**-LOGO-**

**-QURUM ADI-**

**ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN İDARƏEDİLMƏSİ SİYASƏTİ**

# SƏNƏDİN TARİXÇƏSİ

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

MÜNDƏRİCAT

[SƏNƏDİN TARİXÇƏSİ 2](#_Toc183099157)

[1. ÜMUMİ MÜDDƏALAR 4](#_Toc183099158)

[2. MƏQSƏD 4](#_Toc183099159)

[3. ANLAYIŞLAR 4](#_Toc183099160)

[4. ƏHATƏ DAİRƏSİ 4](#_Toc183099161)

[5. SİYASƏT 5](#_Toc183099162)

[5.1. ŞƏBƏKƏ SEQMENTASİYASI 5](#_Toc183099163)

[5.2. ŞƏBƏKƏ İSTİFADƏÇİLƏRİNİN, MƏLUMATLARIN VƏ CİHAZLARIN MƏXFİLİYİ 5](#_Toc183099164)

[5.3. ŞƏBƏKƏ İSTİFADƏÇİLƏRİNİN, MƏLUMATLARIN VƏ CİHAZLARIN BÜTÖVLÜYÜ 6](#_Toc183099165)

[5.4. ŞƏBƏKƏ XİDMƏTLƏRİNİN VƏ MƏLUMATLARININ ƏLÇATANLIĞI 7](#_Toc183099166)

[6. ƏLAQƏLİ SƏNƏDLƏR 7](#_Toc183099167)

[7. İNTİZAM TƏDBİRLƏRİ 8](#_Toc183099168)

[8. SİYASƏTƏ NƏZARƏT 8](#_Toc183099169)

[TƏSDİQETMƏ 8](#_Toc183099170)

# ÜMUMİ MÜDDƏALAR

Şəbəkə Təhlükəsizliyinin İdarəedilməsi Siyasəti (bundan sonra - Siyasət) “Qurum adı”-nın (bundan sonra - Qurum) şəbəkə mühitində məlumatların təhlükəsizliyini qorumaq üçün əsas tələbləri və əməkdaşların vəzifələrini müəyyən edən, eləcə də təhlükəsizlik üzrə nəzarət mexanizmlərini və əsas prinsipləri ehtiva edən əsas sənəddir. Bu siyasət həmçinin şəbəkə təhlükəsizliyinin təmin olunması məqsədilə həyata keçiriləcək təşkilati və texniki tədbirləri müəyyən edir.

Siyasət, informasiya təhlükəsizliyinə dair qabaqcıl beynəlxalq standartlara, o cümlədən ISO/IEC 27001 standartına əsaslanaraq hazırlanmışdır.

# MƏQSƏD

Bu siyasətin əsas məqsədi qurum daxilində məlumatların ötürülməsi zamanı məxfilik, bütövlük və əlçatanlıq prinsiplərinə əməl olunmasını təmin etmək məqsədilə şəbəkə resurslarının qorunması və təhlükəsizliyinin təmin edilməsidir.

# ANLAYIŞLAR

**Şəbəkə Xidmətləri:** Şəbəkə xidmətləri, qurumun (filiallar, şöbələr, işçilər və üçüncü tərəflər) şəbəkə infrastrukturu üzərindən məlumat mübadiləsi, təhlükəsizlik və resursların idarə olunmasını təmin edən xidmətlərdir.

**Şəbəkə:**  Qurumun şəbəkəsi aşağıdakılardan ibarətdir:

1. Yerli Şəbəkə (LAN): Qurumun bir filialı, şöbəsi və ya müəyyən bir binası daxilində cihazlar arasında məlumat mübadiləsini təmin edən sürətli və təhlükəsiz şəbəkədir;
2. Geniş Sahə Şəbəkəsi (WAN): Qurumun müxtəlif coğrafi ərazilərdə yerləşən filialları və şöbələri arasında məlumat mübadiləsini təmin edən geniş miqyaslı şəbəkədir;
3. Şəbəkə emal vasitələri: Qurumun bölmələri , filialları, işçiləri və üçüncü tərəf təşkilatları arasında məlumatların şəbəkə üzərindən düzgün şəkildə ötürülməsi, yönləndirilməsi və idarə olunmasını təmin edən komponentlərdir .

# ƏHATƏ DAİRƏSİ

Bu siyasət, qurum əməkdaşları, podratçıları, auditorları və qurumun informasiya sistemlərinə daxil olmaq üçün icazə verilmiş digər istifadəçiləri əhatə edir. Eyni zamanda, siyasət şəbəkə cihazlarının və onların idarə edilməsinin təhlükəsizliyinə dair tələbləri müəyyən edir.

# SİYASƏT

## ŞƏBƏKƏ SEQMENTASİYASI

Qurum şəbəkə inzibatçılarının informasiya aktivlərinə girişin idarə olunması üzrə məsuliyyətlərini dəqiq şəkildə müəyyənləşdirməlidir. Şəbəkə inzibatçılarının funksiyaları sistem inzibatçılarının vəzifələrindən tamamilə fərqləndirilməli və ayrılmalıdır.

1. Qurumun şəbəkə seqmentasiyası, şəbəkə resurslarına olan icazəsiz girişləri məhdudlaşdırmaq və müxtəlif təhlükəsizlik təhdidlərinə qarşı qorunma təmin etmək məqsədilə düzgün şəkildə tərtib edilməlidir.
2. Hər bir şəbəkə bölgəsinin sərhədləri (şəbəkə perimetri) dəqiq müəyyən edilməli və şəbəkə bölgələri arasında məlumat mübadiləsi yalnız icazə verilən marşrutlar və şluzlar (məsələn, firewall və marşrutlaşdırıcı filtrləri) vasitəsilə həyata keçirilməlidir.
3. Seqmentasiyası həyata keçirilmiş şəbəkə strukturu, şəbəkə daxilindəki məlumat axınını nəzarət altına almağa və təhlükəsizlik məsələlərini idarə etməyə imkan verən sistemlərlə dəstəklənməlidir.
4. Şəbəkə seqmentasiyası prosesində, hər bir şəbəkə bölməsi üçün fərqli təhlükəsizlik protokolları və müdafiə mexanizmləri tətbiq edilməli, daxili və xarici əlaqələr arasındakı təhlükəsizlik hədləri aydın şəkildə tərtib olunmalıdır.

## ŞƏBƏKƏ İSTİFADƏÇİLƏRİNİN, MƏLUMATLARIN VƏ CİHAZLARIN MƏXFİLİYİ

Şəbəkə xidmətləri, emal vasitələri və məlumatları yalnız icazə verilmiş istifadəçilər və tərəflər tərəfindən əldə edilə bilən şəkildə qorunmalı, icazəsiz girişi qarşısını almaq üçün uyğun təhlükəsizlik tədbirləri görülməlidir.

1. Məlumatların ötürülməsi və saxlanması zamanı məxfi məlumatlar, yalnız etibarlı və şifrələnmiş kanallar üzərindən göndərilməli və saxlanmalıdır;
2. Üçüncü tərəf xidmətləri və şəbəkələri vasitəsilə məlumat mübadiləsi yalnız təhlükəsiz şifrələmə metodları ilə həyata keçirilməli və məlumatların müdaxilə edilmədən ötürülməsi təmin edilməlidir;
3. Şəbəkə istifadəçilərinin resurslara, xidmətlərə və ya emal vasitələrinə girişi “Girişlərə Nəzarət Siyasəti” əsasında müəyyən edilmiş “Bilmək Lazımdır” (Need to know) prinsipi ilə müəyyən edilməli, yalnız müvafiq iş fəaliyyəti üçün zəruri məlumatlara icazə verilməlidir;
4. Şəbəkədə istifadə olunan bütün cihazlar və emal vasitələri müvafiq təhlükəsizlik standartlarına uyğun şifrələnməli və məlumatların təhlükəsizliyini təmin etmək məqsədilə qorunmalıdır;
5. Şəbəkə üzərindən mübadilə edilən məlumatların məxfiliyi və bütövlüyü qorunmalı, məlumatın dəyişdirilməsi, silinməsi və ya icazəsiz əldə edilməsi qarşısı alınmalıdır;
6. Şəbəkə xidmətləri və emal vasitələri qurumun “Məlumatların Təsnifləşdirilməsi Proseduru” əsasında müvafiq sənədləşmə ilə təsnif edilməlidir;
7. Şəbəkə resursları və cihazları üzərində hər hansı dəyişikliklər, etibarlı təsdiqləmə və yoxlama proseslərindən keçməli və yalnız səlahiyyətli şəxslər tərəfindən həyata keçirilməlidir;
8. Şəbəkə istifadəsi və məlumat mübadiləsi ilə bağlı bütün prosedurlar, istifadəçi məlumatlarının və təşkilati məlumatların qorunmasını təmin etmək məqsədilə müvafiq sənədləşmə və siyasət qaydalarına uyğun olmalıdır;
9. Şəbəkənin təhlükəsizlik tədbirləri, məlumatların sızması, icazəsiz əldə edilməsi və digər təhlükəsizlik təhdidlərinə qarşı davamlı olaraq yenilənməli və inkişaf etdirilməlidir.

## ŞƏBƏKƏ İSTİFADƏÇİLƏRİNİN, MƏLUMATLARIN VƏ CİHAZLARIN BÜTÖVLÜYÜ

Qurumun şəbəkə vasitələri ilə ötürülən, saxlanılan və ya emal edilən istifadəçi məlumatlarının, şəbəkə avadanlıqlarının və resurslarının həqiqiliyini, etibarlılığını və qanuniliyini təmin etmək üçün şəbəkənin bütövlüyü mütəmadi olaraq yoxlanılmalıdır.

1. Bütün şəbəkə istifadəçiləri və cihazları şəbəkəyə (LAN, WLAN, WAN) qoşulmadan əvvəl autentifikasiya prosesindən keçməli, yalnız müvafiq icazəyə malik olan şəxslər və cihazlar şəbəkəyə daxil ola bilər;
2. İstifadəçilərin və cihazlarının autentifikasiyası şəbəkə sistemlərinə inteqrasiya olunmadan əvvəl həyata keçirilməli və hər bir girişi qeydiyyata alınmalıdır;
3. Şəbəkəyə qoşulmadan əvvəl bütün istifadəçilərin autentifikasiyası biometrik sistemlər, şifrələr və ya digər etibarlı giriş metodları və s. ilə həyata keçirilməlidir;
4. Qurumun şəbəkə avadanlıqlarına daxil olmamışdan əvvəl bütün cihazlar yoxlanmalı və uyğun təhlükəsizlik tədbirləri ilə təsdiqlənməlidir;
5. Şəbəkə daxilindəki bütün əməliyyatlar monitorinq edilməli, şəbəkə istifadəçiləri və avadanlıqları ilə bağlı məlumatlar mütəmadi olaraq toplanmalı və təhlil edilməlidir;
6. Şəbəkə məlumatlarının və aktivlərinin sahibləri müəyyən edilməli və "Məlumatların Təsnifləşdirilməsi Siyasəti"nə uyğun olaraq sənədləşdirilməlidir;
7. Şəbəkə resursları və məlumatlarına daxil olmaq üçün rollar, məsuliyyətlər aydın şəkildə təyin edilməli, sənədləşdirilməli və mütəmadi olaraq monitorinq edilməlidir;
8. Kritik şəbəkə hadisələri daimi olaraq qeyd edilməli və təhlil edilməli, şəbəkə təhlükəsizliyi təmin etmək məqsədilə müvafiq tədbirlər görülməlidir;
9. Şəbəkə xidmətləri və cihazlarından əldə edilən məlumatların saxlanma müddətləri əvvəlcədən müəyyənləşdirilməli və bu müddətə uyğun olaraq qorunmalıdır;
10. Şəbəkə məlumatlarının və cihazlarının təhlükəsizliyi təmin edilməsi üçün girişlər məhdudlaşdırılmalı, məlumatların şifrələnməsi və digər mühafizə metodları tətbiq edilməlidir.
11. Şəbəkə avadanlıqları arasında vaxt sinxronizasiyası təmin edilməli, bu sinxronizasiyanın düzgünlüyü müntəzəm olaraq yoxlanılmalıdır.

## ŞƏBƏKƏ XİDMƏTLƏRİNİN VƏ MƏLUMATLARININ ƏLÇATANLIĞI

Qurumun fəaliyyətinə və mühüm xidmətlərin icrasına uyğun olaraq, şəbəkə xidmətlərinin və emal vasitələrinin əlçatanlığı qəbul edilə bilən məhdudiyyətlər daxilində daim təmin edilməlidir.

1. Şəbəkə xidmətləri və cihazlarının fasiləsiz işləməsi üçün əsas resursların monitorinqi aparılmalı və kritik əməliyyatlar üçün avtomatik xəbərdarlıq sistemləri qurulmalıdır;
2. Şəbəkə kanallarının və xidmətlərin əlçatanlığı, eləcə də cihazların funksionallığı qurumun risk qəbul səviyyəsinə və ya SLA sənədində müəyyən edilmiş dözümlülük və mümkün dayanma müddətləri çərçivəsində təmin edilməlidir;
3. Əsas şəbəkə avadanlıqları və xidmətləri ehtiyat kanallar vasitəsilə replikasiya edilməli, bu proses qurumun RTO (Recovery Time Objective) və RPO (Recovery Point Objective) göstəricilərinə uyğun dizayn edilməlidir;
4. Kritik şəbəkə əməliyyatlarını və inzibati funksiyaları dəstəkləmək üçün ehtiyat işçi heyəti təyin olunmalı və bu heyətin tərkibi RTO məqsədlərinə uyğun şəkildə müəyyən edilməlidir;
5. Şəbəkə əməliyyatlarının kəsilməməsi üçün davamlılıq planları yaradılmalı və fövqəladə hallara cavab verə biləcək prosedurlar tətbiq edilməlidir;
6. Şəbəkə konfiqurasiyalarının və sistem parametrlərinin ehtiyat nüsxələri müəyyən olunmuş intervallarla çıxarılmalı və təhlükəsiz mühitdə saxlanılmalıdır;
7. Bütün kritik şəbəkə məlumatlarının ehtiyat nüsxələri mütəmadi olaraq çıxarılmalı, test edilməli və təhlükəsiz saxlanılmalıdır;
8. Kritik məlumat və xidmətlər üçün tələb olunan əlçatanlıq səviyyələri əvvəlcədən müəyyən edilməli, bu səviyyələrin qorunması üçün texniki və inzibati tədbirlər görülməlidir;
9. Əlçatanlıq siyasətinə uyğun olaraq bütün istifadəçilərin tələb olunan xidmətlərə vaxtında girişinin təmin olunması üçün müvafiq infrastruktur inkişaf etdirilməlidir.

# ƏLAQƏLİ SƏNƏDLƏR

* İnformasiya Təhlükəsizliyi Siyasəti
* ISO 27001:2022 Annex- 8.20, 8.21, 8.22
* Məlumatların Təsnifləşdirilməsi Siyasəti
* Girişlərə Nəzarət Siyasəti
* Məlumatların Təsnifləşdirilməsi Proseduru

# 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]