediyesi ve Bilgi İşlem Müdürlüğünün hiçbir sorumluluk kabul etmeyeceğini bildiğimi,

4. Kurumsal internet, @odunpazari.bel.tr uzantılı e-posta hesabımı ve (varsa) kurumsal Toplu SMS gönderim yetkimi yasalara ve kurumsal ilkelere aykırı amaçlarla (spam, siyasi propaganda, kişisel reklam vb.) kullanmayacağımı, 5651 sayılı Kanun kapsamında internet erişimlerimin kayıt altına alındığını ve kurumsal sistemlerde kişisel gizlilik beklentisi içinde

olamayacağımı bildiğimi,

5. Tarafıma veya sorumluluğumdaki sistemlere tahsis ve zimmet edilen kurumsal iletişim hatlarını (Sabit/IP telefon, Ses, Mobil Veri/Data ve M2M SIM kartlarını) yalnızca kurumsal görev ve hizmetlerin yürütülmesi amacıyla kullanacağımı; SIM kartı hiçbir şekilde üçüncü kişilere kullandırmayacağımı, görevin gerektirdiği meşru kamu işleri dışında kişisel internet paylaşımına (hotspot/tethering) açmayacağımı ve M2M (cihaz/otomasyon) hatlarını tanımlandığı saha ekipmanı dışında şahsi telefon, tablet veya modem gibi başka bir cihaza takmayacağımı; hat üzerinden yapılan tüm iletişim ve veri trafiğinin hukuki/cezai sorumluluğunun şahsıma ait olduğunu; kişisel kullanım, yurt dışı arama/dolaşım (roaming), katma değerli özel ücretli servisler veya mobil ödeme nedeniyle oluşacak her türlü tarife/paket aşım bedelini ödeyeceğimi; SIM kartın (veya takılı olduğu cihazın) kaybolması, çalınması, hurdaya ayrılması ya da görev yerimin değişmesi/işten ayrılmam durumlarında derhal Bilgi İşlem Müdürlüğüne bildirimde bulunarak kurumsal SIM kartı doğrudan Bilgi İşlem Müdürlüğüne tutanakla iade/devir edeceğimi,

6. Görevim gereği eriştiğim vatandaş/mükellef bilgilerini, personel kayıtlarını, nüfus/adres, tapu ve mali veriler ile kurumsal sırları 6698 sayılı KVKK, 5490 sayılı Kanun ve Vergi Usul Kanunu kapsamında koruyacağımı, yetkisiz kişilerle veya sosyal medyada paylaşmayacağımı, kurum dışına çıkarmayacağımı ve kişisel çıkarlarım için kullanmayacağımı; bu sır saklama yükümlülüğümün görevimden ayrıldıktan sonra da süresiz olarak devam edeceğini; sistemsel bir hata veya hatalı yetkilendirme sonucu görev ve yetki alanım dışındaki verilere erişebildiğini fark ettiğimde bu verileri incelemeksizin ve kaydetmeksizin derhal birim amirime ve Bilgi İşlem Müdürlüğüne bildireceğimi,

7. Herhangi bir bilgi güvenliği ihlali veya siber saldırı şüphesi fark ettiğimde derhal Bilgi İşlem Müdürlüğüne bilgi vereceğimi,

8. Kurumsal yazılım ve sistemlerde (Active Directory, EBYS, MIS/ERP vb.) kullanıcı hesaplarımın tanımlanması, Kimlik Paylaşımı Sistemi (KPS) entegrasyonları üzerinden kimlik doğrulaması yapılabilmesi ve kurumsal hesap/e-posta parola sıfırlama işlemlerinin yürütülebilmesi amacıyla aşağıda beyan ettiğim Active Directory (AD) Kullanıcı Adı, Doğum Tarihi, Cep Telefonu ve Kişisel E-Posta Adresi bilgilerimin 6698 sayılı KVKK kapsamında Bilgi İşlem Müdürlüğü tarafından işlenmesini kabul ettiğimi ve bu bilgilerde değişiklik olması halinde güncel bilgileri derhal bildireceğimi,

9. Yukarıda belirtilen hususlara ve Yönerge hükümlerine aykırı hareket etmem durumunda doğacak her türlü idari, mali (kamu zararı rücu işlemleri dâhil) ve cezai sorumluluğu kabul ettiğimi

beyan ve taahhüt ederim.

Tarih: ..... / ..... / 202..

- **Adı Soyadı:** .....
- **Active Directory (AD) Kullanıcı Adı (ad.soyad):** .....
- **T.C. Kimlik No / Sicil No:** .....
- **Doğum Tarihi (Gün/Ay/Yıl):** ..... / ..... / .....
- **Görev Yaptığı Müdürlük:** .....
- **Ünvanı:** .....
- **Cep Telefonu:** 0 (5.....) ....
- **Kişisel E-Posta Adresi (Şifre Sıfırlama İçin):** .....
- **Tahsis Edilen Kurumsal Hat / M2M No (Varsa):** .....
- **İmza:** .....