LGT LOGISTICS
LIQUID · GRANULE · GAS · TANK

20/03/2023

PAROLA GÜVENLİĞİ POLİTİKASI

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.

2. SORUMLULUK

Bu dokümanın düzenlenmesi ve kontrol edilmesinden Kalite ve Süreç Yönetimi Direktörü ve Bilgi İşlem Sorumlusu sorumludur.

3. TANIMLAR

Parola / Şifre : Kullanıcının, bilgi sistemlerine ve uygulamalarına kullanıcı adı ile birlikte kendisini tanıtmasını ve işlem yaratma ve/veya sonuçlandırmasını sağlayan, sadece kendisinin bildiği ve dilediğinde değiştirebileceği alfa nümerik karakterlerden oluşan tanımdır.

Kullanıcı Hesabı: Bilgi sistemlerinde kişiyi tanımlamak için oluşturulan, sistemde kimlik doğrulaması yapmak ve o sistemin kaynaklarına, verilen yetki doğrultusunda, gerekli erişimi (tanımlı parola ile eşleştirilerek) sağlamak için kullanılan, tüm işlemlerde kişiyi temsil eden alfabetik kod veya alfa nümerik kişiye özel koddur.

4. POLİTİKA DETAYI

- En az 8(sekiz) karakterli olmalıdır.
- İçerisinde en az 1(bir) tane büyük ve en az 1(bir) tane küçük harf bulunmalıdır.
- İçerisinde en az 1(bir) tane rakam bulunmalıdır.
- İçerisinde en az 1(bir) tane özel karakter bulunmalıdır. (@, !,?,A,+,$,#,&,/,{,*,-,],=,...)
- Aynı karakterler peş peşe kullanılmamalıdır. (aaa, 111, XXX, abab...)
- Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,1234,zxcvb...)
- Bir kullanıcı adı ve parolası, birim zamanda birden çok bilgisayarda kullanılmamalıdır.
- Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır. (Örneğin 12345678, qwerty, doğum tarihiniz, çocuğunuzun adı, soyadınız gibi)
- Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır.
- Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır.
- Basit bir kelimenin içerisindeki harf veya rakamları benzerleri ile değiştirilerek güçlü bir parola elde edilebilir.

4.1 Parola Yönetimi ve Kullanımı

- 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.
- Parolaların e-posta iletilerine veya herhangi bir elektronik forma eklenmesi yasaktır.
- Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda BGYS Ekibi tarafından yapılan farkındalık eğitimleri ve farkındalık e-postaları ile düzenli aralıklarla bilgilendirilir.
- Danışmanlık çalışanı olmayan kişiler için açılan geçici kullanıcı hesapları da bu yönergenin ilgili maddelerinde belirtilen parola oluşturma özelliklerine uygun olmak zorundadır.
- Bütün parolalar Danışmanlığa 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.
- Kullanıcının son 3 parolayı tekrar kullanması ve aynı parolayı düzenli kullanması engellenmelidir.

GENEL MÜDÜR