1. GİRİŞ

Yükseltilmiş ayrıcalıklara sahip kullanıcı hesapları bazı bakım ve idari fonksiyonları yerine getirmek için gereklidir. İdari parolalar OSTİM Teknik Üniversitesi bilgi sistemlerine ayrıcalıklı erişim için temel doğrulama araçlardır. Yükseltilmiş ayrıcalıklara sahip kullanıcı hesapları genellikle sisteme sınırsız erişim yetkisine sahiptir, bu nedenle kötü niyetli kişilerin baş hedefleridir. Bunun sonucu olarak idari parolaların kullanımında ek önlemler almak gereklidir.

2. AMAÇ VE KAPSAM

Bu standardın amacı parola politikasının gerekliliklerini detaylandırmak ve yerine getirmektir. Bu standart idari parolalar için teknik ve kurumsal gereklilikleri tanımlar. İdari parolalar sistem bakımı veya sistem desteği için kullanılan hesap parolalarıdır. Bu standardın gereklilikleri parola politikası ve diğer eşlik eden parola standartlarına ilave edilir. Bu standart tüm OSTİM Teknik Üniversitesi çalışanlarını ve bünyesindeki şirketleri, OSTİM Teknik Üniversitesi bilgi sistemlerine idari erişimi olan harici iş ortakları ya da tedarikçiler gibi tüm diğer kişi ve kuruluşları bağlayacaktır. Tüm OSTİM Teknik Üniversitesi bilgi sistemleri bu standardın gereklilikleri ile uyumlu olmalıdır. Bu standardın ve "Parola Politikasının" gereklilikleri "Kurumsal Bilgi Güvenliği Politikasının" gerekliliklerini detaylandırmaktadır. Bu standart "Kurumsal Bilgi Güvenliği Politikası" kapsamında etkili olan kurallar ile uyumlu biçimde yürürlükte olacaktır. Bu standart ve "Parola Politikası" idari parolalar konusunda önceden yürürlükte olan tüm politikaların, standartların ve kuralların yerini alır.

3. GEREKLİLİKLER

3.1 Genel Gereklilikler

3.1.1 Yöneticiler "Parola Politikası", "Parola Sıfırlama ve Saklama Standardı" ve "Parola Uygulama Standardı" tarafından şart koşulan gerekliliklerin yanı sıra bu belgede detaylandırılan standartlara bağlı kalmalıdır.

3.1.2 Yöneticiler idari parolaları almadan önce parola politikasının ve tüm eşlik eden standartların koşullarını kabul etmeli ve aşağıdakileri onaylamalıdır:

- Yönetici hesabı ile bağlanan yetkiler
- İdari parolaları gizli tutacaklarına ve kimseye açıklamayacaklarına dair mutabakat
- Hesabı sorumlu ve etik usulde kullanacaklarına dair mutabakat
- Uygulanabilir mahremiyet kanunları ve yönetmeliklerine uyacaklarına dair mutabakat

- Yönetici hesabını şirket hedeflerini desteklemek amacı ile idari faaliyetleri yerine getirmek için kullanacaklarına dair mutabakat.

3.1.3 Yöneticiler yönetici eşdeğer yetkileri yetkili kişilere vermek için yönetici parolasını açıklamak yerine alternatif yollar bulmalıdır (daha fazla bilgi için yönergelere bakınız).

3.1.4 Yöneticiler 3.1.1'de açıkladığı gibi sorumlu olduklarından yönetici parolalarını kullanırken ek önlemler almalıdırlar (daha fazla bilgi için yönergelere bakınız).

3.1.5 Benzer sistem serileri aynı lokal yönetici parolasını kullanmak üzere ayarlanmamalıdır.

3.1.6 Onaylanmış bir yönetici parolalarının yetkili kişilere ulaştırılması süreci en azından teslim teyidi içermelidir. Bu teyitler saklanmalı ve arşivlenmelidir.

3.1.7 Yönetici parolaları asla sözlük kelimeleri içermemeli ancak hatırlanması kolay olmalıdır (güvenli parola oluşturmayla ilgili daha fazla bilgi için yönergelere bakınız).

3.1.8 Herhangi bir servis kesintisi veya personel kaybı durumunda hızlı biçimde onarım sağlamak üzere acil durum yönetici parolaları mevcut tutulmalıdır. Bir adet geçici acil durum yönetici parolası:

- Mühürlü bir zarfta, güvenli bir yerde tutulmalıdır, örneğin kasa.
- Kullanımdan sonra hemen değiştirilmelidir.

3.1.9 Sistem tarafından bir sınırlama yoksa tüm yönetici parolaları en az on (10) karakter içermelidir.

3.1.10 Parolanın gizliliği ile ilgili bir şüphe oluşursa yönetici parolaları hemen değiştirilmelidir.

3.1.11 Yönetici parolaları karmaşıklık gerekliliklerini sağlamalıdır bu bağlamda bir yönetici parolası büyük harfler, küçük harfler, sayılar ve özel karakterler içermelidir. Eğer sistem tarafından bir kısıtlama yoksa parola yukarıdaki dört (4) kriteri de sağlamalıdır.

3.1.12 Süresi bitmiş yönetici parolaları tekrar kullanılmamalıdır.

3.1.13 Sistemler ve uygulamalar yönetim için kullanılan doğrulama parolalarını, tek yönlü şifreleme algoritmalarıyla şifrelenmiş olarak saklamalıdır.

3.1.14 Kullanıcılara idari erişim vermek yerine mümkünse sistem yordamları veya yardımcı programlar kullanılmalıdır.

3.1.15 Yöneticiler, Borusan Lojistik, kullanıcı veya sistem ile kolayca ilişkilendirilebilecek parolalar seçmemelidir.

3.1.16 Yönetici parolaları devirli olmamalıdır, örneğin parola sonuna ek sayılar ekleyerek değiştirilmemelidir.

3.1.17 Varsayılan (üretici) yönetici parolası sistem kurulumu ardından hemen değiştirilmelidir ve işletimde asla kullanılmamalıdır.

3.1.18 Yönetici parolaları asla toplu işlem dosyaları veya dokümanlar içinde açık olarak yazılmamalıdır.

3.1.19 Yönetici parolaları ancak acil durumlarda yazılabilirler.

3.1.20 Yönetici parolaları giriş esnasında ekranda görülmemelidirler.

3.1.21 Her yönetici sistem tarafından bir kısıtlama olmadığı takdirde kendisine ait hesap ve

4. YÖNERGELER

4.1 Kullanıcı yönetici parolasını girmeden önce yakın çevresinde kimsenin parolayı girerken kendisini izlemediğinden emin olmalıdır.

4.2 Kullanıcılara yönetici eşdeğer yetkilerin verilmesi, bu kişilere yaptıkları iş doğrultusunda erişim hakları verilmesi ile veya işletim sistemlerinin diğer özellikleri kullanılarak yapılır. Kullanıcılara yönetici parolası verilmemelidir.

4.3 Aşağıda güvenli aynı zamanda da hatırlanması kolay bir parola oluşturulması için bir örnek verilmiştir:

Hatırlaması kolay bir cümle seçiniz ve her bir kelimenin baş harfi ile noktalama işaretlerini kullanarak bir parola oluşturunuz. Cümle: "Güvenlik için tam 15 farklı yönetici parolası kullanıyoruz!", cümlesinden

5.REVİZYON GEÇMİŞİ

Revizyon No	Tarih	Açıklama
01	07.11.2024	Entegre Kalite Yönetim Sisteminde kalite yönetiminde zorluklar ile karşılaşılması sebebiyle ISO 9001 Kalite Yönetim Sistemi (KYS) ve ISO 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) ve dokümanlarının ayrılması ve ayrı ayrı takip edilmeleri kabul edilmiştir. Bu sebeple doküman kodlamalarında revizyon yapılmıştır.

Hazırlayan	Kontrol Eden	Onaylayan
İlknur ALŞAHİN Kalite Birimi	Kenan IŞIK Kalite Koordinatörü	Prof.Dr. Murat Ali YÜLEK Rektör
E-imzalıdır/paraflıdır	E-imzalıdır	E-imzalıdır