**-LOGO-**

**-QURUM ADI-**

**ŞİFRƏ SİYASƏTİ**

# SƏNƏDİN TARİXÇƏSİ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Kod** | **Hazırlayan** | **Nəzərdən Keçirən** | **Təsdiqləyən/Təsdiq Tarixi** | **Versiya** | **Dəyişiklik Tarixi** | **Dəyişiklik Səbəbi** | **Məxfilik Səviyyəsi** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

MÜNDƏRİCAT

[SƏNƏDİN TARİXÇƏSİ 2](#_Toc189819817)

[1. ÜMUMİ MÜDDƏALAR 4](#_Toc189819818)

[2. ƏHATƏ DAİRƏSİ 4](#_Toc189819819)

[3. ŞİFRƏ İDARƏETMƏSİ 4](#_Toc189819820)

[4. ŞİFRƏ MÜRƏKKƏBLİYİ VƏ ROTASİYASI 4](#_Toc189819821)

[5. ŞİFRƏ İSTİFADƏSİ ÜÇÜN TƏLƏBLƏR 5](#_Toc189819822)

[6. TƏTBİQLƏRİN İNKİŞAF STANDARTLARI 6](#_Toc189819823)

[7. MƏSULİYYƏT 6](#_Toc189819824)

[7.1 TƏTBİQ İDARƏÇİSİ 6](#_Toc189819825)

[7.2 İNFORMASİYA TEXNOLOGİYALARI ŞÖBƏSİ 6](#_Toc189819826)

[7.3 İSTİFADƏÇİLƏR 6](#_Toc189819827)

[7.4 ZƏİF VƏ ETİBARSIZ ŞİFRƏ SİYASƏTİNƏ NÜMUNƏLƏR 7](#_Toc189819828)

[8. ƏLAQƏLİ SƏNƏDLƏR 7](#_Toc189819829)

[9. İNTİZAM TƏDBİRLƏRİ 7](#_Toc189819830)

[10. SİYASƏTƏ NƏZARƏT 7](#_Toc189819831)

[TƏSDİQETMƏ 9](#_Toc189819832)

# ÜMUMİ MÜDDƏALAR

Şifrə siyasəti (bundan sonra- Siyasət) “Qurum adı”-da (bundan sonra- Qurum) şifrələrin yaradılması, idarə edilməsi və təhlükəsizliyinin təmin edilməsi üçün tələbləri təsvir edir. Şifrələr həssas məlumatların və təşkilati təhlükəsizliyin qorunmasında mühüm müdafiə xəttidir.

Bu siyasətin məqsədi qurumun informasiya təhlükəsizliyini təmin etmək üçün güclü və etibarlı şifrə tələblərini müəyyən etməkdir. Şifrə siyasəti istifadəçilərin hesablarının, sistemlərin və məlumat resurslarının icazəsiz girişlərdən qorunmasını təmin etmək məqsədilə hazırlanmışdır.

# ƏHATƏ DAİRƏSİ

Bu siyasət, qurumun İT resurslarına çıxışı olan işçilər, podratçılar və ziyarətçilər də daxil olmaqla “Qurum”-dakı bütün şəxslərə şamil edilir.

# ŞİFRƏ İDARƏETMƏSİ

Şifrələrin idarə edilməsi qurumun təhlükəsizlik siyasətinə uyğun olaraq standartlara əsaslanmalı və nəzarət mexanizmləri ilə təmin edilməlidir:

* Şifrələr həssas məlumatdır və məxfi hesab edilməlidir;
* Həssas məlumatları idarə edən sistemlər güclü, şifrələrə əsaslanan giriş nəzarətləri ilə qorunmalıdır;
* İT şəbəkə xidmətlərinə daxil olmaq üçün hər bir istifadəçinin unikal giriş məlumatları olmalıdır;
* İstifadəçi girişləri mərkəzləşdirilmiş şəkildə idarə olunmalıdır;
* Giriş cəhdlərini məhdudlaşdırmaq üçün şifrələr lock-out nəzarətləri ilə idarə olunmalıdır;
* Şübhəli şifrə pozuntuları dərhal bildirilməlidir;
* Şifrənin təxmin edilməsi aşkar edilərsə, hesablar kilidlənməlidir;
* Şifrələrin paylaşılması qəti qadağandır;
* İT dəstəyi ilə məsləhətləşdikdən sonra təsdiq edilmiş şifrə menecerlərindən istifadə edilməlidir.

# ŞİFRƏ MÜRƏKKƏBLİYİ VƏ ROTASİYASI

* Şifrələr ən azı 12 simvoldan ibarət, güclü və məxfi olmalıdır;
* Şifrələr hərflər və qeyri-hərf simvollarının (rəqəmlər, durğu işarələri və ya xüsusi simvollar) qarışığından və ya ən azı iki növ qeyri-hərf simvolundan ibarət olmalıdır;
* Bəzi imtiyazlı identifikatorlar müddəti bitməyən şifrələrə malik ola bilər və bu şifrələr ən azı 15 simvoldan ibarət olmalıdır;
* Daimi istifadəçilər hər 90 gündən bir şifrələrini dəyişdirməlidir və şifrələr ən azı bir il ərzində təkrar istifadə edilməməlidir;
* Sistem səviyyəsində şifrələr hər rüb dəyişdirilməlidir;
* İstifadəçilər ilk dəfə daxil olduqda şifrələrini dəyişdirməlidirlər;
* İstifadəçi ID-ləri şifrənin bir hissəsi olmamalıdır;
* Paylaşılan istifadəçi ID-ləri üçün minimum şifrə müddəti bir gün və ya bir gündən az ola bilər;
* Bütün digər istifadəçi ID-ləri platformanın icazə verdiyi minimum intervalda, lakin bir gündən az olmamaqla müəyyən edilmiş minimum şifrə müddətinə malik olacaq;
* Ardıcıl 5 uğursuz giriş cəhdindən sonra girişlər deaktiv edilməli və ya gecikdirilməlidir;
* Ardıcıl uğursuz giriş cəhdlərindən sonra bloklama müddəti daimi olmalıdır. Şifrəni yalnız İT dəstək komandası sıfırlaya bilməlidir.

# ŞİFRƏ İSTİFADƏSİ ÜÇÜN TƏLƏBLƏR

* Administrativ giriş məlumatları qeyri-administrativ tapşırıqlar üçün istifadə edilməməlidir. İnzibatçılar adi və administrativ vəzifələri üçün fərqli giriş məlumatlarına sahib olmalıdırlar;
* Mümkün olduqda rəqəmsal sertifikatlar və çoxfaktorlu identifikasiyadan istifadə edilməlidir;
* Şifrələrin elektron ünsiyyətə daxil edilməsi qadağandır;
* "Şifrəni yadda saxla" funksiyasından istifadə edilməməlidir; əvəzinə şifrələr manual olaraq yenilənməlidir;
* Şifrələr təhlükəsiz yerlərdə saxlanmalıdır;
* Sistem səviyyəli girişə malik hesablar üçün ayrı şifrələr istifadə edilməlidir;
* Şifrələr yazılı formada və ya iş masalarında saxlanmamalıdır;
* Fərdi istifadəçilərin ID şifrələri ya istifadə müddəti bitmiş vəziyyətə gətirilməli, ya da istifadəçi növbəti giriş zamanı şifrəni dəyişməlidir. Bu, funksional və ya sistem ID-lərinə şamil edilmir;
* Əməliyyat sistemləri və ya proqram məhsulları ilə birlikdə gələn standart şifrələr quraşdırma/tənzimləmə prosesindən dərhal sonra dəyişdirilməlidir;
* "Şifrə ifadələri" və ya "smart kartlar" ənənəvi şifrələrə məqbul alternativlərdir;
* Şifrə dəyişiklikləri tələb olunan hallarda tətbiq edilməlidir, məsələn, təhlükəsizlik pozuntusundan sonra və ya vəzifə dəyişikliyi zamanı;
* Təhlükəsizliyi olmayan istifadəçi adlarından, tez-tez istifadə olunan şifrələrdən və təhlükəsizliyi pozulmuş sistemlərdən əldə edilmiş şifrə kombinasiyalarından istifadə edilməməlidir;
* Şifrələr ekranda daxil edildikdə görünməməlidir;
* Şifrələnmə və heş funksiyası, şifrələr üçün təsdiq edilmiş kriptoqrafik üsullara uyğun olaraq həyata keçirilməlidir;

# TƏTBİQLƏRİN İNKİŞAF STANDARTLARI

Proqram tərtibatçıları tərəfindən aşağıda qeyd olunan müddəalar həyata keçirilməlidir:

* Tətbiqlərə giriş qruplar tərəfindən deyil, fərdi istifadəçilər tərəfindən həyata keçirilməlidir;
* Şifrələr açıq mətn formatında və ya asanlıqla geri çevrilə bilən hər hansı digər formatda saxlanılmamalıdır;
* Tətbiqlər rol idarəetməsini təmin etməlidir ki, bir şəxs digərinin şifrəsini bilmədən onun funksiyalarını icra edə bilsin;
* Şifrələr təhlükəsiz formatda saxlanmalı və göndərilməlidir.

# MƏSULİYYƏT

## TƏTBİQ İDARƏÇİSİ

* Rəhbərlik adından İT sistemləri üçün şifrə idarəetmə proseduruna nəzarət edilməlidir;
* Şifrə yaradılması, təhlükəsiz saxlanması və idarə olunması üçün siyasət qaydalarını hazırlamalı və idarə etməlidir.

## İNFORMASİYA TEXNOLOGİYALARI ŞÖBƏSİ

* Bu siyasətdə təsvir edilən sistemə giriş və şifrə tələbləri istifadəçilərə çatdırılmalıdır;
* Giriş ləğv ediləcəyi halda və ya şifrə sındırılıbsa, bu barədə dərhal İnformasiya Təhlükəsizliyi komandasına məlumat verilməlidir;
* Siyasətə uyğun olaraq, nəzarətdə olan sistemlər və tətbiqlər üçün şifrələr təyin edilməli və idarə edilməlidir;
* Şifrələr böyük hərflər, rəqəmlər və xüsusi simvolları ehtiva edəcək qədər güclü olmalıdır və bu tələbin tətbiqi İT menecerinin məsuliyyətindədir.

## İSTİFADƏÇİLƏR

* İstifadəçilər şifrə təhlükəsizliyi ilə bağlı vəzifələrindən xəbərdar olmalıdırlar;
* İnformasiya resurslarını tənzimləyən qanunlara və siyasətlərə əməl etmədikləri təqdirdə qarşılaşacaqları nəticələri dərk etməlidirlər;
* Şifrənin sındırıldığından şübhələndikdə, dərhal şöbə rəhbəri məlumatlandırılmalıdır.

## ZƏİF VƏ ETİBARSIZ ŞİFRƏ SİYASƏTİNƏ NÜMUNƏLƏR

Aşağıdakı müddəalar zəif və etibarsız şifrələrin xarakteristikalarıdır:

* Şifrə 8-dən az simvoldan ibarətdirsə;
* Şifrə yerli və ya xarici dildəki lüğət sözlərindən ibarətdirsə;
* Şifrəyə "123456" və ya "abcdef" kimi ardıcıl simvollar, "parol" və ya "şifrə" kimi ümumi ifadələr və "a" və ya "111111" kimi təkrarlanan simvollar daxildirsə;
* Şifrədə "qwertyuiop" (klaviaturanın yuxarı cərgəsi) və ya "asdfghjkl" kimi klaviatura nümunələri istifadə olunubsa;
* Sadə sözlərlə rəqəmlərin birləşdirilməsi, məsələn, “password1” və ya “football111” , eyni zamanda “Facebook” və ya “google123” kimi tanınmış şirkət və ya proqram adlarının istifadəsi;
* “a” hərfi “@” ilə və “o” hərfi “0” ilə əvəz olunduqda, məsələn, 'p@ssw0rd' kimi sadə dəyişdirmələr belə asanlıqla deşifrə edilə bilər.

# ƏLAQƏLİ SƏNƏDLƏR

* ISO 27001:2022 Annex- 5.17

# İNTİZAM TƏDBİRLƏRİ

Siyasət təsdiq olunduğu gündən qüvvədədir. Siyasətdə qeyd olunan müddəaların pozulması halında Daxili Nizam İntizam Proseduru tətbiq olunacaq.

# SİYASƏTƏ NƏZARƏT

Siyasətə nəzarət hər il İT komitəsi tərəfindən həyata keçirilməlidir. Eyni zamanda, aşağıdakı hallarda da siyasət nəzərdən keçirilməlidir:

1. Qurumun strukturunda, iş proseslərində və ya informasiya resurslarında əhəmiyyətli dəyişikliklər baş verdikdə;
2. İnformasiya təhlükəsizliyi ilə bağlı rəhbərlik tərəfindən müəyyən edilən hədəflər və prioritetlər dəyişdikdə;
3. Qurumun fəaliyyət şəraiti, o cümlədən qanunvericilik və ya tənzimləyici tələblərdə dəyişikliklər olduqda;
4. İnformasiya təhlükəsizliyinin idarə olunması sahəsində yeni yanaşmalar tətbiq edildikdə.

# TƏSDİQETMƏ

Bu sənədi imzalamaqla, təqdim olunan məlumatların həqiqiliyini və düzgünlüyünü qəbul edirsiniz.

[vəzifə məlumatları]

[adı soyadı və ata adı]

\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_

[İmza] [Tarix]