İÇİNDEKİLER

İÇİNDEKİLER....1
1. AMAÇ....2
2. KAPSAM....2
3. SORUMLULAR....2
4. TANIM....2
5. UYGULAMA....2
5.1. ŞİFRE ve PAROLA POLİTİKASI....2
5.1.1. PAROLA VE ŞİFRE KULLANIMI....2
5.2. KRİPTOGRAFİ POLİTİKASI....3
5.2.1. KRİPTOGRAFİK KONTROLLERİN KULLANIMI POLİTİKASI....3

Bayburt Üniversitesi'nin, KVKK, DDO ve BGYS ile ilgili uyması gereken bazı kurallar aşağıda belirtilmiştir.

1. AMAÇ

Bayburt Üniversitesi içinde kullanıcı parola politikası, şifre politikası ve kriptografik kontroller politikası kullanım haklarını erişim kurallarını tanımlamak.

2. KAPSAM

Bilgi İşlem Daire Başkanlığı'nın hizmetlerinden yararlanan kapsama dâhil tüm kullanıcı ve birimleri kapsar.

3. SORUMLULAR

Kapsama dâhil tüm kullanıcıların bu politikaya ve erişim haklarına uygun hareket etmesi Rektörlüğün sorumluluğundadır.

4. TANIM

BAYÜ: Bayburt Üniversitesi

KVKK: Kişisel Verileri Koruma Kanunu

CB: Cumhurbaşkanlığı

DDO: Dijital Dönüşüm Ofisi

BGYS: Bilgi Güvenliği Yönetim Sistemi

KVYS: Kişisel Verileri Yönetim Sistemi

5. UYGULAMA

5.1. ŞİFRE ve PAROLA POLİTİKASI

Bayburt Üniversitesi Bilgi işlem Daire Başkanlığı'nın Active Directory üzerinde işlem gören tüm kullanıcıların, şifre ve parola kullanımında uyması gereken bazı kurallar aşağıda belirtilmiştir.

5.1.1. PAROLA VE ŞİFRE KULLANIMI

- Herhangi bir parola, "Çok Gizli" bilgi olarak muhafaza altına alınacak ve iş arkadaşı veya başka bir kişiyle paylaşılmayacaktır. Paroladan kaynaklanan problemlerde sorumluluk hesap sahibine aittir.
- Bilgisayar sistemlerine ve tüm şifre gerektiren uygulamalara boş parola ile erişmek mümkün olmayacaktır.

- Hiçbir m kullanıcı adını ve kullanıcı ile ilgili bir bilgiyi (doğum tarihi, telefon numarası vs.) parola olarak kullanamaz.
- Acil durumlarda, yönetici onayı doğrultusunda parolalar BİDB tarafından resetlenerek yeni şifre tahsisi yapılır.
- Parolaların ilgili kişi ile paylaşımında uygun ve güvenli yöntemler kullanılmalıdır (Örneğin parola sms ile gönderilirken, kullanıcı adı mail ile gönderilebilir.).
- Parolalar hatırlanmak maksadıyla; kâğıt ortamına yazılmayacak ve görülecek mekânlara açık bir şekilde masalara, monitör üstlerine konulmayacaktır. Bu durumların oluşması halinde sorumluluk parola sahibine ait olacaktır.
- Parolalar en az 8 haneli olup; harf, özel karakter ve rakam kombinasyonundan oluşması gerekmektedir.
- Kullanıcının parolasını unutması veya değiştirmek istemesi durumunda; BAYÜ Şifre Güncelleme sistemine giriş yaparak öncelikle TCKN ve Kurum Sicil Numarası bilgisini doğrulamalıdır. Ardından GSM numarasına gelen kodu sisteme girmesi durumunda yeni şifresini oluşturur.
- Şifreler 6 ay süren aralıklarla değiştirilmelidir.
- Personel kullanıcıları uygulamalara girişte kullanıcı adları "adsoyad@bayburt.edu.tr" (kullanıcı adı dolu olması durumunda farklı kombinasyonla verilmektedir), öğrenciler "ogrenciNo@stu.bayburt.edu.tr" olarak tanımlanır.
- Kullanıcı maillerindeki parolalar yukarıda ifade edildiği şekilde parola politikasına uygun olarak verilir.

5.2. KRİPTOGRAFİ POLİTİKASI

5.2.1. KRİPTOGRAFİK KONTROLLERİN KULLANIMI POLİTİKASI

BAYÜ'ye ait "Kuruluşa özel" ve "gizli" bilgilerin yetkisiz erişimlerden korunması için kriptolanarak saklanması gerekmektedir. Sunuculara erişim şifrelidir. Statik IP kontrolü veya VPN ile bağlanılır. (Kullanıcı adı- şifre, Yazılım için Token Kodu) Kripto kullanımında dikkat edilmesi gereken hususlar aşağıda tanımlanmıştır. (E-imza, kep-mobil imza, EBYS, e-fatura da kullanılmaktadır.)

1. Kriptografik kontroller aşağıdaki maksatlarla kullanılır.
   i. **Gizlilik:** Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması.
   ii. **Bütünlük/Güvenilirlik:** Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması.
   iii. **İnkâr edilemezlik:** Bir olay veya faaliyetin oluştuğunun veya oluşmadığının kanıtını elde etmek için kriptografik tekniklerin kullanılması.
2. Bu politikanın uygulanmasından kurum sorumludur.
3. Organizasyon çapında etkin bir uygulama için uyarlanması gereken standartlar takip edilmelidir.
4. İlgili otoritelerle ile yapılan dosya transferlerinde bilginin gizliliği ve hassaslığından dolayı kriptolu özel programlar ve anahtarlama yöntemleri kullanılmaktadır.