

1. AMAÇ:

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde kurumun gizliliği, aslına uygunluğu ve/veya bütünlüğünün korunması için Kriptografi'nin doğru ve etkin kullanımını temin etmek.

2. KAPSAM:

Bu talimat Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığındaki tüm kriptografik kontrollerini kapsar.

3. YASAL DAYANAK: -

4. SORUMLULAR

Sistem Yöneticileri: Sunucu, işletim sistemi, sanallaştırma ve veri tabanı yapılandırmalarından sorumludur.

Ağ Yöneticileri: Switch, router, firewall, kablosuz sistem gibi ağ cihazlarını yönetir.

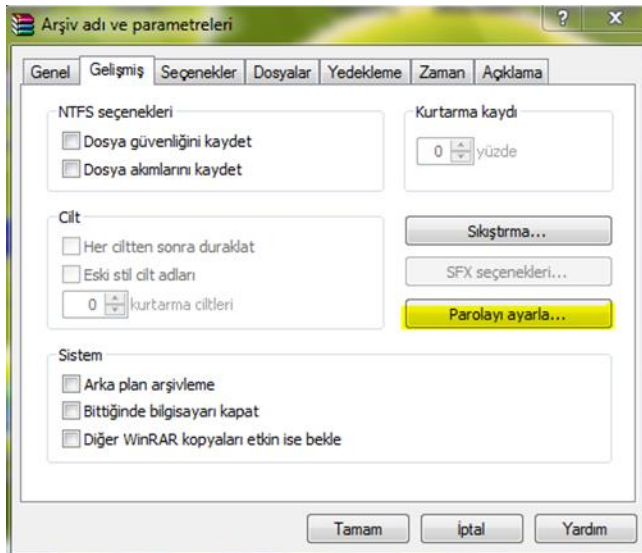
Siber Güvenlik Ekibi: Güvenli yapılandırma gereksinimlerinin uygulanmasını takip eder.

BGYS Ekibi: Konfigürasyon uyumluluğunun denetimini yapar.

5. UYGULAMA

Kriptografi Metodu

- Gizli dereceli bilgiler taşınırken ve aktarılırken Ofis ve Sıkıştırma programlarının şifreleme fonksiyonları kullanılarak şifrelenmelidir. (Örn. Winrar, Winzip, Excel-Word Şifrelemesi). Bu yöntemle şifrelenen bilgi paylaşılırken, şifreleme anahtarı (parola) karşı tarafa ayrı bir kanaldan (Örn. SMS, Telefon Görüşmesi vb.) bildirilmelidir.



- Uygulama yazılımlarındaki kullanıcı ve parola bilgileri LDAP'ta kriptolu şekilde kayıt edilmelidir.

- Kamu kurumları ile yapılan bilgi transferlerinde ilgili kurumlarca sağlanan elektronik imza ve şifreleme yöntemleri kullanılmalıdır.
- Mail haberleşmesi için Outlook vb. uygulamalar yapılandırılırken SSL protokolü kullanılmalıdır.
- Web sayfası, portal vb. geliştirme işlemlerinde https protokolü üzerinden SSL Sertifikaları aracılığı ile şifreli iletişim sağlanmalıdır. Sertifikaların geçerlik süreleri Bilgi İşlem Uzmanı sorumluluğunda takip edilmelidir.
- Kablosuz ağlar WPA2 şifreleme algoritması ile şifrelenmelidir.
- Uzak erişimler sadece ssl sertifikalı vpn sistemleri kullanılmalıdır.
- Taşınabilir bilgisayarların diskleri şifrelenmelidir. Master şifreler kesinlikle aynı cihaz üzerinde barındırılmamalıdır.
- Şifreler açık bir şekilde saklanmamalıdır. Şifre saklamak için PWMan uygulaması kullanılmalı ve Master şifreler aynı cihaz üzerine not alınmamalı ve sadece bilgi varlığının sahipleri tarafından bilinmelidir.
- Taşınabilir medyalar üzerinden veri aktarımı yapılacaksa ilk maddede bahsedilen şifreleme metotları kullanılarak yetkisiz erişime karşı şifrelenmelidir. Şifreler ilgili kişilerle ayrı kanallardan paylaşılmalıdır.
- Alınan harici yedekler şifreli alanlarda saklanmalıdır. Sunucu odamızda ve çelik kasada saklanmaktadır.