BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ GÜVENLİGİ POLİTİKALARI
YÖNERGESİ

BİRİNCİ BÖLÜM
Genel Hükümler

Amaç

MADDE 1. Bu yönergenin amacı; **Bartın Belediye Başkanlığı'nın** sahip olduğu elektronik ortam ve bilgilerinin paylaşımı ve güvenliği konularında tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmektir.

Kapsam

MADDE 2. Bu Yönerge, Bartın Belediye Başkanlığı teşkilatında bulunan bütün birimlerdeki personelin bilgi sistemlerinin kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke ve kurallarını kapsamaktadır.

Hukuki Dayanak

MADDE 3. 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanununa dayanılarak 26.12.2007 tarihli ve 26738 sayılı Resmi Gazetede yayımlanan "Kamu İç Kontrol Standartları Tebliği", 23.05.2007 tarihli ve 26530 sayılı Resmi Gazetede yayımlanan 5651 sayılı kanunun 6. maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4. Bu yönergede geçen;

Başkan: Belediye Başkanı,
Başkan Yardımcısı: Belediye Başkan Yardımcısı,
Müdürlük: Bilgi İşlem Müdürlüğü,
Sistem Yöneticisi: Bilgi Sistemleri Yöneticisini,
Kullanıcı: Bartın Belediye Başkanlığında Bilgi Sistemlerini Kullanan tüm kişileri,
Sunucu: Sunucuların verdiği hizmeti alan bilgisayar sistemini,
İstemci: İstemcilerden gelen isteklere hizmet verebilen bilgisayar sistemini, ifade eder.

(2) Yönergede kullanılan teknik terim ve tanımlar, (Ek-1) tabloda gösterilmiştir.

İKİNCİ BÖLÜM
Bilgi Güvenliği Politikaları

Bilgi Sistemleri Genel Kullanım Politikası

MADDE 5. (1) Bilgi sistemlerine sahip olma ve bu sistemlerin genel kullanım kuralları aşağıda belirtilmiştir.

a. Kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Kurumun bünyesinde oluşturulan tüm veriler, iş ve işlemler için Kurum tarafından kullanıma sunulan tüm bilgisayarlar, taşınabilir cihazlar (kurum bilgisi taşıyan her türlü dizüstü bilgisayar, tablet, akıllı telefon, CD, USB disk, teyp, taşınabilir sabit disk gibi veri saklayabilecek ortamlar) ve bilişim sistemleri Kurumun mülkiyetindedir.

b. Personelin kullanımı için tahsis edilmiş olan tüm bilişim sistemleri, bilgisayarlar, dizüstü bilgisayar, mobil cihazlar, tablet vb. sadece yetkilendirilmiş personel tarafından ve veriliş amaçları doğrultusunda kullanılmalıdır.

c. Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır.

d. Kurum bilgi sistemleri kapsamında üretilen her türlü kurumsal bilgi USB Bellek, CD vb ortamlarda taşınmamalı ve saklanmamalıdır.

e. Kurum, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

f. Kurum bilgisayarları etki alanına (domain) dahil edilmelidir. Etki alanına bağlı olmayan bilgisayarlar yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi olmamalıdır. Kurum içi etki alanı (Domain) oluşmamış ise Bilgi İşlem Müdürlüğünün uygun gördüğü ağ yapılanmasına dahil edilmelidir.

g. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.

h. Kurumda Bilgi İşlem Müdürlüğünün yazılı onayı olmadan Belediye Başkanlığı Ağ sisteminde (web hosting, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.

i. Bilgi İşlem Müdürlüğü personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa cihaz bağlama, ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilememelidir.

j. Bilgisayarlara lisanssız program yüklenmemelidir.

k. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır. Başkanlıktan ortak alan talebinde bulunulmalıdır. Kaynakların paylaşıma açılması halinde mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

(2) Bilgi sistemleri genel yapılandırması ile ilgili kurallar aşağıda belirtilmiştir.

a. Herhangi bir Masaüstü/Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Müdürlüğüne haber verilmelidir. Bilgi İşlem Müdürü bu durumu bağlı olduğu Başkan Yardımcısı ile birlikte Başkan'a iletmelidir.

b. Bütün bilgisayarlar, cep telefonu, tablet bilgisayarlar ve cihazlar kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (kızılötesi, bluetooth, vb) özellikleri aktif halde olmamalıdır ve anti-virüs programları lisanslı ve yeni nesil virüslere karşı anti-virüs firması tarafından otomatik güncelleme ile korunmalıdır.

c. Kullanıcılar tarafından gönderilen e-postalarda aşağıdaki şekilde bir açıklama yer almalıdır.

"Bu elektronik posta ve onunla iletilen bütün dosyalar; göndericisi tarafından alması amaçlanan; yetkili gerçek ya da tüzel kişinin kullanımı içindir. Eğer söz konusu yetkili alıcı değilseniz bu elektronik postanın içeriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı derhal silmeniz gerekmektedir. T.C. Bartın Belediye Başkanlığı bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda herhangi bir garanti vermemektedir ve hiçbir hukuksal sorumluluğu kabul etmemektedir. Bu nedenle bu bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından ve saklanmasından sorumlu değildir. Bu mesajdaki görüşler yalnızca gönderen kişiye aittir ve T.C. Bartın Belediye Başkanlığı'nın görüşlerini yansıtmayabilir. Bu e-posta bilinen bilgisayar virüslerine karşı taranmıştır. Ancak yollayıcı, bu e-posta mesajının - virüs koruma sistemleri ile kontrol ediliyor olsa bile - virüs içermediğini garanti etmez ve meydana gelebilecek zararlardan doğacak hiçbir sorumluluğu kabul etmez."

d. Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı, ek dosyalar eklenecekse dosyalar sıkıştırılmalıdır.

E-Posta Politikası

MADDE 6. (1) E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.

a. Kullanıcılar e-posta başvurularını Ek-2'deki formu kullanmalıdır.

b. Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

c. Bartın Belediye Başkanlığı ile ilgili olan gizli bilgiler, gönderilen mesajlarda yer almamalıdır. Buna kapsamı içerisine iliştirilen öğeler de dahildir. Mesajların, gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.

d. Kullanıcı, Kurumun e-posta sistemini taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajlar göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında ilgili birime haber verilmelidir.

e. Kullanıcı hesapları, ticari ve kar amaçlı olarak kullanılmamalı ve e-posta gönderilmemelidir.

f. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, ilgili birime haber verilmelidir.

g. Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.

h. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pornografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.

i. Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkar, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajları yollamaktan sorumludur.

j. Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarının içinde; 4 karmaşıklığın (büyük harf, küçük harf, rakam ve özel karakter (@,A,+,$,#,&,/,{,*,-,],=...)) en az 3 tanesi bulunmalıdır.

(2) E-Posta ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

a. E-posta kişisel amaçlar için kullanılmamalıdır.

b. Kullanıcı, mesajlarının, yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden parola kullanılmalı ve kullanılan parola en geç 45 günde bir değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

c. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın ilgili birime/başkanlığa haber vermelidir.

d. Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için cevaplandırmalı ve kurumsal mesajlarda kişisel e-posta adresleri değil kurumsal e-posta adresi kullanılmalıdır.

e. Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.

f. Kurum e-posta adresleri ile kişisel sosyal medya ve kurumla alakalı olmayan hiçbir siteye abone olunmamalıdır.

g. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar ilgili birime haber verilmelidir.

h. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren Başkanlığa haber vermelidir.

i. Kurumsal e-postalar yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilecektir.

j. Kullanıcı, e-postalarına erişirken, POP3, SMTP, HTTP vb kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmamalıdır.

k. Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar anti virüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir. Fakat her ne kadar virüs programları ile tarama yapılması sonucu programların fark edemediği yeni nesil virüsler için kullanıcıları dikkatli olması gerekmektedir. Tüm sorumluluk kullanıcıya aittir.

Parola Politikası

MADDE 7. (1) Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

a. Belediye Otomasyon hesapları, e-Belediye hesapları, Sistem hesapları, Eposta, , Veri Depolama cihazlarına ait parolalar (örnek; root, administrator, enable, vs.) en geç 6 (altı) ayda bir değiştirilmelidir. Kullanıcılarının kendilerinin parola değişimlerini yapamadıkları zaman Sistem Yöneticisine başvurulması gerekmektedir.

b. Kullanıcı hesaplarına ait parolalar(örnek, sistem, e-posta, web, masaüstü bilgisayar vs.) en geç 45(kırk beş) günde bir değiştirilmelidir.

c. Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.

d. Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

e. Kullanıcı, parolasını başkası ile paylaşmaması, kağıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.

f. Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları kolayca kırılamayacak güçlü bir parolaya sahip olmalıdır.

g. Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.

(2) Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

a. Parola en az 8 haneli olmalıdır.

b. İçerisinde en az 1 'er tane büyük ve küçük harf bulunmalıdır(A,a, B,b C,c.).

c. İçerisinde en az 1 tane rakam bulunmalıdır(1, 2, 3...).

d. İçerisinde en az 1 tane özel karakter bulunmalıdır(@, !,?,A,+,$,#,&,/,{,*,-,],=,...).

e. Aynı karakterler peş peşe kullanılmamalıdır(aaa, 111, XXX, ababab...).

f. Sıralı karakterler kullanılmamalıdır(abcd, qwert, asdf,1234,zxcvb...).

g. Kullanıcıya ait anlam ifade eden kelimeler içermemelidir(Kullanıcı adı, sicil numarası, aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.).

(3) Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

a. Bütün parolalar Başkanlığa ait gizli bilgiler olarak düşünülmeli ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.

b. Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılmamalıdır.

(4) Uygulama Geliştirme Standartları

a. Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.

b. Parolalar, metin olarak veya kolay anlaşılabilir formatta saklanmamalıdır.

c. Parolalar, şifrelenmiş olarak saklanmalıdır.

d. Uygulamalarda kullanıcının her uygulama için ayrı parola girmesinden kaçınılmalı, parola girişi mümkün mertebe güvenilir tek giriş uygulamaları ile sağlanmalıdır.

Anti Virüs Politikası

MADDE 8. (1) Anti virüs Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurumun tüm istemcileri ve sunucuları anti virüs yazılımına sahip olmalıdır (Sistem yöneticileri tarafından anti virüs yazılımı kullanımına ihtiyaç duyulmayan sunucular hariç).

b. İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalı, virüs temizliğinden sonra tekrar etki alanına alınmalıdır.

c. Sistem yöneticileri, anti virüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.

d. Kullanıcı hiç bir sebepten dolayı anti virüs yazılımını bilgisayarından kaldırmamalıdır.

e. Anti virüs güncellemeleri anti virüs sunucusu/sunucuları ile yapılmalıdır. Anti virüs sunucuları internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak anti virüs sunucusu tarafından anti virüs güncellemeleri yapılmalıdır.

f. Haklı bir gerekçe ile etki alanı dışında tutulması gereken kullanıcı talebi olması durumunda; her türlü maddi/manevi oluşabilecek zararların kişi ve amiri tarafından kabul edildiğini beyan eden form doldurularak Belediye Başkanlığına teslim edilmelidir. Bu tip kullanıcıların her türlü güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartmalıdır.

g. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.

h. Kurumun sunucu/nas cihazlarına ihtiyacı haricinde okuma/yazma hakkı veya disk erişim hakkı tanımlamaktan kaçınılmalıdır. İhtiyaca binaen

yapılan bu tanımlamalar, ihtiyacın ortadan kalkması durumunda iptal edilmelidir.

i. Optik Media ve harici veri depolama cihazları anti virüs kontrolünden geçirilmelidir.

j. Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

İnternet Erişim ve Kullanım Politikası

MADDE 9. (1) İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Kullanıcılar Ek-3'deki İnternet Yetkilendirme Talep Formu doldurmalıdır.

b. Kurumun tüm istemcileri ve sunucuları anti virüs yazılımına sahip olmalıdır.

c. Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvarları üzerinden internete çıkmalıdır. (Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır).

d. Kurumun politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografi, oyun, kumar, şiddet içeren vs.) yasaklanmalıdır.

e. Kurumun ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.

f. Kurumun ihtiyacı ve olanakları doğrultusunda anti virüs sunucuları kullanılmalıdır.

g. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.

h. Kullanıcıların İnternet erişimlerinde firewall, anti virüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.

i. Ancak yetkilendirilmiş kişiler internete çıkarken (Mümkünse Kurumun normal kullanıcılarının bulunduğu ağdan farklı bir ağda olmak kaydıyla) bütün servisleri kullanma hakkına sahip olabilir.

j. Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemeli, İnternet üzerinden TV, radyo ve video izlenmemeli/dinlenmemelidir.

k. İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir. Bu konuda gerekli önlemler alınmalıdır.

l. Üçüncü şahısların İnternet erişimleri için misafir ağı erişimi verilmelidir.

Bilgisayar Güvenlik Politikaları

MADDE 10. (1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurumda bulunan bilgisayarların yönetiminden, ilgili kullanıcı personel sorumludur.

b. Bilgisayar kurulumları, konfigürasyonları, yamaları, güncellemeleri sadece Bilgi İşlem Müdürlüğü personeli tarafından yapılmalıdır. Bilgi İşlem Müdürlüğü personeli tarafından yapılmayan kurulum, konfigürasyon, yama ve güncellemelerinden sorumlu değildir.

c. Kullanıcılar sorumlu olduğu bilgisayar üzerindeki veri niteliği taşıyan verilerin yedeklemelerini yapmak üzere sorumludur.

d. Bilgi İşlem Müdürlüğü Bilgisayarlara ait bilgilerin yer aldığı tablo oluşturulmalıdır. Bu tabloda; sunucuların isimleri, ip adresleri ve yeri, işletim sistemi sürümleri ve yamaları, donanım, kurulum, yedek, yama yönetimi işlemlerinden sorumlu personelin isim bilgileri yer almalıdır.

e. Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır. Kurumun bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvarları üzerinden internete çıkmalıdır. (Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır).

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

a. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

b. Bilgisayar üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti virüs vb. koruma amaçlı yazılımlar sürekli güncellenmelidir. Anti virüs ve yama güncellemeleri otomatik olarak yazılımlar tarafından yapılmalıdır.

c. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş personel olmalıdır.

d. Sistem yöneticileri mümkün olduğu ölçülerde 'Administrator' ve 'root' gibi genel sistem hesapları kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır. Kullanıcılar bilgisayarına kullanıcı tanımı parola ile açmalıdır. 30 dk işlem yapmadığı takdirde kullanıcı adı ve parola ekranı aktif olmalıdır.

e. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSL, IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

f. Sunuculara ait bağlantılar normal kullanıcı hatlarına takılmamalıdır.

g. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.

h. Sunucu / Bilgisayarlar üzerinde lisanslı veya güvenliği test edilmiş açık kaynak kodlu yazılımlar kurulmalıdır.

i. Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

(3) Sunucu gözlemleme kuralları aşağıda belirtilmiştir.

a. Kritik sistem kullanan müdürlükler, uygulama erişimleri kaydedilmeli ve kayıtlar aşağıdaki gibi saklanmalıdır.

b. Kayıtlar sunucu/bilgisayar üzerinde tutulmalarının yanı sıra ayrı bir sunucuda/bilgisayarda da saklanmalıdır.

c. Sunucu/bilgisayar üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.

d. Kayıtlar sorumlu kişi tarafından değerlendirilmeli ve gerekli tedbirler alınmalıdır.

e. Sunucularda port taramaları düzenli olarak yapılmalıdır. Açık olmaması gereken portlar kapatılmalıdır.

f. Yetkisiz kişilerin ayrıcalıklı hesaplara yönelik girişimlerinin kontrolü periyodik yapılmalıdır.

g. Sunucu yedekleri Bilgi İşlem Müdürlüğü tarafından saklanmalıdır.

h. Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar düzenli takip edilmelidir.

i. Denetimler, Bilgi İşlem Müdürlüğü tarafından yetkilendirilmiş kişilerce yönetilmeli ve belli aralıklarda yapılmalıdır.

j. Sunucuların bilgileri yetkilendirilmiş kişi tarafından tutulmalı ve güncellenmelidir. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

(4) Sunucu / Bilgisayar işletim kuralları aşağıda belirtilmiştir.

a. Sunucular/Bilgisayarlar elektrik, ağ altyapısı, sıcaklık ve nem değerleri düzenlenmiş olmalıdır.

b. Sunucuların yazılım ve donanım bakımları üretici firma veya yetkili firma tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

c. Bilgisayarların yazılım ve donanım güncellemeleri belirli aralıklarla, Bilgi İşlem Müdürlüğü personeli tarafından yapılmalıdır.

d. Sistem/Kritik sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.

Ağ Yönetim Politikası

MADDE 11. (1) Ağ yönetim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Ağ cihazlarının yönetim sorumluluğu, sunucu ve istemcilerin yönetiminden ayrılmalıdır.

b. Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler yapılmalı ve güncellemeler uygulanmalıdır.

c. Erişimine izin verilen ağlar için ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmeli ve yetkisiz erişimle ilgili tedbirler alınmalıdır.

d. Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.

e. Sınırsız ağ dolaşımı engellenmelidir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmalıdır.

f. Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmalıdır.

g. İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmalı ve kayıtlar tutulmalıdır.

h. Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır.

i. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall)üzerinden sağlanmalıdır.

j. Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmalıdır.

k. Bilgisayar ağına bağlı bütün bilişim makinelerinde (Bilgisayar, tablet, vb.) kurulum ve yapılandırma parametreleri, Kurumun güvenlik politika ve standartlarıyla uyumlu olmalıdır.

l. Sistem tasarımı ve geliştirilmesi yapılırken Kurum tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmalıdır.

m. İnternet trafiği ilgili standartlarda anlatıldığı şekilde izlenebilmelidir.

n. Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmalıdır.

o. Ağ cihazları görevler dışında başka bir amaç için kullanılmamalıdır.

p. Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmalıdır.

q. Kurum içi ve dışı birimlerin kendilerine ait olan kablolu/kablosuz ağların tüm sorumluluğu birim müdürlerine aittir.

Ağ Cihazları Güvenlik Politikası

MADDE 12. (1) Ağ cihazları güvenlik politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Cihazlarının IP ve MAC adres bilgileri envanter dosyasında yer almalıdır.

b. Ağ cihazlarında parola kullanmalıdır.

c. Yönlendirici ve anahtarlardaki tam yetkili şifre olan 'enable şifresi' kodlanmış formda saklanmalıdır. Bu şifrenin tanımlanması kurumun içerisinden yapılmalıdır.

d. Yazılım ve firmware güncellemeleri çalışma günlerinin/mesai saatleri dışında yapılmalıdır.

e. Cihazlar üzerinde kullanılmayan servisler kapatılmalıdır.

f. Bilgisayar ağında bulunan kabinetler, aktif cihazlar, ağ kabloları (UTP ve fiber optik aktarma kabloları), cihazların portları etiketlenmelidir.

g. Yönlendiriciye erişen tüm kullanıcılar uyarılmalıdır.

h. Kurum içi birimlerin network ağların loğlarını kayıt altına Bilgi İşlem Müdürlüğü tarafından alınıp saklanmalıdır. Kurum dışı birimlerin kullandıkları network ağların loğlarını kayıt altına almalıdır. Kayıt altına alınması birim müdürünün sorumluluğundadır.

i. Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır.
"BU CİHAZA YETKİSİZ ERİŞİMLER YASAKLANMIŞTIR."

j. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir."

Uzaktan Erişim Politikası

MADDE 13. (1) Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. İnternet üzerinden Kurumun herhangi bir yerindeki bilgisayar ağına erişen kişiler ve/veya kurumlar VPN teknolojisini kullanmalıdırlar. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, gizliliğin korunması ve sistem devamlılığını sağlamaktadır. VPN teknolojileri IpSec, SSL, VPDN, PPTP, L2TP vs. Protokollerinden birini içermelidir.

b. Uzaktan erişim güvenliği denetlenmelidir.

c. Kurum çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

d. Firma ve personeline veya 3. şahıslara Kurum ağına uzaktan bağlanma yetkisi verilmesi için Kurumun herhangi bir birimi ile bir bilişim projesi sözleşmesi olmalı ve VPN talep formu ile gizlilik taahhütnameleri imzalanmalıdır.

e. Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

f. Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.

g. Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve anti virüs yazılımı güncellemeleri yapılmış olmalıdır.

h. Kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcıların yetkileri ve hesap özellikleri buna göre güncellenmelidir.

Kablosuz İletişim Politikası

MADDE 14. (1) Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları kayıt altına alınmalıdır.

(2) Bütün kablosuz erişim cihazları Bilgi İşlem Müdürlüğü tarafından onaylanmış olmalı ve Bilgi İşlem Müdürlüğünün belirlediği güvenlik ayarlarını kullanmalıdır. Bilgi İşlem Müdürlüğünün onayı olmadan hiçbir birim hiçbir şekilde bilgisayar ağına kablolu/kablosuz ağ cihazları takmamalıdır.

(3) Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir.

a. Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılmalıdır. IEEE 802. lx erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri kullanılmalıdır.

b. Erişim cihazlarındaki firmwareler düzenli olarak güncellenmelidir.

c. Cihaza erişim için güçlü bir parola kullanılmalıdır.

d. Erişim parolaları varsayılan ayarda bırakılmamalıdır.

e. Varsayılan SSID isimleri kullanılmamalıdır. SSID yayan bilgisi içerisinde kurumla ilgili bilgi olmamalıdır (mesela kurum ismi, ilgili bölüm, çalışanın ismi vb).

f. Kullanıcıların erişim cihazları üzerinden ağa bağlanabilmeleri için, Kurum kullanıcı adı ve parolası bilgilerini etki alanı adı ile beraber girmeleri sağlanmalı ve Kurum kullanıcısı olmayan kişilerin, kablosuz ağa yetkisiz erişimi engellenmelidir.

g. Erişim Cihazları üzerinden gelen kullanıcılar güvenlik duvarı(Firewall) üzerinden ağa dahil olmalıdırlar.

h. Erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından Kurum'un tüm İnternet bant genişliğinin tüketilmesi engellenmelidir.

i. Erişim cihazları üzerinden gelen kullanıcıların ağ kaynaklarına erişim yetkileri, İnternet üzerinden gelen kullanıcıların yetkileri ile sınırlı olmalıdır.

j. Kullanıcı bilgisayarlarında kişisel anti virüs ve güvenlik duvarı yazılımları yüklü olmalıdır.

k. Erişim cihazları bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir.

l. Kurum içi ve dışı birimlerin mevcut ağın haricinde kullandıkları kablosuz ağların tüm sorumluluğu birim müdürlerine aittir.

Donanım ve Yazılım Envanteri Oluşturma Politikası

MADDE 15. (1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.

a. Oluşturulan envanter tablosunda şu bilgiler olmalıdır; sıra no, bilgisayar adı, bölüm, marka, model, seri no, özellikler, ek aksamlar, işletim sistemi, garanti süresi vs.

b. Bu tablolar Bilgi İşlem Müdürlüğünde tutulmalı ve belirli aralıklarla (3 ay) güncellenmelidir.

c. Birimler bilgisayar ve diğer bilişim teknoloji envanterlerinde yer değişikliği yapması halinde 3 iş günü içerisinde Bilgi İşlem Müdürlüğüne bildirmekle mükelleftir.

d. İlgili bilgiler Bilgi İşlem Müdürlüğü'ne eksiksiz tam anlaşılır şekilde gönderilmelidir. Bilgi İşlem Müdürlüğü gönderilen bilgileri yerinde denetleme hakkına sahiptir.

e. Bilgileri eksik yada hatalı gönderen birimler ile ilgili Başkan Yardımcısı ve Başkan'a bilgi verilir. Başkan veya Başkan Yardımcısı onayı ile yasal işlem başlatılır.

f. Envanter bilgileri sık sık kontrol edilmelidir.

Fiziksel Güvenlik Politikası

MADDE 16. (1) Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.

a. Kritik sistemleri olan Birimlerin bu sistemleri özel sistem odalarında tutmalıdır.

b. Sistem odaları elektrik kesintilerine ve voltaj değişkenliklerine karşı korunmalı, yangın ve benzer felaketlere karşı koruma altına alınmalı ve iklimlendirilmesi sağlanmalıdır.

c. Bilgisayar, Fotokopi, yazıcı vs. türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.

Kimlik Doğrulama ve Yetkilendirme Politikası

MADDE 17. (1) Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenmelidir.

b. Kurum sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanmalı ve dokümante edilmelidir.

c. Kurum bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve açılış ekranları olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümante edilmeli ve denetim altında tutulmalıdır.

d. Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.

e. Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

f. Sistemlere başarılı ve başarısız erişim istekleri düzenli olarak tutulmalı, tekrarlanan başarısız erişim istekleri/girişimleri incelenmelidir.

g. Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar ve rollerin sistem kaynakları üzerindeki yetkileri uygun araçlar kullanılarak belirli

aralıklarla listelenmelidir. Bu listeler yetki seviyeleri ile karşılaştırılmalıdır. Eğer uyumsuzluk varsa dokümanlar ve yetkiler düzeltilerek uyumlu hale getirilmelidir.

h. İstisnai durumlar dışında Belediye Başkanlığı bünyesindeki tüm uygulamalar için parola olmalıdır.

i. Kurum içi ve dışı kullanılan Belediye Otomasyon Sistemi kullanıcı yetkileri sırasıyla Kullanıcı, Bilgi İşlem Müdürü, Kullanıcın bağlı olduğu Birim Müdürü, bağlı olduğu Başkan Yardımcısı ve Başkan tarafından onaylanmalıdır.

Veri tabanı Güvenlik Politikası

MADDE 18. (1) Veri tabanı güvenlik kuralları aşağıda belirtilmiştir.

a. Veri tabanı sistemleri envanteri dokümante edilmeli ve bu envanterden sorumlu personel tanımlanmalıdır.

b. Veri tabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.

c. Veri tabanı sistem kayıtları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.

d. Veri tabanında kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) kaydedilmelidir.

e. Veri tabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.

f. Yedekleme planları dokümante edilmelidir.

g. Disk, Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 2 (iki) yıl süre ile güvenli ortamlarda saklanmalıdır.

h. Veri tabanı erişim politikaları "Kimlik Doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.

i. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

j. Veri tabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.

k. Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

l. Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.

m. İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.

n. Veri tabanı sunucusu sadece ssh, rdp, ssl ve veri tabanının orijinal yönetim yazılımına açık olmalı; bunun dışında ftp, telnet vb. gibi açık metin şifreli bağlantılara kapalı olmalıdır. Ancak ftp, telnet vb. açık

metin şifreli bağlantılar veri tabanı sunucudan dışarıya yapılabilmelidir.

o. Uygulama sunucularından veri tabanına login vb. şekilde erişilememelidir.

p. Veri tabanı sunucusuna ancak zorunlu hallerde "root" veya "admin" olarak bağlanılmalıdır. Root veya admin şifresi, tanımlı kişi/kişilerde olmalıdır.

q. Bağlanacak kişilere kendi adına kullanıcı adı verilmeli ve yetkilendirme yapılmalıdır.

r. Bütün kullanıcıların yaptıkları işlemler kaydedilmelidir.

s. Veri tabanı yöneticiliği yetkisi en fazla 2 (iki) kullanıcıda olmalıdır.

t. Veri tabanında bulunan şemalara, tablolara kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.

u. Veri tabanı sunucularına İnternet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir. Veri tabanı sunucularına ancak yetkili kullanıcılar erişmelidir.

v. Veri tabanı sunucularına diğer kullanıcılar bağlanıp sorgu yapmamalıdır. İstekler ara yüzden sağlanmalıdır (örnek; Kullanıcılar tablolardan "select" sorgu cümleciklerini yazarak sorgulama yapmamalıdır).

w. Veri tabanı sunucularına giden veri trafiği mümkünse şifrelenmelidir.

x. Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için Şifreleme Politikasına bakılmalıdır.

y. Veri tabanı sunucuları için yukarıda bahsedilen ve uygulanabilen güvenlik kuralları uygulama sunucuları için de geçerlidir.

Değişim Yönetim Politikası

MADDE 19. (1) Değişim Yönetim Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.

b. Yazılım ve donanım envanteri oluşturularak, yazılım sürümleri kontrol edilmelidir.

c. Herhangi bir sistemde değişiklik yapmadan önce, bu değişiklikten etkilenecek tüm sistem ve uygulamalar belirlenmeli ve dokümante edilmelidir.

d. Değişiklikler gerçekleştirilmeden önce ilgili diğer yöneticilerin onayı alınmalıdır.

e. Tüm sistemlere yönelik yapılandırma dokümantasyonu oluşturulmalı, yapılan her değişikliğin bu dokümantasyonda güncellenmesi sağlanarak kurumsal değişiklik yönetimi ve takibi temin edilmelidir.

f. Planlanan değişiklikler yapılmadan önce yaşanabilecek sorunlar ve geri dönüş planlarına yönelik kapsamlı bir çalışma hazırlanmalı ve ilgili yöneticiler tarafından onaylanması sağlanmalıdır.

g. Teknoloji değişikliklerinin Kurumun sistemlerine etkileri belirli aralıklarla gözden geçirilmelidir.

Bilgi Sistemleri Yedekleme Politikası

MADDE 20. (1) Bilgi Sistemleri Yedekleme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Belediye Otomasyon Sisteminde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgileri ve kurumsal veriler düzenli olarak yedeklenmelidir.

b. Belediye Otomasyon Sisteminde Verinin operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerinde/farklı disk sistemlerinde yedekleri alınmalıdır.

c. Belediye Otomasyon Sisteminde düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.

d. Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.

e. Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.

f. Yedek ünite üzerinde gereksiz yer tutmamak amacıyla, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.

g. Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.

h. Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.

i. Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

j. Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.

k. Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanması sağlanmalıdır.

l. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.

m. Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyaları bir felaket anında etkilenmeyecek bir ortamda bulundurulmalıdır.

n. Veri Yedekleme Standardı, yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği belirlenmelidir. Yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

o. Kullanıcıların mevcut kullandıkları bilgisayarların hard disklerindeki bilgilerin yedeklerinin alınması kullanıcıların sorumluluğundadır.

p. Belediye Veri Cihazı üzerindeki verilerin yedeklenmesi Bilgi İşlem Müdürlüğü sorumludur.

Personel Güvenliği Politikası

MADDE 21. (1) Personel Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Yetkiler Ek-4'deki kullanıcı yetkilendirme talep formu ile yapılacaktır.

b. Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.

c. Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi İnsan Kaynakları ve Eğitim Müdürlüğü tarafından araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden veya dışından referans sorulması sağlanmalıdır.

d. Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.

e. Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.

f. Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

g. İş tanımı değişen veya Kurumdan ayrılan kullanıcıların erişim hakları kaldırılması için Bilgi İşlem Müdürlüğüne bildirilmelidir.

h. Fiilen çalışanlar, kimliklerini belgeleyen kartları görünür şekilde üzerlerinde bulundurmalıdır.

i. Kurum bilgi sistemlerinin işletmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan, eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı, eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmelidir.

j. Yetkiler, "görevler ayrımı" ve "en az ayrıcalık" esaslı olmalıdır. "Görevler ayrımı", rollerin ve sorumlulukların paylaştırılması ile ilgilidir. Bu paylaşım ile kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılmalıdır. "En az ayrıcalık" ise kullanıcıların gereğinden fazla yetkiyle donatılmamasıdır.

Sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmalıdır.

k. Çalışanlar, işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler, görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar için de bu eğitim, uyum süreci sırasında verilmelidir.

l. Çalışanların güvenlik ile ilgili aktiviteleri izlenmelidir.

m. Çalışanların başka görevlere atanması ya da işten ayrılması durumlarında işletilecek süreçler tanımlanmalıdır. Erişim yetkilerinin, kullanıcı hesaplarının, token, akıllı kart gibi donanımların iptal edilmesi, geri alınması veya güncellenmesi sağlanmalı, varsa devam eden sorumluluklar kayıt altına alınmalıdır. Bu durum İnsan Kaynakları ve Eğitim Müdürlüğü tarafından Bilgi İşlem Müdürlüğüne bildirilmelidir.

E-imza Güvenliği Politikası

MADDE 22. (1) E-imza Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurum Personeli ve İmza yetkilileri Ek-5'deki E-imza talep formu ile başvuru yapılacaktır.

b. E-imzası tarafına ulaşan personel bundan sonra kullanımı, kaybolması gibi her türlü durumdan sorumludur.

c. E-imza TUBİTAK SM ile personel arasında yapılan sözleşme şartlarından sorumludur.

d. E-imza sertifikası ve okuyucusu için Başkan, Meclis Üyeleri, Başkan Yardımcıları, Müdür, idari personel ile vekâlet verebilecekleri yardımcıları başvurabilirler.

e. E-imza sertifikaları 3 yıllık alınır ve ücreti kurum tarafından ödenir. İdari görevler devam ettiği sürece kurum tarafından yenilemeler yapılır.

f. Daha önceden e-imza sertifika sahibi olan sertifikalarını kullanmaya devam edebilirler. Başvuru yapmaları gerekmez. Ancak sertifika süresi bitmeye yakın başvuru yapabilirler.

g. E-imza okuyucularını kaybeden personel ücretini kendileri yatırmak suretiyle KAMUSM web sitesinden şahsi başvuru yapabilirler.

Bakım Politikası

MADDE 23. (1) Bakım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

a. Kurum sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bunun için gerekli anlaşmalar için yıllık bütçe ayrılmalıdır.

b. Kurum envanterine kayıtlı tüm bilişim teknoloji ürünlerine bakım yapmak veya yaptırmakta yetkili Bilgi İşlem Müdürlüğüdür.

c. Kurum envanterine kayıtlı tüm bilişim teknoloji ürünlerine Ek-6'daki bakım formu düzenlenecektir.

d. Üreticilerden sistemler ile ilgili bakım prosedürleri sağlanmalıdır.
e. Firma teknik destek elemanlarının bakım yaparken "Bartın Belediye Başkanlığı Bilgi Güvenliği Politikalarına" uygun davranmaları sağlanmalı ve kontrol edilmelidir.
f. Bakım yapıldıktan sonra gerekiyorsa tüm sistem dokümantasyonu güncellenmelidir.
g. Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.
h. Sistem bakımlarından sonra bir güvenlik açığı yaratıldığından şüphelenilmesi durumunda "Bartın Belediye Başkanlığı Bilgi Güvenliği Politikaları" uyarınca hareket edilmelidir.

ÜÇÜNCÜ BÖLÜM
Çeşitli Hükümler

Yürürlük

MADDE 24. (1) Bu Yönerge Bartın Belediye Başkanının onayı ile yürürlüğe girer.

Yürütme

MADDE 25. (1) Bu Yönerge hükümlerini Bartın Belediye Başkanı yürütür.

05 / 03 / 2020

Cemal AKIN
Belediye Başkanı

EK-1. Kısaltmalar Tablosu

Kısaltma	**Tanım**
Zincir e-posta	Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip epostanın art arda diğer kullanıcılara gönderilmesi
Spam	Yetkisiz ve/veya istenmeyen reklam içerikli e-postalar
Sahte e-posta	Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişmek
RADIUS (Remote Authentication Dial-in User Service)	Sunucular uzaktan bağlanan kullanıcılar için kullanıcı ismi-şifre doğrulama, raporlama/erişim süresi ve yetkilendirme işlemlerini yapan İnternet protokolü
X.509/LDAP(Light weight Directory Access Protocol	Aktif dizin ve e-posta gibi programlardan bilgi aramak için kullanılan bir İnternet protokolü
Portal	Birden çok içeriği bir arada bulunduran alan
SSL (Secure Socket Layer)	Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla geliştirilmiş bir güvenlik protokolü
VPN	Bir ağa güvenli bir şekilde, uzaktan erişimi sağlayan teknoloji
IPSec (Internet Protocol Security) VPN	Genel ve özel ağlarda şifreleme ve filtreleme hizmetlerinin bir arada bulunduğu ve bilgilerin güvenliğini sağlayan iletişim kuralı ile uç kullanıcıya güvenli uzaktan erişim sağlama
IP	Bilgisayar ağına bağlı cihazların, ağ üzerinden birbirleri ile veri alış verişi yapmak için kullandıkları adres
MAC adresi	Bir ağ cihazının tanınmasını sağlayan kendisine özel adres
SNMP	Bilgisayar ağları üzerindeki birimleri denetlemek amacıyla tasarlanmış protokol
Firmware	Sayısal veri işleme yeteneği bulunan her türlü donanımın kendisinden beklenen işlevleri yerine getirilebilmesi için kullandığı yazılımlar
DMZ	Kurum içi ağı ile kurum dışı ağı birbirinden ayıran bölge
Uzaktan Erişim	İnternet, telefon hatları veya kiralık hatlar vasıtası ile Kurumun ağına erişilmesi
Risk	Kurumun bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörler
Güvenli Kanal	Güçlü bir şifrelemeden oluşan iletişim kanalı
Uygulama Sunucusu	Dağıtık yapıdaki bir ağda bulunan bir bilgisayarda çalıştırılan sunucu yazılımıdır. Üç katmanlı uygulamaların bir parçasıdır. Bu üç katman: Kullanıcı ara yüzü (GUI), uygulama sunucusu ve veritabanı sunucusu
Yetkilendirme	Sisteme giriş izni verilmesi, çok kullanıcılı sistemlerde sistem yöneticisi tarafından, sisteme girebilecek kişilere giriş izni ve kişilere bağlı olarak da sistemde yapabileceği işlemler için belirli izinler verilmesi
Yedekleme	Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritaba nının başkabir yere kopyalanması işlemi.
Veri tabanı	Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğu
Şifreleme	Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan özel bir algoritma
VLAN (Virtual LAN)	Sanal yerel ağ. Birçok farklı ağ bölümüne dağılmış olan, ancak aynı kabloya bağlıymışlar gibi birbiri ile iletişim kurmaları sağlanan, bir veya birkaç yerel ağ üzerindeki cihazlar grubu

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
ELEKTRONİK POSTA BAŞVURU FORMU

Aşağıda detayı bildirilen Kurumsal E-posta adresinin tarafıma açılmasını talep ediyorum. Ayrıca bu sözleşmenin 2.sayfada bulunan sözleşme maddelerini, T.C. Bartın Belediye Başkanlığı Bilgi İşlem Müdürlüğü Yönetmeliğini, Bilgi Güvenliği Politikalarını, Kanun ve yönetmelikleri okunduğumu ve bunlara uygun hareket edileceğini taahhüt ederim.

Talep Eden Kişinin;

T.C. Kimlik No		
Adı Soyadı		
Birimi		
Ünvanı		
Görevi		
Atanma Tarihi		
Cep Telefonu		
Talep Edilen E-Posta adresi	@bartin.bel.tr	
Kullanılacak E-posta adresinin kullanım amacı Açıklama	☐ Kurumsal E-posta amacıyla	☐ Proje amacıyla Proje bitiminde iptal Edilecektir.
	☐ Konferans Seminer	☐ Çalışma Grubu Diğer
Başvuru Tarihi	/ / 20___	

Başvuru Sahibinin Adı, Soyadı, imzası

Yukarıda ayrıntıları verilen personelin belirttiği gerekçeler tarafımdan incelenmiş ve talebi uygun görülmüştür.

Birim Sorumlusu Adı, Soyadı, imzası

Başkan Yardımcısı Adı, Soyadı, imzası

O L U R
__/__/20__
Cemal AKIN
Belediye Başkanı

Kemerköprü Mahallesi Elmalık Sokak No:1 Merkez / BARTIN
Telefon 0 378 227 10 25 Faks 0 378 227 40 13

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
ELEKTRONİK POSTA BAŞVURU FORMU

BARTIN BELEDİYE BAŞKANLIĞI ELEKTRONİK POSTA (e-mail) ADRESİ KULLANIM KURALLARI:

1- KANUNİ YÜKÜMLÜLÜK: ,

1.1-@bartin.bel.tr domain'i T.C. Bartın Belediyesi personeline hizmet vermektedir. Bu hizmet Bartın Belediyesinin araştırma ve geliştirme faaliyetleri içermektedir.

1.2-@bartin.bel.tr domain'ine ait e-posta hesaplarını kullanan şahıslar Türkiye Cumhuriyeti kanun ve bunlara bağlı olan yönetmeliklere, T.C. Bartın Belediyesi politikaları, yönetmeliklerine aykırı hareket edemezler.

1.2.1-İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

1.2.2-İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik

2- GİZLİLİK ve GÜVENLİK:

2.1-T.C. Bartın Belediyesi personel e-posta adresi talep eden şahısları, bu formu doldurup imzalayarak, personel kimlikleri ile birlikte Bilgi İşlem Müdürlüğüne şahsen müracaat etmeleri gerekmektedir. Diğer talepler değerlendirmeye alınmayacaktır.

2.2-Bartın Belediyesinden e-posta adresi alan kişi, Bilgi İşlem Müdürlüğünün belirleyeceği bir **e-posta hesap adı**, personel adından oluşan bir **kullanıcı adı** ve kendisinin belirleyeceği bir **kullanıcı şifresine** sahip olur.

2.3-Kullanıcı adı ve e-posta adı kişiye özeldir ve **@bartin.bel.tr** domainin de bir benzeri daha yoktur.

2.4-Kullanıcı şifresi sadece kullanıcı tarafından bilinir. Kullanıcı dilediği zaman şifresini değiştirebilir. Şifrenin seçimi ve korunması tamamıyla kullanıcının sorumluluğundadır. Bilgi İşlem Müdürlüğü, şifre kullanımından doğacak problemlerden kesinlikle sorumlu değildir.

2.5-E-posta şifresini unutan kullanıcılar, Bartın Belediyesi Bilgi İşlem Müdürlüğüne bizzat müracaat etmek zorundadır.

3- E-POSTA ADRESİ ALAN KİŞİNİN YÜKÜMLÜLÜKLERİ: Kişi;

3.1-E-posta hesabı sahibi, bu servisi kullanırken ileri sürdüğü şahsi fikir, düşünce ve ifadeler ile elektronik ortama eklediği dosya ve/veya bilgilerin sorumluluğunun şahsına ait olduğunu ve bundan dolayı bu e-posta ile ekli dosyalardan dolayı hiçbir şekilde Bartın Belediyesi sorumlu tutulmayacağını kabul eder.

3.2-Bartın Belediyesi e-posta hizmetlerinde, e-posta sitesinin geneline zarar verecek veya Bartın Belediyesi'ni başka şahıs ya da kuruluşlarla adli (mahkemelik) duruma getirecek herhangi bir yazılım veya materyal bulunduramayacağını, paylaşamayacağını ve hukuki bir durum doğarsa tüm adli ve cezai sorumlulukları üstüne aldığını kabul eder.

3.3- E-posta servisinin kullanımı sırasında kaybolacak ve/veya eksik alınacak, yanlış adrese iletilecek bilgi, mesaj ve dosyalardan Bartın Belediyesi Bilgi İşlem Müdürlüğünün sorumlu olmayacağını kabul eder.

3.4-E-posta hesabı sahibi, teknik nedenlerden (arıza, güncelleme, aktarma vb.) dolayı e-posta lardaki gecikme ve kayıplardan dolayı Bartın Belediyesi Bilgi İşlem Müdürlüğünü sorumlu olmayacağını kabul eder.

3.5-E-posta hesabı sahibi, posta hesaplarındaki verilerinin, Bartın Belediyesi Bilgi İşlem Müdürlüğünün ihmali görülmeden, yetkisiz kişilerce okunmasından (e-posta sahiplerinin, gizli bilgilerini başka kişiler ile paylaşması, siteden ayrılırken çıkış yapmaması, vb. durumlardan) dolayı gelebilecek maddi ve manevi zararlardan ötürü, Bartın Belediyesi Bilgi İşlem Müdürlüğünün sorumlu olmadığını kabul eder.

3.6- E-posta hesabı sahibi, başka şahıs veya kuruluşlardaki bilgisayara, bu bilgisayarlardaki bilgilere ya da yazılıma zarar verecek bilgi veya programlar göndermemeyi ve barındırmamayı, aksi takdirde doğacak tüm hukuki ve cezai sorumluluğun şahsına ait olduğunu kabul eder.

3.7- Bartın Belediyesi e-posta servisini kullanarak elde edilen herhangi bir bilgi veya materyalin tamamıyla kullanıcının rızası dahilinde olduğunu, kullanıcı bilgisayarında yaratacağı arızalar, bilgi kaybı ve diğer kayıpların sorumluluğunun tamamıyla kendisine ait olduğunu, e-posta servisinin kullanımından dolayı uğrayabileceği zararlardan Bartın Belediyesinin sorumlu olmadığını kabul eder.

3.8- E-posta hesabı sahibi, genel ahlak ve adaba aykırı, ırkçı, ayrımcı, ticari, siyasi propaganda, taciz ve tehdit edici ile Türkiye Cumhuriyeti yasalarına, vatandaşı olduğu diğer ülkelerin yasalarına ve uluslararası anlaşmalara aykırı e-posta göndermemeyi, barındırmamayı ve bunlara aykırı her türlü uygulamalardan doğacak cezai ve hukuki sorumluluğun şahsına ait olduğunu kabul eder.

3.9- E-posta hesabı sahibi, T.C. Kanunlara göre postalanması yasak, gizli olan bilgileri postalamamayı, barındırmamayı ve gönderilme yetkisi olamayan postaları dağıtmamayı ile bunlara ait yasal yükümlülüğü kabul eder.

3.10- E-posta hesabı sahibi, zincir posta (chain mail), yazılım virüsü vb. postaları başka posta hesaplarına dağıtmamayı, barındırmamayı ve bunlara ait cezai ve yasal yükümlülüğü kabul eder.

3.11- E-posta hesabı sahibi, rastgele ve alıcının istemi dışında mesaj (spam iletiler) göndermeyeceğini ve bunlara ait yasal yükümlülüğü kabul eder.

3.12-E-posta hesabı sahibi, e-posta **kullanıcı** adıyla yapacağı her türlü işlemden bizzat kendisinin sorumlu olduğunu kabul eder.

3.13-E-posta hesabı sahipleri, kullanım haklarını, doğrudan ya da dolaylı olarak 3. şahıslara devredemez ve kiralayamazlar.

3.14-E-posta hesabı sahibi yasa ve kurallara aykırı davrandığı takdirde Bartın Belediyesi Bilgi İşlem Müdürlüğünün gerekli müdahalelerde bulunma, kişiyi hizmet dışına çıkarma ve üyeliğine son verme hakkına sahip olduğunu kabul eder.

3.15- E-posta hesabı sahibi, yasa ve kurallara aykırı davrandığı takdirde T.C. Bartın Belediyesi makamlarının; gerekli sözlü ve yazılı uyarıda bulunmaya, kişiyi sınırlı veya sınırsız hizmet dışına çıkarmaya, Belediye içi idari soruşturma başlatmaya ya da adli yargıya bildirimde bulunma hakkına sahip olduğunu kabul eder.

3.16- E-posta hesabı sahibi, e-posta hesabını tek taraflı olarak iptal ettirse bile, bu iptal işleminden önce, üyeliği sırasında gerçekleştirdiği icraatlardan kendisinin sorumlu olacağını kabul eder.

3.17- E-posta sahibi, Bartın Belediyesi e-posta hizmetinden yararlandığı sırada, kayıt formunda yer alan bilgilerin doğru olduğunu ve bu bilgilerin gerekli olduğu (şifre unutma gibi) durumlarda, bilginin hatalı veya noksan olmasından doğacak zararlardan dolayı sorumluluğun kendisine ait olduğunu, bu hallerde e-mail adresinin iptal edileceğini kabul eder.

3.18- T.C. Bartın Belediyesi Bilgi İşlem Müdürlüğü, kullanıcıların bilgisi olmaksızın E-posta hizmetleri servis politikasında değişiklik yapma hakkına sahiptir. Kullanıcılar bu metinde yer alan bilgileri izlemek ve olası değişikliklerden haberdar olmakla yükümlüdürler.

3.20-Tüm bu maddeleri daha sonra hiçbir itiraza mahal vermeyecek şekilde okuduğunu, **KABUL ve TAAHHÜT ETMİŞTİR.**

4- YÜRÜRLÜLÜK: Kullanıcı, adına düzenlenmiş bu formu doldurup, imzaladıktan sonra bu sözleşme yürürlüğe girer ve T.C. Bartın Belediyesi olduğu sürece devam eder.

Başvuru Sahibinin Adı, Soyadı, imzası	

Kemerköprü Mahallesi Elmalık Sokak No:1 Merkez / BARTIN
Telefon 0 378 227 10 25 Faks 0 378 227 40 13

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
İNTERNET YETKİLENDİRME TALEP FORMU

Aşağıda detayı bildirilen ayrıcalıklı erişim hakkının görevim nedeniyle tarafıma verilmesi hususunda gereğini saygılarımla arz ederim.

Talep Eden Kişinin;

T.C. Kimlik No		
Adı Soyadı		
Birimi		
Ünvanı		
Görevi		
IP / MAC adresi	/	
Cep Telefonu		
E-Posta	@bartin.bel.tr	
Kullanıcı Tipi	☐ Standart Kullanıcı	☐ Araştırmacı Kullanıcı
Açıklama		

Ayrıcalıklı erişim hakkının kurum politikasına uygun ve işlerimin tamamlanabilmesi açısından gerekli olduğunu, statüsü değiştiğinde ayrıcalıklı erişim hakkının iptalini bildireceğimi, aksi takdirde bu IP, MAC adresinin ayrıcalıklı erişim haklarından doğacak zararların sorumluluğunu kabul ettiğimi beyan ederim.

Başvuru Sahibinin Adı, Soyadı, imzası

Yukarıda detayları belirtilen ayrıcalıklı internetin gerekçeleri tarafımdan incelenmiş ve talebi uygun görülmüştür.

Birim Sorumlusu Adı, Soyadı, imzası

Başkan Yardımcısı Adı, Soyadı, imzası

O L U R
__/__/20__
Cemal AKIN
Belediye Başkanı

NOT :

1. ***Bu form ıslak imzalı olarak düzenlenip EBYS üzerinden Bilgi İşlem Müdürlüğüne bir üst yazı ekinde gönderilecektir. Eksik bilgilerin olması veya anlaşılır olmaması halinde işleme alınmayacaktır.***
2. *Standart Kullanıcı haber siteleri, kamu kurum siteleri gibi,*
3. *Araştırmacı Kullanıcı sosyal medya, video siteleri, 5651 sayılı kanun, BTK erişim engeli olan ve ağ trafiğini artıran siteler hariç diğer tüm siteler gibi.*

Kemerköprü Mahallesi Elmalık Sokak No:1 Merkez / BARTIN
Telefon 0 378 227 10 25 Faks 0 378 227 40 13

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
KULLANICI YETKİLENDİRME TALEP FORMU

Aşağıda detayı bildirilen Platform ve Modüllerin görevim nedeniyle tarafıma verilmesi hususunda gereğini saygılarımla arz ederim.

Talep Eden Kişinin;

T.C. Kimlik No		
Adı Soyadı		
Birimi		
Ünvanı		
Görevi		
Atanma Tarihi		
Cep Telefonu		
E-Posta	@bartin.bel.tr	
Platform	☐ İçişleri Bakanlığı e-Belediye	☐ Belediye Otomasyon Sistemi (WİNKENT)
Açıklama		

Platform Adı	Asıl Ek	Modül Adı Ve Sayfa Yetkileri	Modül		Veri Kayıtlarında					
			Verilsin	İptal edilsin	Ekleme	Yenileme	Silme	Sorgulama	Gezinme	Yazdırma
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐

Kemerköprü Mahallesi Elmalık Sokak No:1 Merkez / BARTIN
Telefon 0 378 227 10 25 Faks 0 378 227 40 13

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
KULLANICI YETKİLENDİRME TALEP FORMU

Platform Adı	Asil Ek	Modül Adı Ve Sayfa Yetkileri	Modül		Veri Kayıtlarında					
			Verilsin	İptal edilsin	Ekleme	Yenileme	Silme	Sorgulama	Gezinme	Yazdırma
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐
			☐	☐	☐	☐	☐	☐	☐	☐

Yukarıda ayrıntıları verilen personelin belirttiği gerekçeler tarafımdan incelenmiş ve talebi uygun görülmüştür.

Birim Sorumlusu Adı, Soyadı, imzası		Başkan Yardımcısı Adı, Soyadı, imzası

O L U R __/__/20__ Cemal AKIN Belediye Başkanı

NOT :

1. ***Bu form ıslak imzalı olarak düzenlenip EBYS üzerinden Bilgi İşlem Müdürlüğüne bir üst yazı ekinde gönderilecektir. Eksik bilgilerin olması veya anlaşılır olmaması halinde işleme alınmayacaktır. İşleme alınmadığı ilgili personele EBYS üzerinden duyurulacaktır.***
2. *e-Belediye EBYS sayfa yetkileri belirtilmelidir. Örnek Birim düzeyinde "Gelen Evrak Sayfa Grubu", "Evrak İşlem Sayfa Grubu" gibi.*
3. *Belediye Otomasyonu Modülleri belirtilmelidir. Örnek Muhasebe, Satınalma, Su tahakkuk gibi.*
4. *Birimi alanına görevde bulunduğu birimi ve ek birim görevleri yazılmalıdır. Örneğin Yazı İşleri Müdürlüğü asıl görevi ek görev Encümen, Meclis Sekretarya görevleri gibi ek birimler.*
5. *Kullanıcıların yetkileri görevler ayrılığı ilkelerine göre verilmelidir.. Bkz. "Belediye Bilgi Güvenliği Politikaları Yönergesi"*

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
KULLANICI YETKİLENDİRME TALEP FORMU

Aşağıda detayı bildirilen Platform ve Modüllerin görevim nedeniyle tarafıma verilmesi hususunda gereğini saygılarımla arz ederim.

Talep Eden Kişinin;

T.C. Kimlik No		
Adı Soyadı		
Birimi		
Ünvanı		
Görevi		
Atanma Tarihi		
Cep Telefonu		
E-Posta	@bartin.bel.tr	
Platform	☐ İçişleri Bakanlığı e-Belediye	☐ Belediye Otomasyon Sistemi (WİNKENT)
Açıklama		

Platform Adı	**Asıl Ek**	**Modül Adı Ve Sayfa Yetkileri**	**Modül**		**Veri Kayıtlarında**					
			Verilsin	**İptal edilsin**	**Ekleme**	**Yenileme**	**Silme**	**Sorgulama**	**Gezinme**	**Yazdırma**
			☐	☐	☐	☐	☐	☐	☐	☐

Yukarıda ayrıntıları verilen personelin belirttiği gerekçeler tarafımdan incelenmiş ve talebi uygun görülmüştür.

Birim Sorumlusu Adı, Soyadı, imzası

Başkan Yardımcısı Adı, Soyadı, imzası

O L U R __/__/20__ Cemal AKIN Belediye Başkanı

NOT :*Bu form ıslak imzalı olarak düzenlenip EBYS üzerinden Bilgi İşlem Müdürlüğüne bir üst yazı ekinde gönderilecektir. Eksik bilgilerin olması veya anlaşılır olmaması halinde işleme alınmayacaktır. İşleme alınmadığı ilgili personele EBYS üzerinden duyurulacaktır.* *e-Belediye EBYS sayfa yetkileri belirtilmelidir. Örnek Birim düzeyinde "Gelen Evrak Sayfa Grubu", "Evrak İşlem Sayfa Grubu" gibi.Belediye Otomasyonu Modülleri belirtilmelidir. Örnek Muhasebe, Satınalma, Su tahakkuk gibi.Birimi alanına görevde bulunduğu birimi ve ek birim görevleri yazılmalıdır. Örneğin Yazı İşleri Müdürlüğü asıl görevi ek görev Encümen, Meclis Sekretarya görevleri gibi ek birimler.Kullanıcıların yetkileri görevler ayrılığı ilkelerine göre verilmelidir.. Bkz. "Belediye Bilgi Güvenliği Politikaları Yönergesi"*

Kemerköprü Mahallesi Elmalık Sokak No:1 Merkez / BARTIN
Telefon 0 378 227 10 25 Faks 0 378 227 40 13

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
NİTELİKLİ ELEKTRONİK SERTİFİKA (E-İMZA) BAŞVURU FORMU

Aşağıda detayı bildirilen idari görevim nedeniyle resmi evraklarda ıslak imza atma yetkim bulunmaktadır. İçişleri Bakanlığı e-Belediye sistemi, idarenin kullanacağı digital platformlarda ve Elektronik Belge Yönetim Sistemi (EBYS) otomasyonunda ıslak imza yerine kullanılacak e-imza için Kamu Sertifikasyon Merkezi'nden (KAMUSM) şahsıma Nitelikli Elektronik Sertifika (NES) ve USB E-imza Kart Okuyucu cihaz alınması hususunda;

Gereğini saygılarımla arz ederim.

E-İmza Talep Eden Kişinin;

T.C. Kimlik No	
Adı Soyadı	
Birimi	
Ünvanı	
Görevi	
Atanma Tarihi	
Cep Telefonu	
E-Posta	@bartin.bel.tr
Talep Nedeni	○ İlk sertifika ○ Kimlik bilgisi güncelleme ○ Yenileme ○ Para limiti güncelleme ○ Akıllı kart kayıp/çalıntı ○ Donanım arızası ○ PIN/PUK kayıp/çalıntı ○ Diğer
Nitelikli Elektronik Sertifika (NES)	○ İstiyorum ○ İstemiyorum
Kart Okuyucu	○ İstiyorum ○ İstemiyorum

Başvuru Sahibinin Adı, Soyadı, imzası

Yukarıda ayrıntıları verilen personelimizin belirttiği gerekçeler tarafımdan incelenmiş ve talebi uygun görülmüştür.

Birim Sorumlusu Adı, Soyadı, imzası

Başkan Yardımcısı Adı, Soyadı, imzası

O L U R __/__/20__ Cemal AKIN Belediye Başkanı

NOT :

1. E-imza sertifikası ve okuyucusu için Başkan, Meclis Üyeleri, Başkan Yardımcıları, Müdür, idari personel ile vekâlet verebilecekleri yardımcıları başvurabilirler.
2. E-imza sertifikaları 3 yıllık alınır ve ücreti kurum tarafından ödenir. İdari görevler devam ettiği sürece kurum tarafından yenilemeler yapılır.
3. Daha önceden e-imza sertifika sahibi olan sertifikalarını kullanmaya devam edebilirler. Başvuru yapmaları gerekmez. Ancak sertifika süresi bitmeye yakın başvuru yapabilirler.
4. E-imza okuyucularını kaybeden personel ücretini kendileri yatırmak suretiyle KAMUSM web sitesinden şahsi başvuru yapabilirler.
5. ***Bu form ıslak imzalı olarak düzenlenip EBYS üzerinden Bilgi İşlem Müdürlüğüne bir üst yazı ekinde gönderilecektir. Eksik bilgilerin olması halinde işleme alınmayacaktır.***

BARTIN BELEDİYE BAŞKANLIĞI
BİLGİ İŞLEM MÜDÜRLÜĞÜ
TEKNİK SERVİS BAŞVURU FORMU

Kuruma ait bilişim teknoloji ürünü aşağıda detayı bildirildiği şekilde arızalanmıştır. Gereğinin yapılmasını saygılarımla arz ederim.

Teknik Servis Talep Eden Kişinin;

Adı Soyadı		Sorun Açıklaması
Birimi		
Ünvanı		
Görevi		
Talep Tarihi		
Cep Telefonu		
E-Posta	@bartin.bel.tr	
Sorun	○ Montaj ○ İşletim Sistemi Kurulumu ○ Yenileme ○ Donanım ○ Yazılım ○ Bilgisayar Ağı	
Teslim Edilen		
Bulunduğu Kat-Oda No-Data Priz No-Mac Adres		
Marka-Model-S/N		

1. Onarım için gönderilen cihazın, yapılan işlem sonucunu, yetkili kişiye (**e-posta veya telefon ile**) bildiriliş tarihinden itibaren **1-HAFTA** içerisinde alınması gerekmektedir. Alınmayan cihazlardan **BİLGİ İŞLEM MÜDÜRLÜĞÜ** sorumlu **DEĞİLDİR.**
2. Bilgisayar içindeki bilgilerin sorumluluğu kullanıcılara aittir. Bilgi kaybından **BİLGİ İŞLEM MÜDÜRLÜĞÜ** sorumlu **DEĞİLDİR.**
3. Bilgisayarda kullanılan **LİSANS 'SIZ** yazılımların (Programların) sorumluluğu Bilgisayar Kullanıcılarına aittir. İlerde oluşabilecek sorunlardan **BİLGİ İŞLEM MÜDÜRLÜĞÜ** sorumlu **DEĞİLDİR.**

Başvuru Sahibinin Adı, Soyadı, imzası	Birim Sorumlusu Adı, Soyadı, imzası

Teknik Servis Hizmeti Sonucu;

	Açıklamalar
Yedek Makine Verildi	
Sorun Çözüldü	
İlgili Servise Gönderildi	
Ek Bilgi	

İşe Başlama Tarih/Saat	…/…/20.. -- … : …	İşi Bitirme Tarih/Saat	…/…/20.. -- … : …

İşlemi Yapan Adı, Soyadı, imzası	Teslim Eden Adı, Soyadı, imzası	Teslim Alan Adı, Soyadı, imzası

Kemerköprü Mahallesi Elmalık Sokak No:1 Merkez / BARTIN
0 (378) 227 10 25