

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

1. AMAÇ

İşbu Kişisel Verilerin Korunması Uyum Süreci Politikası (“**Politika**”), Kayseri Develi Belediye Başkanlığı (“**Develi Belediyesi**”) nezdinde gerçekleştirilen veri işleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun (“**Kanun**”) ilgili hükümleri uyarınca hukuka uygun şekilde yerine getirilmesi ve Kanun’un 12 inci maddesi kapsamında kişisel verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla hazırlanmıştır.

2. KAPSAM VE SORUMLULUKLAR

Bu politika elektronik veya fiziki ortamda Develi Belediyesi bilgi ve belgeleri ile bilgi sistem hizmeti erişimine izin verilmiş olan tüm memur ve personelleri kapsamaktadır. Politika’nın uygulanması ve revizyonundan KVKK Komisyonu sorumludur. Develi Belediyesi nezdindeki tüm kullanıcılar, bu Politikada yer alan uygulamaları bilmek ve belirtilen kurallara uymakla yükümlüdür.

3. TANIMLAR

| | |
|-------------------------------------|--|
| 5651 sayılı Kanun | İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun |
| 6698 sayılı Kanun | 6698 sayılı Kişisel Verilerin Korunması Kanunu |
| Develi Belediyesi / Belediye | Kayseri Develi Belediye Başkanlığı |
| Güvenlik Duvarı (Firewall) | Güvenlik duvarı kurulduğu sisteme gelen ve giden ağ trafiğini kontrol ederek yetkisiz veya istenmeyen yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanım |
| Kişisel Veri | Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi |
| Kişisel Verilerin İşlenmesi | Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem |
| Özel Nitelikli Kişisel Veri | Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, |

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

| | |
|----------------------------------|---|
| | vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler |
| Politika | İşbu Kişisel Verilerin Korunması Uyum Süreci Politikası |
| Sunucu (Server) | Bilgisayar ağlarında, diğer ağ bileşenlerinin (kullanıcıların) erişebileceği, kullanımına ve/veya paylaşımına açık kaynakları barındıran bilgisayar birimi |
| Veri İşleyen | Veri sorumlusunun vermiş olduğu yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişi |
| Veri Sahibi / İlgili Kişi | Kişisel verisi işlenen gerçek kişi |
| Veri Sorumlusu | Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi |
| VPN | Belediye dışında da Belediye ağına bağlanılmak üzere kullanılan sanal özel ağ |

4. İÇERİK

İşbu Politika kapsamında Develi Belediyesi nezdinde gerçekleştirilen faaliyetlerin 6698 sayılı Kanun'a uygun şekilde uygulanması amacıyla birçok prosedüre yer verilmiştir. İçerikte yer alan diğer politikalara ait dokümantasyon listesi EK-1 de yer almaktadır.

Develi Belediyesi nezdinde kullanılan bilgi ve haberleşme sistemleri ve donanımları (internet, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, taşınabilir cihazlar ve cep telefonları da dahil olmak üzere) Develi Belediyesi işlerinin yürütülmesi için kullanılmalıdır. Bu sistemlerin yasa dışı, rahatsız edici, Develi Belediyesi'nin diğer kural ve standartlarına aykırı veya Develi Belediyesi'ne zarar verecek herhangi bir şekilde kullanımı bu Politikanın ihlal edildiği anlamına gelecektir.

Develi Belediyesi, bu sistemleri ve bu sistemlerle gerçekleştirilen aktiviteleri izleme, kaydetme ve periyodik olarak denetleme hakkını saklı tutmaktadır.

Develi Belediyesi, nezdinde bulunan taraflar ile ihtiyaç ve beklentilerin hangi yöntem veya araç ile ortaya konulduğu, bu ihtiyaç ve beklentilerden hangilerinin uyum yükümlülüğü olduğu ve tarafların iletişim metodu aşağıdaki tabloda gösterilmiştir.



KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI

Doküman No: 1

Yayın Tarihi: 23/03/2022

Revizyon No/Tarih: 00/-

| | İlgili taraflar | İlgili taraf ile beklentilerin belirlendiği araç / yöntem | İletişim Metodu |
|-------------------------|--|--|--|
| Birinci Taraflar | Memur ve Personeller | Kişisel verilerin korunması, görev ve talimatların belirlenmesi, sürekli eğitim ve etkinliklerin artırılması, eğitim katılımlarının değerlendirilmesi, takdir, objektif ve şeffaf performans değerlendirmesi, mesai ve dinlenme saatlerine yasal uyumluluk, sağlıklı ve temiz bir çalışma ortamı | E-posta, telefon, yüz yüze görüşme, Belediye içi toplantılar |
| | Üst Yönetim | Yasal ve mevzuat şartlarına tam uyum, memur ve personellerin görev ve sorumluluklarına riayet edilmesi, politikalara uyum | |
| | Yükleniciler / Doğrudan Temin ile Hizmet Alınan Gerçek veya Tüzel Kişiler | Develi Belediyesi çalışma alanlarının güvenliğinin sağlanması, Develi Belediyesi'nin taahhütlerine uyması, sürekli iletişim sağlanması, sağlıklı geri beslemelerin alınabilmesi, beklentilerin açık bir şekilde ifade edilmesi | |
| Üçüncü Taraflar | Develi Belediyesi'nin tabi olduğu yasal mevzuatlar gereği herhangi bir iş ilişkisi içerisinde olmaksızın geçici veya sürekli faaliyet kapsamına dahil olan kişiler | Yasal mevzuat şartlarına tam uyum sağlanması, her zaman insanı ve çevreyi korumaya yönelik faaliyetlerde bulunulması, Develi Belediyesi'nin taahhütlerine uyması ve sürekli iletişim sağlanması | Resmi yazışma, e-posta, telefon, yüz yüze görüşme, toplantılar |

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

5. UYGULAMA POLİTİKALARI

5.1. P.01. İNTERNET ERİŞİMİ POLİTİKASI

Amaç

İnternetin uygun olmayan kullanımı, Belediyenin yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenemeyen sonuçlara neden olabilir. İşbu İnternet Erişimi Politikası, Belediye içinde güvenli internet erişimi için sahip olunması gereken standartları belirlemeyi, bilerek veya bilmeyerek bu türden olumsuzluklara neden olunmaması ve internet kurallarına, etiğe ve yasalara uygun kullanımının sağlanmasını amaçlamaktadır.

Kapsam

İnternet Erişimi Politikası Belediye internetini kullanan veya kullanacak olan tüm memur ve personelleri kapsamaktadır. Memur ve personel dışında yapılan bağlantılar için erişim sağlanan internet hizmetine ilişkin Wi-Fi Kullanım Koşulları uygulanacaktır.

Politika

- Belediye bilgisayarları içerik denetimi yapan uygulama üzerinden internete çıkacaktır. Belediye kültürüne ve yasalara uymayan sitelere girilmesi yasaklanmıştır. Ancak Belediye Başkanlık Olur'u ile yetkilendirilmiş Belediye personeline internete çıkarken gerekli servisleri kullanma hakkı tanımlanabilecektir.
- 5651 sayılı Kanun uyarınca Belediye internet erişim kayıtları en az iki yıl arşivlenmektedir.
- Belediye internetinin kullanımı vasıtasıyla bilgisayarlar veya mobil cihazlar üzerinden yasalara aykırı internet sitelerine girilmesi ve dosya indirilmesi yasaktır.
- Başkalarının fikri haklarını ihlal edici materyallerin dağıtımı yasaktır.
- Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Belediye bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer Belediye tarafından bir suç oluşturduğundan şüphe duyulursa Develi Belediyesi İnsan Kaynakları ve Eğitim Müdürlüğü disiplin süreçlerini uygulayabilir veya yasal başvuruları yapabilir.
- İnternet üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ile Belediye'ye ve Belediye memur ve personeline, bunların aile fertlerine ve Türkiye Cumhuriyeti devletine, ulusuna, yasama, yürütme ve yargı organlarına, askeri ve emniyet teşkilatına, vatandaşlarına yönelik iftira, karalama mahiyetinde mesajlar göndermek ve yayınlamak yasaktır.
- Kullanıcıların internet üzerinden görevleri ile ilgisi bulunmayan, internet trafiğini kısıtlayabilecek veya zarar verebilecek online olarak yayın yapan televizyon, radyo, film, oyun vb. içerikli yayınların kullanılması yasaktır.
- Belediye internet kaynakları öncelikli olarak Belediye işlerinin yapılması için kullanılmalıdır. Çalışma saatleri içerisinde uzun süreli olarak iş ile ilgisi olmayan sitelere giriş yapılmamalıdır.
- Belediye e-posta adresi ile internet üzerinde forum, alışveriş vb. sitelere üye olunması yasaktır.
- Kullanıcıların sistemi kullanmak için gerekli kullanıcı adı, parola ve benzeri kişisel bilgilerini başkalarıyla paylaşmaları yasaktır.
- İnternet üzerinde Belediye kritik bilgisinin ortaya çıkmasına veya Belediye servislerinin ulaşılamaz hale gelmesine neden olacak tüm aktiviteler yasaktır.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

- Belediye içerisinde kullanılan kullanıcı adı ve şifreler ile sosyal hayatta kullanılan kullanıcı adı ve şifrelerin aynı olması yasaktır.
- Belediye, internet sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar ve gerektiğinde bu hakkı kullanabilir.
- Belediye, kullanıcının internet sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet birimleriyle veya resmî kurumlar ile kullanıcının izni olmadan paylaşma hakkını saklı tutar.
- İnternet üzerinden yapılan kişisel işlemlerden oluşabilecek olumsuzluklardan Belediye sorumlu değildir. Ayrıca Belediye veya kişisel hesabınızı ele geçiren kişi veya kişiler Belediye memur ve personeli adına suç işleyebilir ve bu işlemde Belediye memur ve personeli sorumludur.
- İnternet üzerinde yapılan gezinmelerde reklam veya bilgi almak amaçlı (tebrikler, ödül kazandınız, ödülünüzü almak için tıklayın vb.) aldatıcı resim ve yazılara karşı dikkatli olunmalı ve tıklanmamalıdır.
- Üçüncü şahısların Belediye internet bağlantısı Hotspot üzerinden gerçekleşmektedir. Belediye memur ve personellerinin internet bağlantı şifresi paylaşması yasaktır.
- Belediye network ağına Belediye dışı cihazların takılması yasaktır.
- Belediye interneti kullanılarak erişim sağlanan whatsapp vb. programlar üzerinden kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyaller ile Belediye ait görsel ve gizli bilgilerin paylaşımı yasaktır.

5.2. P.02. E-POSTA POLİTİKASI

Amaç

Belediye e-postalarının uygun olmayan kullanımı, Belediyenin yasal yükümlülükleri, kapasite kullanımı ve kurumsal imajı açısından istenemeyen sonuçlara neden olabilir. İşbu Politika, Belediye e-posta altyapısına yönelik kuralları ortaya koymaktadır. Belediyeye oluşturulan e-postalar resmi bir kimlik taşımaktadır. E-posta, Develi Belediyesi'nin en önemli iletişim kanallarından birisidir ve gönderilecek tüm e-postalarda Belediye memur ve personellerinin işbu Politika ile belirtilen kurallara uyması gerekmektedir.

Kapsam

E-posta Politikası Belediye e-postasını kullanma yetkisi bulunan tüm memur ve personelleri kapsamaktadır.

Politika

- Belediye e-posta kaynakları öncelikle Belediye işlerinin gerçekleştirilmesi için kullanılmalıdır.
- Belediye memur ve personellerinin Belediye e-postalarından gönderdikleri, aldıkları veya sakladıkları e-postalar Develi Belediyesi'nin bilgi varlığıdır. Bu yüzden yetkili kişiler gerekli durumlarda önceden haber vermeksizin e-posta mesajlarını denetleyebilir veya yasal merciler ile paylaşabilir.
- Memur ve personellerin e-posta adresi isim soyisim olacak şekilde açılmaktadır. Benzer isimlerin olması durumunda e-posta belirleme yöntemlerine göre kurulum işlemi gerçekleştirilir.
- Belediye e-posta kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
- Kullanıcılar kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur. Memur ve personel kendi kullanımı için verilen kullanıcı adını ve şifresini başkaları ile paylaşmamalı, kullanımı için başkasına vermemelidir.
- Kurumsal e-posta hesaplarının kişisel amaçlı kullanımı yasaktır.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

- Kişisel kullanım için internet sitelerine üye olunması durumunda Belediye e-posta adreslerinin kullanılması yasaktır.
- Belediyenin e-posta sistemi taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine veya Bilgi İşlem Müdürlüğü'ne haber verilmesi ve bu mesajın tamamen silinmesi gerekmektedir.
- E-postaların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- Belediye dışına gönderilen tüm e-postalarda aşağıdaki uyarı mesajı bulunmalıdır.

“Bu e-posta ve ekleri gönderilen kişi veya Belediye ile gönderildiği kişi veya Belediyeye ait özel, gizli veya yasak bilgiler içeriyor olabilir. İletinin yetkili muhatabı değilseniz e-posta içeriğinde yer alan gizli bilgileri ve kişisel verileri yetkisiz olarak elinizde bulundurmuş ve işlemiş kabul edileceğinizden iletiyi saklamayınız, kopyalamayınız, kullanmayınız veya iletmeyiniz. Mesajda yer alan bilgilerin üçüncü kişilere ifşa edilmesi etik kuralların ihlali anlamına geleceğinden mesajı ve ekleri gecikmeden yok ediniz, içindeki bilgileri kimseyle paylaşmayınız ve göndereni uyarınız. Develi Belediyesi bu iletinin ve iletinin içeriğinde yer alan bilgi ve kişisel verilerin doğruluğu, bütünlüğü, iletilmesi ve benzeri hususlar konusunda garanti vermemektedir. İleti içeriğinde yer alan kişisel verilerin yetkisiz kullanımı ve işlenmesi sonucu Develi Belediyesi'nin uğrayacağı her türlü zararı talep ve tazmin hakkı saklıdır. Gönderici, elektronik posta aktarımı sırasında meydana gelebilecek hata ve ihmallerden dolayı herhangi bir sorumluluk kabul etmemektedir. Kişisel Verilerin Korunması Kanunu kapsamında Aydınlatma Metinlerimize <https://www.develi.bel.tr/kurumsal/kvkk-hakkinda-aydinlatma-metni> linkinden ulaşabilirsiniz.”

- Zincir mesajlar ve mesajlara iliştilenmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında derhal Bilgi İşlem Müdürlüğü'ne haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemelidir. Spam, zincir e-posta vb. zararlı e-postalara yanıt yazılması yasaktır.
- Kullanıcıların kullanıcı adı/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak herhangi bir işlem yapılmaksızın derhal Bilgi İşlem Müdürlüğü'ne haber verilmeli, posta kutusundan silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Memur ve personeller e-postalarını düzenli olarak kontrol etmeli, gelen e-postalara en geç 7 gün içerisinde cevap vermelidir.
- Memur ve personeller, Belediye e-postalarının Belediye dışındaki kişiler ve yetkisiz kişilerce görülmesini engellemelidir.
- Kurumsal e-posta hesaplarına gelen e-postaların Belediyeye ait olmayan kişisel e-posta hesaplarına yedeklemek veya bilgi amaçlı göndermek yasaktır.
- Belediye adı kullanılarak resmi iletişimlerde kullanılması amacıyla Hotmail, Gmail vb. mail hesaplarının açılması ve kullanılması yasaktır.
- Belediye e-posta kaynakları hiçbir şekilde yasa dışı kullanılamaz ve Belediye çıkarlarıyla çatışamaz, Belediyenin normal operasyon ve iş aktivitelerini engelleyemez.
- Belediye e-posta kaynakları uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.
- Belediyenin e-posta sistemi taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

- Memur ve personeller tarafından geçici veya sürekli haklara sahip olunması durumunda dahi e-posta yazılımının mevcut güvenlik ayarlarının değiştirilmesi yasaktır.
- Kullanıcılar e-posta yazılımının gönderenin kimliğini gizleyecek özelliklerini kullanamazlar.
- Kullanıcılar e-posta yazılımının otomatik mesaj iletme özelliklerini kullanamazlar.
- Belediye, e-posta sistemleri kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar ve gerektiğinde bu hakkı kullanabilir.
- Belediye, kullanıcının e-posta sisteminde gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar.

5.3. P.03. YAZILIM KULLANIM POLİTİKASI

Amaç

İşbu Politika, Belediye nezdinde kullanılan lisanlı yazılımların kullanım amaçlarının belirlenmesi amacıyla oluşturulmuş olup Belediye memur ve personellerinin işbu Politika ile belirtilen kurallara uyması gerekmektedir.

Kapsam

Yazılım Kullanım Politikası Belediye nezdinde mevcut olan herhangi bir yazılımı kullanan veya kullanma yetkisi bulunan tüm memur ve personellerini kapsamaktadır.

Politika

- Kullanıcılar yazılımlarla ilgili tüm telif hakkı yasalarına uymak zorundadırlar.
- Belediye tarafından kullanılan tüm yazılımların lisansları yasal yollardan temin edilmiştir.
- Belediyeye ait yazılımlar kullanılırken ilgili yasa ve düzenlemelere uyulmalıdır.
- Kullanıcıların Bilgi İşlem Müdürlüğü'nün izni olmaksızın mevcut yazılımlar dışında herhangi bir yazılımı yüklemesi veya kullanması yasaktır.
- Standart olarak Belediye bilgisayarlarında kurulan programlar aşağıda belirtilmiştir.
Microsoft Office, Adobe Reader, AntiVirüs yazılımı, Chrome, java, Winrar
- Standartta belirlenmeyen fakat iş yapma amacıyla ihtiyaç olunan yazılımların memur ve personellerinin müdürlük yöneticisi onaylı e-posta yoluyla kurulum talep etmesi ardından Bilgi İşlem Müdürlüğü tarafından yazılımın uygunluğu kontrol edilerek Belediye bilgisayarına yüklenir.
- Belediyeye ait yazılımlar yasa dışı, Belediye politikalarına aykırı ve Belediye çıkarlarına ters düşecek şekilde kullanılamaz.
- Belediyeye ait yazılımların izinsiz çoğaltılması ve kişisel amaçlarla kullanılması yasaktır.
- Belediye haberleşme alt yapısı ticari hiçbir yazılımın izinsiz kopyalanması, gönderilmesi, alınması veya çoğaltılması için kullanılamaz.
- Belediye, kullanıcı bilgisayarlarında yüklü bulunan veya kullanılan yazılımları herhangi bir zamanda kontrol edebilir.
- Belediye, kullanıcının yazılımlar üzerinden gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar ve gereken durumlarda bu hakkı kullanabilir.
- Belediye yetkili personelince tespit edilen ve lisans anlaşmalarına uymayan yazılımlar Bilgi İşlem Müdürlüğü tarafından kaldırılır.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

5.4. P.04. SUNUCU GÜVENLİK POLİTİKASI

Amaç

İşbu Politika, Belediyenin sahip olduğu sunucuların temel güvenlik kurallarının belirlenmesi amacıyla oluşturulmuştur

Kapsam

Sunucu Güvenlik Politikası Belediyenin sahip olduğu tüm sunucuları kapsamaktadır.

Politika

- Belediye bünyesinde bütün sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur.
- Sunucu işletim sistemleri üzerindeki kullanılmayan servisler ve uygulamalar kapatılmalıdır. Port açma talepleri Bilgi İşlem Müdürlüğü e-posta adresine e-mail olarak gönderilmeli ve yapılan talepte portun açık kalma süresi de beyan edilmelidir.
- Kullanılmayan sunucular güvenlik ve elektrik tasarrufu açısından kapalı tutulmalıdır.
- Sunucular üzerinde yapılan işlemlerin log kayıtları en az 2 yıl süre saklanacak şekilde ayarlanmalıdır.
- İşletim sistemleri, uygulamalar, veri tabanları, ağ donanımları yetkili erişim logları tutulmalıdır.
- Sunucuların yönetimi için her yetkili kişi kendi hesabı ile bağlanarak işlem yapmalıdır, domainde olan sunucuların lokal admin hesapları kullanılmamalıdır.
- Sunuculara dışarıdan yapılan bağlantılar uzak bağlantı politikasının belirlediği kurallara göre yapılmalıdır.
- Sunucular fiziksel olarak güvenlik önlemi alınmış sistem odalarında bulundurulmalıdır.
- Sistem odaları sıcaklık, nem değerleri ve su basmasına karşı denetlenmelidir.
- Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt altına alınmalıdır. Sistem odalarına girişler çift güvenlik kontrolü ile yapılmalıdır.
- Sunucu odalarında ekipmanların bakımları düzenli olarak yapılmalı ve bakım kayıtları tutulmalıdır. Sistem odalarında cihazların bakımları yetkili kişiler gözetiminde yapılmalıdır.
- Elektrik ve data kabloları sunucu odaları dahil Belediye içerisinde kanallardan geçmelidir.
- Sunucuların bulunduğu odalar kamera ile kayıt altına alınıp, gerektiğinde izlenebilir olmalıdır. Sunucuların bulunduğu odalara girişler sırasında kamera sistemi otomatik olarak e-mail ile yetkili kişilere fotoğraf göndermelidir.
- Elektrik kesintilerinden sistem odalarındaki sunucu ve diğer ekipmanların etkilenmemesi için UPS sistemine bağlı olması ve jeneratör ile desteklenmesi gerekmektedir.
- Sunucular yılda en az 2 kez zafiyet testinden geçirilmelidir.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

5.5. P.05. MOBİL CİHAZLAR KULLANIM POLİTİKASI

Amaç

İşbu Politika Develi Belediyesi'ne ait bilgi içeren mobil cihazların kullanımı ile ilgili kuralların belirlenmesi amacıyla oluşturulmuştur.

Kapsam

Mobil Cihazlar Kullanım Politikası, Develi Belediyesi mobil cihazlarını kullanan tüm memur ve personelleri kapsamaktadır.

Politika

- Belediyeye ait bilgi içeren tüm taşınabilir cihazlar ilgili kişiye zimmetlenerek teslim edilmelidir.
- Belediye mobil cihazları öncelikli olarak Belediyenin işlerinin gerçekleştirilmesi için kullanılmalıdır.
- Her memur ve personel kendisine zimmetlenen mobil cihazın güvenliğinden ve amacına uygun kullanımından sorumludur.
- Kullanıcıların mobil cihazlara erişim için şifre ya da parmak izi güvenlik sistemi kullanılmalıdır. Şifre konulması için memur ve personellere gerekli bilgilendirme ve hatırlatmalar yapılmalıdır.
- Etki alanı dahilindeki bilgisayarlar admin yetkisi sınırlandırılarak yalnızca user yetkilendirmesi ile ilgili kişiye teslim edilmelidir. Etki alanında bağımsız olan bilgisayarların sorumluluğu memur ve personele aittir.
- Etki alanı dahilindeki bilgisayarlar üzerinde yapılan çalışmalar ve oluşturulan dosyalar Belediye birimlerine ait ve yetki erişimi belirlenmiş olan ortak alanlara kaydedilmelidir.
- Mobil cihazların memur ve personelin aile bireyleri dahil zimmetlenen kişiler dışında kullanılması yasaktır.
- Kaybolması ve çalınması kolay olduğundan mobil cihazlar başıboş bırakılmamalıdır.
- Belediye mobil cihazlarının uygunsuz içeriği saklamak, erişmek, indirmek ve iletmek için kullanılması yasaktır.
- Belediye sabit telefonlarının kullanımı esnasında hoparlörler, ses ve video kayıt cihazları, video konferans ve benzeri cihazlar kullanılmadan önce görüşmede yer alan herkese bildirilmeli ve katılımcılardan izin alınmalıdır.
- Belediyeye ait hassas bilginin yetkisiz kişilerin eline geçebileceği ortamlarda kullanıcılar bu bilgileri tartışmamalıdır.
- Memur ve personeller Belediye için gizli kabul edilebilecek belge ve dokümanları, ofis ortamında görünebilir yerlerde bırakması yasaktır. Yazıcı, faks veya fotokopi makinesinin kullanımlarında veri gizliliğine dikkat edilmelidir.
- Belediye, yazıcı ve faks cihazları kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar.
- Belediye, kullanıcının yazıcı ve faks cihazları ve Belediyeye ait mobil cihazlar ile gerçekleştirdiği aktivitelerle ilgili bilgileri üçüncü partilere, emniyet birimlerine ve yargı makamlarıyla paylaşma hakkı saklıdır.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

5.6. P.06. SABİT VE TAŞINABİLİR BİLGİSAYAR KULLANIM POLİTİKASI

Amaç

İşbu Politika, Belediye nezdinde memur ve personeller tarafından kullanılan sabit ve taşınabilir bilgisayarların kullanımı ile ilgili kuralların belirlenmesi amacıyla oluşturulmuştur.

Kapsam

Sabit ve Taşınabilir Bilgisayar Kullanım Politikası Belediye nezdinde memur ve personel ile sabit ve taşınabilir bilgisayarları kullanım yetkisi bulunan tüm memur ve personelleri kapsamaktadır.

Politika

- Belediye bilgi kaynaklarına uzaktan veya yerel ağ üzerinden erişmek için sadece Belediye envanterinde bulunan onaylanmış sabit ve taşınabilir bilgisayar cihazları kullanılmalıdır.
- Belediyeye ait taşınabilir bilgi işleme cihazları öncelikli olarak Belediye işlerinin gerçekleştirilmesi için kullanılmalıdır.
- Taşınabilir bilgi işleme cihazları gözetimsiz bırakıldıklarında mutlaka fiziksel olarak güvenli bir yerde veya şekilde saklanmalıdır.
- Memur ve personeller sabit ve taşınabilir bilgisayarları Belediye bünyesindeki domain'e bağlı olarak çalıştırmalıdır.
- Tüm bilgisayar sistemi yöneticisinin yetkisi altındadır. Sistem yöneticisi; tüm kullanıcı sistemlerine erişme, bilgisayar hesabının kontrol sahipliği, ihtiyaç olduğunda uzaktan erişim, sistem konfigürasyonunda değişiklik, sistem loglarına erişim, yeni software/hardware kurulumu ve düzenlemesi yetkilerine sahiptir.
- Belediye çıkarlarıyla çakışmadığı sürece taşınabilir bilgisayarların kişisel kullanımına kısıtlı olarak izin verilebilecektir.
- Belediye bünyesinde memur ve personeller, ofis ortamında veya dışında, sabit ve taşınabilir bilgisayarlarını terk ettikleri zaman kilitlemeli diğer kişi, memur ve personellerin izinsiz ve uygunsuz kullanımlarına izin vermemelidir.
- Bilgisayar üzerinde kişisel oturumlardan birinci derecede memur ve personeller sorumludur.
- Bilgisayarlarda şifre korumalı ekran koruyucu aktif olmalıdır.
- Cihazların kullanımı esnasında ilgili yasa ve düzenlemelere uyulmalıdır.
- Belediyeye ait taşınabilir bilgisayar cihazları hiçbir şekilde yasa dışı, Belediye çıkarlarıyla çatışabilecek veya normal operasyon ve iş aktivitelerini engelleyecek şekilde kullanılamaz.
- Belediye bilgileri sabit ve taşınabilir bilgisayarlardan aksi belirtilmedikçe birim yöneticileri ve yönetim dışındaki memur ve personeller tarafından taşınabilir medya aracılığıyla (USB, CD vb.) veri aktarımı yapılamaz. İş amaçlı özel kullanım taleplerinde ilgili birim yöneticisinin yazılı onayı olmak suretiyle diğer memur ve personellere gerekli durumlarda bu yetki sadece o iş sürecinde verilebilmektedir.
- Her tür bilgi, zararlı yazılımlara karşı taramadan geçirilmeden Belediye ağına aktarılamaz.
- Belediye, sabit ve taşınabilir bilgisayarlar kullanılarak yapılan tüm işlemleri izleme hakkını saklı tutar ve gerektiğinde bu hakkını kullanabilir.
- Belediye kullanıcıların sabit ve taşınabilir bilgisayar cihazları ile gerçekleştirdiği aktivitelerle ilgili bilgiyi üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

5.7. P.07. ŞİFRE POLİTİKASI

Amaç

İşbu Politika, Belediye nezdinde kullanılacak her türlü şifreleme sistemlerinin güvenli bir şekilde oluşturulması ve aynı düzeyde koruma sağlanması amacıyla oluşturulmuştur.

Kapsam

Şifre Politikası, Belediye nezdindeki bilgisayarları ve sunucuları kullanan tüm kullanıcı hesaplarını ve memur ve personeli kapsamaktadır.

Politika

- Şifreleme, bilgisayar ve hesap güvenliği için önemli bir özelliktir. Şifreler kompleks olmalıdır. Kolay tahmin edilen (memleket, çocuk, doğum tarihi, ardışık rakam ve harfler, İstanbul, Ankara, Kayseri, 1qaz2wsx, qwerty vb.) şifreler kullanılmamalıdır.
- Belediye içerisinde kullanılan genel kullanıcı bilgisayarları şifreleri 90 günde bir değiştirilmesi zorunlu kılınmıştır. Sistemler ile zorunluluk getirilmeyen hesapların şifreleri de 90 günde bir değiştirilmesi zorunludur.
- Üretim sürecinde kullanılan tüm bilgisayarların şifreleri 6 ayda bir değiştirilmesi zorunludur.
- Oluşturulacak şifre son 3 şifre ile aynı olamaz.
- Oluşturulacak şifre içerisinde Türkçe karakter bulunmamalıdır.
- Bilgisayar kullanıcı hesaplarının şifreleri en az 8 karakter olmalıdır. Kompleks şifre içeriğinde Büyük Harf, Küçük Harf, Rakam, Özel Karakter seçeneklerinden en az 3 tanesinin olması gerekmektedir.
- Kullanıcılar bilgisayar başından kalktığı zaman mutlaka oturumlarını kitlemelidirler. (Windows +L) Genel kullanıcı bilgisayarları kullanılmadığı zaman otomatik olarak 5 dakika içerisinde şifreli ekran korumasına girmelidir.
- Hatalı şifrelerin 10 defa üst üste denenmesi sonucunda kullanıcı hesabı otomatik olarak 20 dakika kilitlenecektir. Şifrelerin unutulması durumunda Bilgi İşlem Müdürlüğü ile iletişime geçilmelidir.
- Kurumsal hesaplara ait şifrelerin e-posta iletilerine veya herhangi bir elektronik forma yazılması yasaktır.
- Şifrelerin aile bireyleri dahil herhangi bir üçüncü kişi ile paylaşılması, kağıtlara veya elektronik ortamlara yazılması yasaktır.
- Bilgi İşlem Müdürlüğü tarafından oluşturulan geçici şifrelerin değiştirilmesi zorunludur.
- Belediye memur ve personeli olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de şifre kuralına göre belirlenmelidir.
- Uygulamalara, hesaplara veya bilgisayarlara giriş şifresinin unutulması veya herhangi bir sorun yaşanması durumunda derhal Bilgi İşlem Müdürlüğü'ne haber verilmelidir.
- Belediye, şifre ile kullanılan hesapları ve bilgisayarları izleme hakkını saklı tutar ve gerektiğinde bu hakkını kullanabilir.
- Belediye kullanıcıların şifre ile gerçekleştirdiği işlemlere ait bilgileri üçüncü partilerle, emniyet birimleri veya yargıyla paylaşma hakkını saklı tutar.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

5.8. P.08. FİZİKSEL GÜVENLİK POLİTİKASI

Amaç

İşbu Politika, Belediye personeli ve kritik kurumsal bilgilerin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve Belediye binalarına yetkisiz girişlerin önlenmesi amacıyla oluşturulmuştur.

Kapsam

Fiziksel Güvenlik Politikası, Belediye binalarında yer alan bilgi varlıklarına erişim sağlayan tüm fiziksel güvenlik konularını kapsamaktadır.

Politika

- Kurumsal bilgi varlıklarının dağılımı ve bulundurulan bilgilerin kritiklik seviyelerine göre binada ve çalışma alanlarında farklı güvenlik bölgeleri tanımlanmalı ve erişim izinleri bu doğrultuda belirlenerek gerekli kontrol altyapıları oluşturulmalıdır.
- Belediye dışı ziyaretçilerin ve yetkisiz memur ve personelin güvenli alanlara girişi, yetkili görevliler gözetiminde gerçekleştirilmelidir.
- Tanımlanan farklı güvenlik bölgelerine erişim yetkileri düzenli aralıklar ile kontrol edilmelidir.
- Belediye girişleri, toplantı salonları ve sistem odaları gibi kritik alanlar güvenlik açısından kamera ile kayıt altına alınmalıdır.
- Kritik sistemler özel sistem odalarında tutulmalıdır.
- Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketslere karşı koruma altına alınmalıdır.
- Açık ofislerde bulunan gizli bilgi varlıklarının olduğu dolaplar ve çekmeceler kilitli ve kontrol altında tutulmalıdır.
- Kritik bilgi içeren idari alanlara kargo teslimatı yapılması yasaktır. Kargolar ilgili kişilere güvenlikte teslim edilmelidir.
- Ekipmanların kullanımı zimmetlenen kişiye aittir. Ekipmanların güvenliğinin sağlanması kişinin sorumluluğundadır. Teslim edilen ekipmanlara gelecek zararlar zimmet edilen kişiden tahsil edilecektir.
- Belediye içerisine giriş ve çıkışlar kamera sistemi ile kayıt altına alınmalıdır.

5.9. P.09. ÜÇÜNCÜ TARAF GÜVENLİK POLİTİKASI

Amaç

İşbu Politika, Belediye'nin bilgi sistemlerine ve bilgi varlıklarına üçüncü taraflar tarafından ulaşılması durumunda uyulması gereken kuralları belirlemek amacıyla oluşturulmuştur.

Kapsam

Üçüncü Taraf Güvenlik Politikasının uygulanmasından Belediye müdürlüklerinin tamamı sorumludur.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

Politika

- Belediyeye ait bilgi sistemlerinin veya bilgi varlıklarının bakımı, güncellenmesi vb. amaçlar ile işlem yapmak üzere Belediyeye gelen yüklenici, doğrudan hizmet temin edilen gerçek ve tüzel kişiler veya üçüncü taraflar ile Gizlilik Sözleşmeleri yapılmalıdır.
- Üçüncü taraflar Belediye içerisinde buldukları sürece Belediye politikalarına uygun hareket etmekte yükümlüdürler.
- Bilgi sistemlerinde veya bilgi varlıkları üzerinde yapılacak çalışmalar hakkında Develi Belediyesi Bilgi İşlem Müdürlüğü'ne bilgi verilmesi zorunludur.
- Yükleniciler, doğrudan hizmet temin alınan gerçek veya tüzel kişiler ile üçüncü taraflar Belediyenin bilgi sistemlerine kendilerine verilen yetki kapsamında erişim sağlayabilirler.
- Yükleniciler, doğrudan temin hizmeti alınan gerçek veya tüze kişiler ile üçüncü taraflara verilen erişim yetkileri, erişim amaçlarına uygun olacak şekilde kısıtlı verilmeli, loğları saklı tutulmalı ve çalışma bittikten sonra verilen yetkiler hemen geri alınmalıdır.
- Yüklenici, doğrudan hizmet temin alınan gerçek ve tüzel kişiler ile üçüncü taraflar bilgi sistemlerine ve bilgi varlıklarına eriştikleri süre boyunca refakatçisiz bırakılmamalıdır.
- Belediye, işbu Politika ile düzenlenen kurallar üzerinde değişiklik yapma ve ek önlemler alma hakkını saklı tutar.

5.10. P.10. GİZLİLİK POLİTİKASI

Amaç

İşbu Politika, Belediye memur ve personellerin sistem, bilgi ve varlıkların gizlilik, bütünlük ve erişilebilirlik sınıfları açısından yapılması ve uyulması gereken iş kurallarının belirlenmesi amacıyla hazırlanmıştır.

Kapsam

Gizlilik Politikası Belediye bünyesindeki tüm memur ve personelleri kapsamaktadır.

Politika

- Belediyenin gizli olarak belirlediği tüm bilgilerin gizliliğine sıkı bir şekilde uyulacaktır. Belediyenin iş gereksinimi dışında bu bilgilerin kopyalanması ve iletilmesi yasaktır.
- Belediye personeli, kendilerine tahsis edilmiş tüm bilgisayar erişim bilgilerini ve kendisine verilmiş cihazların güvenliğini sağlamakla yükümlüdür. Erişim bilgileri herhangi birine söylenemez ve bu bilgiler başkaları ile paylaşılamaz.
- Hiçbir personel, bilgisayarındaki anti virüs koruma yazılımını devre dışı bırakamaz.
- Ortak alanlar üzerinde bulunan herkesin kullanımına açılmış olan "GENEL" klasörüne gizli ya da çok gizli bilgiler kopyalanmamalıdır. Bu alan üzerinde film, müzik gibi bilgiler paylaşılmamalıdır.
- Kullanıcı bir bilginin çok gizli olduğunu düşünüyorsa o bilgi şifrelenmeli veya yetkili kişiler dışında erişilemeyecek alanlarda saklanmalıdır.
- Bilgisayarlar üzerinden Belediyeye ait dokümanlar haricinde dosya alışverişinde bulunulmamalıdır.
- Kritik veya gizli raporların dökümünü alan memur ve personel, rapor içeriğindeki bilginin uygun şekilde (kilitli dolap, çekmece vb.) korunmasından sorumludur.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

- Herhangi bir kişi kendisine ait olmayan kritik bir rapor bulur ise bu durumu derhal Bilgi İşlem Müdürlüğü'ne bildirmelidir.
- Sunucu ve bilgisayarların saatleri kullanıcılar tarafından değiştirilemez. Saatler sistem tarafından otomatik olarak yönetilmektedir.
- Taşınabilir bilgisayarlar güvenlik açıklarına karşı daha dikkatli korunmalıdır. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Cihazların çalınması veya kaybolması durumunda hemen Bilgi İşlem Müdürlüğü'ne bildirilmelidir.
- Belediye bünyesinde edinilmiş olan ticari sır, patent, üretim, üye bilgileri kesinlikle yetkisiz kişiler ile paylaşılmamalıdır.
- Belediye bilgisayarlarında kişisel verilerin barındırılması yasaktır. Belediyeye ait cihazlarda tutulan ve iletilen tüm bilgiler Belediye malıdır ve Belediye bu bilgileri izleme ve denetleme hakkına sahiptir.
- Hiçbir memur ve personel, izin almadan kendi bilgisayarından veya başka bir kaynak kullanarak Belediyenin bilişim ağını tarayamaz, izleyemez veya dinleyemez.
- Hiçbir memur ve personel, Belediye içinde kendilerine tahsis edilen bilgisayar yetkilerinin dışına çıkamaz ve bu konuda yetki aşma işlemine girişemez.
- Sosyal medya erişim izni verilen memur ve personellerin görevlerinin dışında bu hesapları kullanmaları yasaktır.
- Sosyal medya üzerinden Belediyeyi rencide edici, karalayıcı paylaşımlar yapılmamalıdır. Belediyenin hassas bilgileri sosyal medya üzerinden paylaşamaz.
- Belediyeye ait bilgisayar, telefon, yazıcı, faks, fotokopi, tarayıcı vb. donanımlar şahsi işlemler için kullanılmamalıdır. Bilgisayar, telefon, yazıcı, faks, fotokopi, tarayıcı vb. cihazlarda şahsi kullanım tespit edildiğinde İnsan Kaynakları ve Eğitim Müdürlüğüne bilgi verilecektir.
- Belediye, işbu Politikanın uygulanabilirliği denetimi amacıyla kullanıcıların sahip olduğu tüm varlıkları izleme yetkisini saklı tutar.
- Belediye, kullanıcılar tarafından işbu Politika kapsamında gerçekleştirilen işlemleri izleme yetkisi kapsamında elde edeceği bilgileri üçüncü partilerle, emniyet birimleriyle veya yargıyla paylaşma hakkını saklı tutar.

5.11. P.11. TEMİZ MASA TEMİZ EKCRAN POLİTİKASI

Amaç

İşbu Politika, Develi Belediyesi bünyesindeki kağıtlar, taşınabilir depolama ortamları ve kişisel bilgisayar için mesai saatleri içinde ve dışında bilgiye yetkisiz erişim ve bilginin hasar görmesi gibi riskleri azaltmak için gerekli olan şartların oluşturulması amacıyla hazırlanmıştır.

Kapsam

Temiz Masa Temiz Ekran Politikası Develi Belediyesi bünyesindeki tüm memur ve personeli kapsamaktadır.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

Politika

- Belediyeye ait uygulamalarda kullanılan şifreler iş arkadaşları da dahil olmak üzere kimse ile paylaşılamaz. Şifrelerin yazılı olarak post-it ya da not kağıtlarına yazılarak pano, bilgisayar ekranı, klavye gibi donanımlara yapıştırılmaz.
- Evrak ve dokümanların güvenliği için çalışma saatleri dışında ofis kapılarının kilitli tutulması gerekmektedir.
- Evrak ve dokümanlarda yer alan bilgilerin farklı kişiler tarafından ele geçirilmemesi için klasörlerde saklanmalıdır.
- Hassas bilgi içeren evrak klasörleri ve Belediyeye ait başlıklı kağıtlar kilitli dolaplarda saklanmalıdır.
- Kağıtların doğrudan çöp kutusuna atılması yasaktır. İmha edilecek kağıtlar için kâğıt kırma makinesi kullanılmalıdır.
- Hassas ve kritik bilgi içeren evraklar ağ üzerinden paylaşılamaz.
- Masaüstü doküman sayısını artırmamak için mümkün olduğu kadar elektronik dokümanların yazıcıdan çıktılarının alınmamasına dikkat edilmelidir.
- Masa üzerinde kartvizit kutuları, kişisel ajandalar, değerli bilgilere sahip dokümanlar bırakılmaz ve bunlar kilitli çekmecelerde muhafaza edilmelidir.
- Masa çekmecelerinin anahtarları, ev ve araba gibi özel anahtarlar, kasa anahtarları masa üzerinde bırakılmamalıdır.
- Belediyeye ait kritik bilgi içeren dokümanlar başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.
- Memur ve personelin kişisel gizli bilgileri (maaş bordrosu vb.) başkaları tarafından fark edilmeyecek şekilde muhafaza edilmelidir.
- Memur ve personelin telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranmakla yükümlüdür.
- Bilgi ve veri alışverişinden önce dış tarafların kimlikleri tespit edilmelidir.
- Belediye bünyesinde kullanılan toplantı salonlarında gizli ve kritik bilgi içeren dokümanları toplantı sonrasında ilgili salonlarda bırakmamalı ve salonlardaki tahtalara alınan notlar silinmelidir.
- Gizlilik içeren bilgilerin umumi yerlerde konuşulması yasaktır.
- Gizlilik içeren bilgiler telefonlarda ses dışarıya açık olarak görüşülmemelidir. Faks yoluyla gizlilik içeren herhangi bir bilgi gönderilmemelidir.
- Bilgisayar gibi elektronik ortamlarda bulunan bilginin korunması için çalışma saatleri dışında da ofis kapıları kilitli tutulmalıdır.
- Kısa süreli ayrılmalarda dahi, cep telefonu, taşınabilir bellek, harici hard disk, CD, DVD gibi eşyalar çalışma masası üzerinde bırakılmamalıdır.
- Bilgisayarlar gözetimsiz bırakıldığında kapatılmalı veya parola kullanılarak korunmalıdır. Ekran koruyucu aktif hale getirilmelidir. Bu işlem Windows bilgisayarlarda Windows +L, Mac bilgisayarlarda Control+Shift+Eject tuşlarına basılarak kolayca yapılabilir.
- Bilgisayarların masaüstlerindeki klasör ve dosyalar düzenli şekilde tutulmalıdır.
- Fotokopi cihazlarının yetkisiz kullanımı önlenmelidir.
- Fotokopi cihazlarının belleğinde bulunan kritik ve hassas bilgiler silinmelidir.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

- Hassas ve sınıflandırılmış bilgi içeren ortamlardaki bilgiler yazıcıdan çıktı alındıktan sonra hemen silinmelidir.
- Şifreler yazılı olarak saklanmamalı ve hassas bilgiler silinmelidir.
- Kullanılan şifreler tahmin edilebilir olmamalıdır. Şifreyi oluşturan kişi ile ilgili bilgiler içermemelidir. Ardışık, tümü sayısal ya da tümü alfabetik karakterlerden oluşmamalıdır.
- Memur ve personelleri kendilerine ait bilgisayarlarda, taşınabilir belleklerde, harici diskte ve benzeri depolamanın mümkün olduğu ortamlardaki gizlilik dereceli bilgi ve belgelerin güvenliğini sağlamakla yükümlüdür. Taşınabilir bellek veya harici diske gizli, önemli veya özel nitelikli kişisel veri konulması gerekiyor ise kriptolayarak korunması gerekmektedir.
- Gizli belgelerin, şifrelerini adreslerin, özellikle taşınabilir bellek, e-posta, sosyal medya gibi alanlarda paylaşılmamasına dikkat edilmelidir.
- Bilinmeyen e-posta ve haber gruplarına üye olunmamalıdır.
- Elektronik posta ortamında kişisel şifre bilgileri paylaşılmamalıdır.
- Silinebilir ortamlara kaydedilmiş olan gizli bilgilerin kullanımından sonra etki yöntemler kullanılarak geri dönlmeyecek şekilde silinmesi gerekmektedir.
- Belediyeye ait yürütülen iş ve işlemlerde Belediyeye ait e-posta adreslerinin kullanılması zorunludur.
- Kurumsal işlerin yapıldığı bilgisayarlar memur ve personelin kendi sorumluluğundadır. Belediye bilgisayarlarının memur ve personel haricinde yetkisiz kullanıcılara teslim edilmesi yasaktır.

5.12. P.12. KRİPTOGRAFİK KONTROLLER POLİTİKASI

Amaç

İşbu Politika, bilginin gizliliği, erişilebilirliği veya bütünlüğünün korunması amacıyla oluşturulmuştur.

Kapsam

Kriptografik Kontroller Politikası, kritik bilgilerin güvenli erişimi ve paylaşımı amacıyla tüm Belediye memur ve personellerini kapsamaktadır.

Politika

- Belediye içerisinde tanımlanan gizli bilgi varlıkları ve özel nitelikli kişisel veriler kriptografik şifreleme yöntemleri ile saklanmalıdır. Her memur ve personel kendi barındırdığı bilgi varlıklarının ve özel nitelikli kişisel verilerin güvenliğinden sorumludur.
- Belediyeler arası bilgi alışverişlerinde ve özellikle kamu kurumları ile yapılan yazışmalarda e-imza, mali mühür gibi sistemler kullanılarak veri transferi yapılmalıdır.
- Belediye sistemlerine dışarıdan yapılacak her türlü uzak bağlantı SSL VPN sistemi üzerinden yapılmalıdır.
- Mobil cihazlardaki verilerin korunmasında güçlü şifre kullanılmalıdır.
- Belediye, Kriptografik verilerin paylaşımını ve saklanmasını izleme hakkını saklı tutar ve gerektiğinde bu hakkını kullanabilir.

| | | |
|---|---|--------------------------|
|  | KİŞİSEL VERİLERİN KORUNMASI UYUM SÜRECİ POLİTİKASI | Doküman No: 1 |
| | | Yayın Tarihi: 23/03/2022 |
| | | Revizyon No/Tarih: 00/- |

5.12. P.12. KİMLİK DOĞRULAMA VE YETKİLENDİRME POLİTİKASI

Amaç

İşbu Politika, Belediyenin bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme politikalarının belirlenmesi amacıyla oluşturulmuştur.

Kapsam

Belediyenin bilgi sistemlerine erişim Belediye memur ve personelleri ile Belediye dışı kullanıcılar Kimlik Doğrulama ve Yetkilendirme Politikası kapsamındadır.

Politika

- Belediye sistemlerine erişecek tüm kullanıcıların bilgisayar erişim hesapları doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.
- Belediye sistemlerine erişmesi gereken yüklenici, doğrudan hizmet temin edilen gerçek ve tüzel kişiler veya üçüncü kişilere yönelik kullanıcı hesabı Bilgi İşlem Müdürlüğü tarafından ilgili yetkiler verilerek tanımlanacaktır.
- Belediye bünyesinde kullanılan ve merkezi olarak erişilen uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri üzerindeki kullanıcı yetkileri belirlenmeli ve denetim altında tutulmalıdır.
- Memur ve personeller ile üçüncü kişilere verilen erişim yetkilerinin güncelliği sağlanmalıdır.
- İşletim sistemleri üzerindeki erişim logları düzenli olarak tutulmalı, gerektiği durumlarda kontrol edilebilmelidir.
- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
- Erişim gereksinimi artık kalmamış kullanıcıların hesapları Bilgi İşlem Müdürlüğü tarafından pasif duruma alınmalı veya kaldırılmalıdır.
- Belediye, kendi inisiyatifi doğrultusunda erişim yetkilerini belirleme, pasife alma veya kaldırma yetkisini saklı tutar.

6. UYGULAMA VE YAPTIRIM

Belediye memur ve personellerinin işbu Politika kapsamında yer alan politikalara ve Belediyeye ait diğer politika ve prosedürlere aykırı kasti veya kasıtsız davranışları hakkında Bilgi Güvenliği Disiplin Prosedürü uygulanacaktır. Belediyenin 5393 sayılı Belediye Kanunu ile 4857 sayılı İş Kanunu, iş sözleşmeleri ve sair mevzuat hükümleri kapsamında yaptırım uygulama ve zararlarının tazmini için rücu etme hakkı saklıdır.

7. REVİZYON KAPSAMI

İlk yayındır.

| Hazırlayan | Onaylayan |
|--|------------------------|
| KVKK Komisyonu | KVKK Komisyonu Başkanı |
| Muhammed Seyyid ŞAHİN Alper GÜRLEK Ergün İLHAN | Mustafa KÜÇÜKTEPE |