1b

Kişisel Verilerin Korunması ve Parola Yönetimi Politikası

sürüm 1.0

accert.com.tr
Haziran 2022 Ankara

	MALATYA TİCARET BORSASI	Doküman No : KVK-1.B
	KİŞİSEL VERİLERİN KORUNMASI ve PAROLA YÖNETİMİ POLİTİKASI	Sayfa No :
		Yayın Tarihi : 30.06.2022
		Sürüm : 1.0

Hazırlayan:	Sistem Onayı:	Yürürlük Onayı:
Kişisel Veri Koruma Yöneticisi	Kalite Yöneticisi	Genel Sekreter

REVİZYON TAKİBİ

Revizyon No	: 01	Açıklama:
Tarih	: 30.06.2022	
Dağıtım	: Tüm Bölüm ve Birimler	

PAROLA YÖNETİMİ POLİTİKA BELGESİNİN İÇERİK VE NİTELİĞİ

Bu Politika Belgesi, [**MALATYA TİCARET BORSASI**] için yapılan 6698 sayılı Kişisel Verilerin Korunması Kanunu'na Uyumluluk çalışmaları kapsamındaki bulgu ve değerlendirmeleri içerir.

Bu bulgu ve değerlendirmeler, [**MALATYA TİCARET BORSASI**] tarafından ACCERT Sertifikasyon Belgelendirme Danışmanlık Eğitim ve Denetim A.Ş (ACCERT A.Ş.) ile paylaşılan bilgi, belge ve beyanlar ölçüsünde, KVKK mevzuatı ile verilerin depolanıp işlendiği ortamlar temel alınarak hazırlanmıştır. ACCERT A.Ş. danışmanlık hizmetini, danışmanlık hizmetinin verildiği tarihteki yasal mevzuat ve mevcut düzenlemeler ile [**MALATYA TİCARET BORSASI**'nın] kendisi ile paylaştığı bilgi ve veriler kapsamında sağlamış olup [**MALATYA TİCARET BORSASI**'nın] kendisiyle paylaşmadığı veyahut sonradan mevzuat değişikliği, içtihat değişiklikleri gibi sebeplerle uygulamada ortaya çıkacak farklılıklar nedeniyle ACCERT A.Ş.'nin herhangi bir sorumluluğu bulunmamaktadır.

Ayrıca, bu belgede yer alan değerlendirme ve öneriler tavsiye niteliğinde olup özellikle verilerin toplanması, işlenmesi, aktarılması ve yok edilmesi konusundaki idari ve teknik tedbirlerin KVKK düzenlemelerine uygun biçimde uygulanması konusundaki sorumluluk ve riskler [**MALATYA TİCARET BORSASI**'nın] uhdesindedir. Kişisel veriler ile ilgili bilgilerin güncel ve doğru olarak işlenmesi için gerekli önlemlerin alınması [**MALATYA TİCARET BORSASI**'nın] sorumluğundadır.

KVKK düzenlemelerinin öngördüğü bütün tedbirlerin yanı sıra uygulamadan kaynaklanabilecek risklerin yönetimi ve bunların önlenmesine için gerekli denetim sorumluluğu (KVKK Madde 12 (3)) Veri Sorumlusu olarak [**MALATYA TİCARET BORSASI**'ya] ait olup, ilgili iş birimlerinin beyan etmediği veya eksik beyan ettiği bilgiler nedeniyle ortaya çıkabilecek zararlar başta olmak üzere, [**MALATYA TİCARET BORSASI**'nın] yükümlülüklerini gereği gibi yerine getirilmesine rağmen diğer nedenlerden oluşabilecek doğrudan veya dolaylı zararlardan ACCERT A.Ş. sorumlu değildir.

İÇİNDEKİLER

1. Amaç

Bu politikanın amacı, personelin tüm bilgi sistemleri uygulamalarında ve kurumsal e-posta hesaplarında kullanılacak olan parolaların üretilmesi, korunması, kullanılması ve değiştirilme sıklığı hakkında kurumsal bir standart oluşturmaktır.

Ayrıca, [BORSA] bünyesinde her türlü sisteme erişim için kullanılan/kullanılabilecek kullanıcı adı ve parola ile erişim sağlanan sistemlerin güveliği için gerekli parolaların minimum gereksinimleri bu politika belgesinde tanımlanmıştır.

2. Kapsam

[BORSA] bünyesinde çalışan tüm personel ve çalışan sistemler bu politika kapsamındadır. [Uygulama kapsamı ise [BORSA] Bilgi Güvenliği Prosedürü metninde yer alan kapsam maddesinde belirlenmiş olan kapsamdır.]

3. Sorumlular

Bu prosedürün oluşturulmasından Bilgi Teknolojileri (BT) Yönetim Temsilcisi sorumludur. Politikanın uygulanmasından tüm [BORSA] personeli sorumludur.

4. Parola Politikası

Güçlü parola politikası, bilgi güvenliğinin sağlanması açısından kritik bir öneme sahip olup, varlıkların yetkisiz erişimlerinden korunması açısından kullanıcı hesaplarında en önemli güvenlik katmanını teşkil etmektedir. Zayıf seçilmiş bir parola ağ ve sistem güvenliği başta olmak üzere tüm altyapıyı, uygulamaları ve verileri riske atabilir. Uzaktan erişenler dahil tüm [BORSA] personeli ve öğrencileri aşağıdaki tanımlanmış genel kurallara uymakla sorumludur.

a. Parola Oluşturma Kuralları(Genel)

Parolalar en az 8 karakter uzunluğunda olmalıdır ve bu karakterlerin en az bir tanesi sayılardan, bir tanesi büyük harf bir tanesi de küçük harften oluşmalıdır. Aşağıdaki karakterlerin en az üçünü içermelidir;

- Büyük harf, (ABCDEF vb.)
- Küçük harf, (abcdef vb.)
- Rakam, (1234567890)
- Noktalama işareti, (!?., vb.)
- Özel karakterler (@#$%^&*() _+|~=\`{}[]:";'<>/ vb)

Parolalar aşağıdaki şekilde oluşturulmamalıdır;

- İçeriğinde, kişisel bilgiler bulunmamalıdır (örneğin aile bireylerinin isimleri, doğum tarihleri, telefon numarası veya adres bilgileri gibi)
- Kelime veya rakam dizileri kullanılmamalıdır. (Örn; aaabbb, qwerty, zyxwvuts, 12345678, 123321, vb.)
- Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda BT Birimi tarafından yapılan farkındalık eğitimleri ve farkındalık e-postaları ile düzenli aralıklarla bilgilendirilir.
- Kurum çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu yönergenin ilgili maddelerinde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.
- Bütün parolalar (kurum adı yazınız) ait gizli bilgi niteliğindedir. Paylaşılamaz, kâğıtlara ya da elektronik ortamlara yazılamaz.
- Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılması bilgi güvenliği açısından sakıncalı olup, kullanıcılara farkındalık eğitimlerinde bu hususun önemi iletilir.
- Parola kırma ve tahmin etme operasyonları belli aralıklar ile güvenlik tatbikatlarında gerçekleştirilir. Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilir.

b. Parola Oluşturma Kuralları(Sistem)

- ✓ Tüm kullanıcı hesaplarına ait bir parola vardır.
- ✓ Yeni kullanıcı hesaplarına ait parolaların ilk kez giriş yapılırken kullanıcı tarafından kurallara uygun olarak tanımlanması sağlanır.
- ✓ Başarısız parola denemeleri üst üste 3 kere ile sınırlandırılmıştır. Üçüncü denemeden sonra şifre ve bağlı olduğu kullanıcı, kullanım dışı bırakılır. Parolanın yenilenmesi için konu ile ilgili çağrı açılır. Eğer kullanıcı çalışan ise kimlik ile birlikte BT Sistem Destek birimine şahsen gelmesi gerekmektedir.
- ✓ Yazılan parolanın ekranda görünmemesi veya maskelenerek görünmesi sağlanır.
- ✓ Kullanıcı parolaları, saklandıkları ortamlarda, geri dönüşü mümkün olmayan bir şekilde maskelenerek korunur (örneğin Hash), bu sayede en yetkili kişilerin bile kullanıcı parolasını görmesi engellenir.
- ✓ Bilgi kaynaklarına başarılı ve başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydı tutulur.
- ✓ Kullanıcıların kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında (sisteme parola ile giriş yapıldıktan sonra sistem açık bırakılması halinde) en geç 30 dakika sonra otomatik olarak kapanması (sistemin kilitlenmesi) sağlanır.
- ✓ Halka açık veya paylaşılan ağlardan iletilen kimlik bilgileri güçlü şifreleme metotları ile (SSL,TLS) korunur.
- ✓ Başkaları tarafından öğrenildiğinden şüphelenilen parolalar hemen değiştirilir.

c. Parola Kullanım Kuralları(Sistem Yönetim Birimi)

- ✓ Bütün sistem seviyesinde kullanılan parolalar (örnek: root, administrator, vb.) ve kullanıcı hesaplarına ait parolalar (örnek: e-posta, web, masaüstü bilgisayar vs.) en geç 6 (altı) ayda bir değiştirilmelidir.
- ✓ Sistem yöneticileri, kendi yönetimindeki sistem ve kendi kullanıcı hesapları için farklı parolalar kullanmalıdır.
- ✓ Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- ✓ Parolalar herhangi bir yerde not edilerek saklanmamalıdır.
- ✓ Parolalar güçlü (örnek: parola uzunluğu, karakter çeşitliliği, sözlük dışı ifadeler gibi) sayılabilecek nitelikle özellikleri barındırmalıdır.
- ✓ Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının parolaları da kolayca kırılamayacak güçlü bir yapıya sahip olmalıdır.

Tüm kullanıcılar:

- ✓ Her yeni parola için, son kullanılan 3 paroladan farklı yeni bir parola kullanılmalıdır.
- ✓ Parolalar hiç kimse ile paylaşılmamalıdır.
- ✓ Parolaların klavyeden girilmesi sırasında dikkatli olunmalı ve çevredeki kişilerin görmesine izin vermeyecek şekilde girilmelidir.
- ✓ E-posta yoluyla parolaların onaylanması veya güncellenmesi istenmez, bu yönde gelen e-postalar dikkate alınmamalıdır.
- ✓ Parolaların e-posta iletilerine veya herhangi bir elektronik forma eklenmesi yasaktır.
- ✓ Aynı parola birden fazla kaynakta kullanılmamalıdır.
- ✓ Parolalar ilave bir şifreleme metodu kullanılmadan hatırlamak amacıyla kayıt edilmemelidir (kâğıt, bilgisayardaki bir dosya, cep telefonu gibi ortamlarda saklanmamalıdır).
- ✓ İnternet tarayıcılarında (internet explorer, chrome, firefox vb.) “Parolayı hatırla” seçeneğinin kişisel bilgisayarlar dışında kullanılması yasaktır, kişisel bilgisayarlarda ise bir güvenlik açığı olduğu hatırlanmalıdır.

d. Parola Oluşturmada Dikkat Edilecek Noktalar

Parolalar aşağıda detayları verilen “zayıf parola” yapısından uzak olmalı ve “güçlü parola” yapısına uygun olmalıdır.

Zayıf Parolalar

Zayıf parolalar aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip özelliklerden parola seçiminden kaçınmalıdır.

- ✓ Zayıf Parolalar 6 veya daha az karaktere sahiptirler.
- ✓ Zayıf Parolalar aşağıdaki gibi ortak değere sahiptir.
  - Harf ve rakamlardan karmaşık oluşmayan
  - Sözcükte geçen kelimelerden oluşturulan
  - Bilgisayar terminolojisi vb. isimleri: komutlar, siteler, şirketler, donanım, yazılım vb.
  - ”Ahmet”, ”Mersin”, ”Deniz” gibi özel isimler.
  - Doğum tarihi, adres ve telefon numaraları gibi kişisel bilgiler.
  - Aaabbb, qwerty, zyxwuts, 123321 vb. gibi sıralı harf veya rakamlar.
  - Yukardaki herhangi bir kelimenin geri yazılış şekli.
  - Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek, gizli1, gizli2).

Güçlü Parolalar

Güçlü parolalar aşağıdaki karakteristiklere sahip olup kullanıcılar bu tip parola kurallarını uygulamalıdır:

- ✓ Hem küçük hem de büyük karakterlere sahiptir (örnek, a-z, A-Z)
- ✓ Hem sayısal hem de noktalama karakterleri gizi özel karakterlere sahiptir. (0-!@#$%^&*()_+|~=\`{}[]:";'<>?,./)
- ✓ Sözlük isimleri gibi kelime bilgilerine ait olmamalıdır.
- ✓ Parolalar herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Karmaşık parolaları seçerken, herhangi bir yere yazmadan kolayca hatırlanabilen parolalar oluşturulmalıdır.
- ✓ Kurum içinde kullanılması zorunlu olan şifre politikası minimum 8 karakterden oluşan en az bir büyük harf, en az bir küçük harf ve en az bir sayı karakteri barındıran parolalardır.

Not: Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.

e. Parolaların Korunması

Bütün kullanıcılar aşağıdaki kurallara titizlikle uymalıdır.

- ✓ Kurum bünyesinde kullanılan parolalar, kurum dışında herhangi bir şekilde kullanılmamalıdır. (örnek: internet erişim parolaları, bankacılık işlemlerinde veya diğer yerlerde).
- ✓ Değişik sistemler için farklı parolalar kullanılmalıdır. Örnek: Unix sistemler için farklı parolalar, Windows sistemler için farklı parolalar.
- ✓ Kurum bünyesinde kullanılan parolalar hiç kimseyle paylaşılmamalıdır. Bütün parolalar kurum ait özel bilgiler olarak düşünülmelidir.
- ✓ Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda BT Birimi tarafından yapılan farkındalık eğitimleri ve farkındalık e-postaları ile düzenli aralıklarla bilgilendirilir.
- ✓ Hiçbir kişiye kendisine ait parolayı sözlü veya yazılı telefonla paylaşmamalıdır.
- ✓ Üst yönetici dahil hiç kimseye parola söylenmemelidir.
- ✓ Başkaları önünde parolalar hakkında konuşulmamalıdır.
- ✓ Aile bireylerine ait isimler parola olarak kullanılmamalıdır.
- ✓ Herhangi form üzerinde parola belirtilmemelidir.
- ✓ Parolalar aile bireyleri ile paylaşılmamalıdır.
- ✓ Parolalar, işten uzakta olunan zamanlarda iş arkadaşlarına söylenmemelidir.
- ✓ Uygulamalardaki “parola hatırlatma” özellikleri parola olarak seçilmemelidir. (örnek: Outlook, Internet Explorer vs.)

5. Yaptırım

- ✓ Bu politikanın ihlal edilmesi durumunda BT yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir.
- ✓ İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır.
- ✓ Personel BT Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.
- ✓ Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse personel hakkında işlem yapılır.
- ✓ Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, "Veri Güvenlik İhlal Yönetim Politika" belgesinde
- ✓ tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

6. İlgili Dokümanlar

Veri Güvenlik İhlal Yönetim Politikası