	ŞİFRELEME (KRİPTOGRAFİ) POLİTİKASI	Doküman No: PLT-11
		Toplam Rev. Sayısı: --
		Revizyon Tarihi: --
		Yayın No: 01
		Yayın Tarihi: 20.05.2024

Kriptografik kontroller aşağıdaki maksatlarla kullanılır;

- Gizlilik: Saklanan veya iletilen hassas veya kritik bilgiyi korumak için şifrelemenin kullanılması,
- Bütünlük/Güvenilirlik: Saklanan veya iletilen hassas veya kritik bilginin güvenilirlik veya bütünlüğünü korumak için sayısal imzaların veya mesaj doğrulama kodlarının kullanılması,
- İnkâr edilemezlik: Bir olay veya faaliyetin oluşumu veya oluşmadığının kanıtını elde etmek için
- İşletim sistemi üzerinde saklanan kullanıcı ve yönetici hesabı şifreleri kriptolu olarak saklanmaktadır.
- Sunucu, anahtarlama cihazları, yönlendirici cihazlar vb. cihazlara bağlanırken kriptolu bağlantı(SSH,RDP) ile bağlanılmakta, kripto kullanmayan yöntemler tercih edilmemektedir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portlar ile erişim yapılmamaktadır.
- İnternete açılan ya da açılmayan, önem arz eden servislerimiz HTTPS portu üzerinden çalışmaktadır ve veri trafiği şifrelenmektedir.
- Gizlilik arz eden ve önem derecesi yüksek olan verinin taşınabilir ortamlarda kurum dışına çıkarılması durumunda, taşınabilir ortam içeriği Microsoft Bitlocker ürünü ile şifrelenerek yetkisiz kişilerin erişmesine karşı korunur.
- Ayarları üzerinde bulunan cihazların, şifre bilgileri açık metin şeklinde değil kriptolu bir şekilde tutulmaktadır.
- Kurum bünyesinde kullanılan ve gizlilik derecesi yüksek olan dokümanlar, kullanılan programların desteklediği ölçüde şifrelenmektedir.
- Kurum bünyesinde kullanılan şahsa özel elektronik imzalar başıboş şekilde ortalıkta bırakılmaması kurum çalışanlarına farkındalık eğitimiyle anlatılmıştır.
- Elektronik imza cihazları ve şifreleri bir başka personel ile paylaşılmaz.
- Elektronik imza şifrelerini yenilemek amaçlı kullanılan güvenlik sözcükleri başka personellerce bilinmez.
- Kullanılan ortamları kriptolarken kullanılan şifreler basit, tahmin edilebilir ve yalnızca sözlük kelimelerinden oluşturulamaz.
- Her kullanıcı üzerinde çalıştığı ortam için kullandığı kriptolamadan sorumludur.
- Birimi ilgilendiren ortamlar üzerindeki kriptolama yönteminden ise birim amiri sorumludur.
- Dış kurumlara resmi yazılar gönderilirken mümkün olduğu sürece elektronik imza ile imzalanarak KEP üzerinden gönderilir.

Denizli Organize Sanayi Bölgesi Müdürlüğü