**-LOGO-**

**-QURUM ADI-**

**İNFORMASİYA TƏHLÜKƏSİZLİYİ SİYASƏTİ**

# SƏNƏDİN TARİXÇƏSİ

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

**MÜNDƏRİCAT**

[SƏNƏDİN TARİXÇƏSİ 2](#_Toc183788189)

[1. ÜMUMİ MÜDDƏALAR 5](#_Toc183788190)

[2. MƏQSƏD 5](#_Toc183788191)

[3. ANLAYIŞLAR 5](#_Toc183788192)

[4. ƏHATƏ DAİRƏSİ 6](#_Toc183788193)

[5. İNFORMASİYA TƏHLÜKƏSİZLİYİ KOMİTƏSİ 6](#_Toc183788194)

[6. RİSKLƏRİN İDARƏOLUNMASI KOMİTƏSİ 7](#_Toc183788195)

[7. MƏSULİYYƏTLƏR 9](#_Toc183788196)

[8. TƏTBİQ 10](#_Toc183788197)

[9. İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏŞKİLİ 11](#_Toc183788198)

[9.1 Daxili Nizamlama 11](#_Toc183788199)

[10. İNSAN RESURSLARININ TƏHLÜKƏSİZLİYİ 11](#_Toc183788200)

[10.1 İşə Başlamadan Əvvəl 11](#_Toc183788201)

[10.2 İş Müddətində 11](#_Toc183788202)

[10.3 İşə Xitam Verilməsi Və Dəyişdirilməsi 12](#_Toc183788203)

[11. AKTİVLƏRİN İDARƏOLUNMASI 12](#_Toc183788204)

[11.1 Aktivlərə Görə Məsuliyyət 12](#_Toc183788205)

[11.2 İnformasiyanın Təsnifatı 12](#_Toc183788206)

[11.3 İnformasiya Daşıyıcıları İlə İşləmə 12](#_Toc183788207)

[12. GİRİŞ NƏZARƏTİ 13](#_Toc183788208)

[12.1 Giriş Nəzarətində Biznes Tələbləri 13](#_Toc183788209)

[12.2 İstifadəçi Girişinin İdarə Edilməsi 13](#_Toc183788210)

[12.3 İstifadəçinin Məsuliyyətləri 13](#_Toc183788211)

[12.4 Sistem Və Proqram Girişinə Nəzarət 14](#_Toc183788212)

[13. KRİPTOQRAFİYA 14](#_Toc183788213)

[13.1 Kriptoqrafik Nəzarət 14](#_Toc183788214)

[14. FİZİKİ VƏ ƏTRAF MÜHİT TƏHLÜKƏSİZLİYİ 15](#_Toc183788215)

[14.1 Təhlükəsiz Ərazilər 15](#_Toc183788216)

[14.2 Avadanlıq Və Cihazlar 15](#_Toc183788217)

[15. ƏMƏLİYYAT TƏHLÜKƏSİZLİYİ 16](#_Toc183788218)

[15.1 Əməliyyat Prosedurları Və Məsuliyyətlər 16](#_Toc183788219)

[15.2 Zərərli Proqramlardan Qorunma 16](#_Toc183788220)

[15.3 Ehtiyat Nüsxələrinin Yaradılması Və Bərpası 17](#_Toc183788221)

[15.4 Loqlaşdırma Və Monitorinq 18](#_Toc183788222)

[15.5 Proqram Təminatına Nəzarət 18](#_Toc183788223)

[15.6 Texniki Zəifliyin İdarə Edilməsi 19](#_Toc183788224)

[15.7 İnformasiya Sistemlərinin Audit Tələbləri 19](#_Toc183788225)

[16. KOMMUNİKASİYA TƏHLÜKƏSİZLİYİ 19](#_Toc183788226)

[16.1 Şəbəkə Təhlükəsizliyinin İdarəolunması 19](#_Toc183788227)

[17. SİSTEMİN ƏLDƏ EDİLMƏSİ, İNKİŞAFI VƏ SAXLANMASI 20](#_Toc183788228)

[17.1 İnformasiya Sistemlərinin Təhlükəsizlik Tələbləri 20](#_Toc183788229)

[17.2 İnkişaf Və Dəstək Proseslərində Təhlükəsizlik 20](#_Toc183788230)

[17.3 Test Məlumatları 21](#_Toc183788231)

[18. XARİCİ TƏRƏFLƏRLƏ ƏLAQƏLƏR 21](#_Toc183788232)

[18.1 Xarici Tərəflərlə Əlaqədə İnformasiya Təhlükəsizliyi 21](#_Toc183788233)

[18.2 Xarici Tərəf Xidmətlərinin İdarə Edilməsi 22](#_Toc183788234)

[19. İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİNİN İDARƏ EDİLMƏSİ 22](#_Toc183788235)

[19.1 İnformasiya Təhlükəsizliyi İnsidentlərinin İdarə Edilməsi Və Təkmilləşdirilməsi 22](#_Toc183788236)

[20. FƏALİYYƏT DAVAMLILIĞININ İDARƏ EDİLMƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ 23](#_Toc183788237)

[20.1 İnformasiya Təhlükəsizliyinin Davamlılığının Təmin Edilməsi 23](#_Toc183788238)

[21. UYĞUNLUQ 23](#_Toc183788239)

[21.1 Qanun Və Müqavilə Tələblərinə Uyğunluq 23](#_Toc183788240)

[21.2 İnformasiya Təhlükəsizliyi Rəyləri 24](#_Toc183788241)

[22. SİYASƏTƏ NƏZARƏT 24](#_Toc183788242)

[23. İNTİZAM TƏDBİRLƏRİ 24](#_Toc183788243)

[24. ƏLAQƏLİ SƏNƏDLƏR 25](#_Toc183788244)

[TƏSDİQETMƏ 25](#_Toc183788245)

# ÜMUMİ MÜDDƏALAR

İnformasiya Təhlükəsizliyi Siyasəti (bundan sonra – Siyasət) “Qurum adı”-nın (bundan sonra – Qurum) informasiya təhlükəsizliyinin qorunması ilə bağlı ümumi qaydaları, təşkilati vahidlərin və əməkdaşların əsas öhdəliklərini və bu sahədə həyata keçiriləcək nəzarət tədbirlərini müəyyən edir. Bu Siyasət, həmçinin informasiya təhlükəsizliyi ilə bağlı təşkilati və texnoloji yanaşmaları sistemli şəkildə tənzimləyən təməl sənəd funksiyasın ı daşıyır.

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

# MƏQSƏD

Bu siyasətin məqsədi, informasiya təhlükəsizliyinin idarə edilməsi ilə bağlı qurumda effektiv yanaşmaların tətbiqini, risklərin idarə olunmasını və müvafiq sənədləşdirmə tələblərinin təmin edilməsidir.

# ANLAYIŞLAR

Bu sənəddə istifadə olunan anlayışlar aşağıdakı mənaları daşıyır:

**İnformasiya** – müxtəlif formatlarda (mətn, rəqəmsal, səs, görüntü və s.) mövcud ola bilən və ötürülməsi, emalı, saxlanması, eləcə də istifadə edilməsi mümkün olan strukturlaşdırılmış və ya strukturlaşdırılmamış məlumatlar toplusu;

**Sənədləşdirilmiş informasiya** – müəyyən edilmiş qaydalar və prosedurlar əsasında yazılı və ya rəqəmsal formatda təsbit edilən və saxlanılan məlumatlar. Sənədləşdirilmiş informasiya qurumun fəaliyyətini sübut edən və ya dəstəkləyən resurs kimi xidmət edir;

**Məxfi informasiya** – hüquqi və təşkilati tələblərə əsasən yalnız məhdud şəxslər qrupuna açıqlanması nəzərdə tutulan və xüsusi mühafizə tədbirləri tələb edən informasiya növü, habelə peşə, kommersiya, istintaq və məhkəmə sirləri;

**İnformasiya Texnologiyaları (İT)** – informasiyanın yaradılması, saxlanması, emalı və ötürülməsi üçün istifadə olunan sistemlərin, texnologiyaların və proseslərin məcmusu;

**İnformasiya resursları** – informasiyanın emalı və saxlanması üçün istifadə edilən fiziki və ya rəqəmsal aktivlər, o cümlədən məlumat bazaları, serverlər, proqram təminatı və şəbəkələr;

**Təhlükə** - informasiya və sistemlərin məxfiliyini, bütövlüyünü və əlçatanlığını pozaraq quruma və ya fərdlərə zərər yetirə biləcək potensial hadisə və ya vəziyyət;

**Boşluq** – informasiya təhlükəsizliyində mövcud olan zəifliklər və ya riskləri artıran mühafizə tədbirlərinin natamamlığı;

**Risk** – informasiya sistemlərinə, məlumatlarına və biznes proseslərinə təhlükələrin təsir etmə ehtimalı və bunun nəticəsində yaranacaq itkilərin miqyası;

**İnformasiyanın təsnifatı** – informasiyanın həssaslıq səviyyəsinə, əhəmiyyətinə və qorunma tələblərinə uyğun olaraq kateqoriyalara ayrılması və bu kateqoriyalar əsasında təhlükəsizlik tədbirlərinin tətbiqi (identifikasiyası, prioritetləşdirilməsi və nişanlanması);

**İnsident** – informasiya təhlükəsizliyi siyasətinin, standartlarının və prosedurlarının pozulmasına səbəb olan və ya potensial olaraq belə nəticələrə gətirə biləcək hadisə;

**Ehtiyat bərpa mərkəzi** – fövqəladə hallar zamanı qurumun kritik informasiya texnologiyaları xidmətlərinin və məlumatlarının davamlılığını təmin etmək məqsədilə yaradılmış alternativ mərkəz;

**Server** – şəbəkə üzərindən digər cihazlara xidmət göstərmək, məlumatları emal etmək və saxlamaq üçün nəzərdə tutulmuş yüksək performanslı kompüter sistemi;

**Sistem inzibatçısı** – qurumun informasiya sistemlərinin funksional və təhlükəsiz işləməsini təmin edən və onların idarə edilməsinə cavabdeh olan mütəxəssis;

**İTİS** - İnformasiya Təhlükəsizliyi İdarəetmə Sistemi.

# ƏHATƏ DAİRƏSİ

Bu siyasət, qurumun informasiya təhlükəsizliyinin təmin edilməsi üçün struktur bölmələrini, əməkdaşlarını, podratçılarını və üçüncü tərəfləri əhatə edir. Qurumun mülkiyyətində və ya nəzarətində olan bütün informasiya aktivləri, o cümlədən məlumat bazaları, sistemlər, şəbəkələr, avadanlıqlar və sənədlər siyasətin tələblərinə tabedir. Həmçinin, siyasət qurumun fəaliyyət göstərdiyi bütün fiziki məkanları, ofisləri, uzaqdan iş yerlərini və filiallarını əhatə edir. Qurum resurslarından istifadə edən bütün şəxslər, o cümlədən daimi və müvəqqəti işçilər, podratçılar bu siyasətə uyğun fəaliyyət göstərməlidir. Siyasət yerli və beynəlxalq qanunvericiliyə, tənzimləyici tələblərə və müqavilə öhdəliklərinə uyğun şəkildə həyata keçirilir və bütün təsnifləşdirilmiş məlumatları əhatə edir. Bundan əlavə, qurum tərəfindən istifadə olunan texnologiyalar, proqram təminatları, tətbiqlər və şəbəkə qurğuları bu siyasətin tələblərinə uyğun idarə olunur. Qurum daxilində və onun resurslarından istifadə zamanı həyata keçirilən bütün fəaliyyətlər, o cümlədən məlumatların emalı, saxlanması və ötürülməsi prosesləri bu siyasətə daxildir.

# İNFORMASİYA TƏHLÜKƏSİZLİYİ KOMİTƏSİ

* 1. İnformasiya Təhlükəsizliyi Komitəsi (İTK), qurumda informasiya təhlükəsizliyinə dair siyasətlərin hazırlanması, idarə olunması, tətbiqi və daimi nəzarətin təmin edilməsi məqsədilə yaradılır. Komitənin tərkibində müxtəlif funksiyaları yerinə yetirən daimi üzvlər iştirak edir:

***Daimi üzvlər:***

* Qurumun İcraçı Direktoru
* İnformasiya Təhlükəsizliyi Direktoru
* İnformasiya Təhlükəsizliyi Direktoruna birbaşa tabe olan şöbələrin rəhbərləri.

***Komitənin iclaslarında qəbul edilən qərarlara aidiyyəti olan digər üzvlər:***

* Qurumun informasiya resurslarının sahibləri və nəzərdən keçirilən məsələlərə və qəbul edilən qərarlara aidiyyəti olan qurumun digər əlaqədar şöbələrin rəhbərləri
* Kənar məsləhətçilər və ekspertlər
* İnformasiya təhlükəsizliyi üzrə nəzərdə tutulmuş tədbirlərin yerinə yetirilməsi üçün məsul olan əməkdaşlar.
  1. Komitə yığıncaqları ən azı rübdə bir dəfə olmaqla, informasiya təhlükəsizliyinin idarə edilməsi tədbirlərinin səmərəliliyini nəzərdən keçirmək, qurumun informasiya ehtiyatlarında baş verən dəyişikliklərlə bağlı qərarlar qəbul etmək və risklərin idarə edilməsi üzrə fəaliyyətləri müzakirə etmək üçün zərurət yarandıqda keçirilir.
  2. Komitənin sədri yığıncaqların təşkili, müzakirələrin istiqamətləndirilməsi və qəbul edilən qərarların icrası üçün zəruri resursların təmin olunmasına cavabdehdir.
  3. Komitənin vəzifələrinə aşağıdakılar daxildir:
     1. Qurumun informasiya təhlükəsizliyi üzrə siyasət və əsas sənədlərinin nəzərdən keçirilməsi, razılaşdırılması və təsdiqlənməsi;
     2. İnformasiya təhlükəsizliyi üzrə idarəetmə sistemi proseslərinin və tədbirlərinin səmərəliliyinin təhlili və onların uyğunluğunun təmin edilməsi;
     3. Qurumun informasiya resurslarında yaranan risklərin, audit nəticələrinin və insidentlərin təhlil edilməsi, həmçinin risklərin azaldılmasına və insidentlərin həllinə yönəldilmiş işlərin planlaşdırılması və nəzarəti;
     4. Strategiya və biznes proseslərdə mühüm dəyişikliklərin, eləcə də böhran idarəçiliyi və fasiləsiz fəaliyyət planlarının müzakirəsi və razılaşdırılması;
     5. Komitə iclaslarında qəbul edilmiş qərarların İdarə Heyətinə təqdim edilməsi və iclas protokollarının təsdiq olunması;
  4. Komitənin iclaslarının qərarları barədə məlumat qurumun İdarə Heyətinin sədrinə təqdim olunur.
  5. Komitənin iclaslarının protokolları sədr tərəfindən yazılı şəkildə imzalanır və möhürlə təsdiq olunur.

# RİSKLƏRİN İDARƏOLUNMASI KOMİTƏSİ

6.1 Risklərin İdarəolunması Komitəsi, qurumun qarşılaşdığı potensial risklərin müəyyən edilməsi, qiymətləndirilməsi və effektiv idarə olunması məqsədilə yaradılır. Bu komitə, qurumun biznes məqsədlərinə və strateji hədəflərinə nail olmaq üçün risklərin minimuma endirilməsini, risklərə nəzarət tədbirlərinin hazırlanmasını və həyata keçirilməsini təmin edir. Komitənin tərkibinə aşağıdakı üzvlər daxildir:

***Daimi üzvlər:***

* Qurumun İcraçı Direktoru
* İnformasiya Təhlükəsizliyi Direktoru
* Kiber İdarəetmə və Risk şöbəsinin rəhbəri.

***Komitənin iclaslarında qəbul edilən qərarlara aidiyyəti olan digər üzvlər:***

* Qurumun informasiya resurslarının sahibləri və nəzərdən keçirilən məsələlərə və qəbul edilən qərarlara aidiyyəti olan qurumun digər əlaqədar şöbələrinin rəhbərləri
* Kənar məsləhətçilər və ekspertlər
* Risklərin idarəolunması üzrə nəzərdə tutulmuş tədbirlərin yerinə yetirilməsi üçün məsul olan əməkdaşlar.
  1. Komitə yığıncaqları rübdə ən azı bir dəfə olmaqla, qurumun risk idarəetmə strategiyalarının, tədbirlərinin və proseslərinin səmərəliliyini qiymətləndirmək, risklərin azaldılmasına dair planları razılaşdırmaq və qərarlar qəbul etmək məqsədilə zərurət yarandıqda keçirilir.
  2. Komitə sədri yığıncaqların təşkilini təmin edir, üzvlər arasında işin koordinasiyasını həyata keçirir və komitənin vəzifələrinin effektiv şəkildə yerinə yetirilməsinə nəzarət edir.
  3. Komitənin vəzifələrinə aşağıdakılar daxildir:
     1. İnformasiya təhlükəsizliyinə dair əsas sənədlərin və risklərin idarəolunması üzrə tədbirlərin nəzərdən keçirilməsi, razılaşdırılması və təkmilləşdirilməsi;
     2. Qurumun risklərinin, audit və insidentlərin nəticələrinin qiymətləndirilməsi, onların aradan qaldırılması üçün planların hazırlanması və təsdiq edilməsi;
     3. Risklərin azaldılmasına, fasiləsiz fəaliyyətin təmin edilməsinə və ciddi insidentlərin nəticələrinin idarə olunmasına yönəlmiş işlərin planlaşdırılması və icrasına nəzarət;
     4. Qurumun biznes proseslərində və informasiya təhlükəsizliyinə dair mühüm dəyişikliklərin nəzərdən keçirilməsi və təsdiq edilməsi;
     5. İnformasiya sahəsində qurumun risklərinin azaldılmasına yönəldilmiş iş planlarının razılaşdırılması, habelə onların icrasına nəzarət edilməsi;
     6. İnsidentlərin və mübahisələrin nəticələri ilə bağlı hesabatların təsdiq edilməsi və qəbul edilən qərarların yerinə yetirilməsinə nəzarət;
  4. Komitənin iclaslarının qərarları barədə məlumat yazılı şəkildə Qurumun İdarə Heyətinin sədrinə təqdim olunur.
  5. Komitənin iclaslarının protokolları sədr tərəfindən imzalanır və möhürlə təsdiq olunur.

# MƏSULİYYƏTLƏR

Məsuliyyət və səlahiyyətlər ixtisas və peşəkar bacarıqlara uyğun olaraq vəzifə bölgüsündə dəqiq şəkildə müəyyən edilmişdir. İnformasiya təhlükəsizliyinin davamlılığı və inkişafı İTİS Komandasına həvalə edilir, hansı ki, Baş İdarə tərəfindən təyin olunan nümayəndələr tərəfindən idarə olunur.

**7.1 Rəhbərlik Məsuliyyəti**

Qurum rəhbərliyi, təsdiq edilmiş və tətbiq olunan İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin (İTİS) effektivliyini təmin etməyi, bu sistemə riayət edilməsini təmin etməyi və onun uğurlu işləməsi üçün zəruri resursların (kadr, texniki vasitələr və proqram təminatı və s.) ayrılmasını öhdəsinə götürür.

Rəhbərlik, eyni zamanda, İTİS-in qurumun bütün səviyyələrində başa düşülməsini təmin etmək və işçilərin bu sistemin məqsəd və tələblərinə uyğun fəaliyyət göstərməsini dəstəkləmək üçün müvafiq tədbirlər görməyə məsuldur. Rəhbər şəxslər və müəyyən olunmuş idarəçilər İTİS-in qurulması, tətbiqi və davamlı inkişafı üçün aşağı səviyyəli işçilərlə əməkdaşlıq etməli, təhlükəsizlik təlimatlarına əməl etməli və zərurət yarandıqda proseslərə aktiv şəkildə qatılmalıdırlar.

**7.2 Rəhbərlik Nümayəndəsinin Məsuliyyəti**

* İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin (İTİS) planlaşdırılması və risklərin idarə edilməsi sahəsində qəbul edilə bilən risk səviyyəsinin müəyyənləşdirilməsi;
* Risklərin qiymətləndirilməsi metodologiyasının hazırlanması və tətbiqi;
* İTİS-in qurulmasında və tətbiqində dəstəkləyici fəaliyyətlər üçün lazımi resursların təmin edilməsi;
* İTİS tətbiqlərinin effektiv şəkildə icrası və idarə edilməsi;
* İTİS-in və nəzarət tədbirlərinin daxili auditlər vasitəsilə qiymətləndirilməsi;
* Rəhbərliyin nəzarət etmə (RNE) iclasları vasitəsilə İTİS-in effektivliyinin qiymətləndirilməsi;
* Mövcud strukturun qorunmasına və İTİS-də davamlı təkmilləşdirmələrin həyata keçirilməsinə cavabdehdir.
  1. **İTİS Komanda Üzvlərinin Məsuliyyəti**
* Bölmə və ya departamentlərə aid informasiya aktivlərinin müntəzəm inventarlaşdırılmasını və risk analizini aparmaq;
* İnformasiya aktivlərində təhlükəsizlik risklərinə təsir edəcək hər hansı bir dəyişiklik baş verdikdə, İdarəetmə Nümayəndəsini dərhal məlumatlandırmaq və risk qiymətləndirməsini həyata keçirmək;
* Bölmə/Şöbə işçilərinin siyasət və prosedurlara uyğun fəaliyyət göstərməsini təmin etmək, işlərin təhlükəsizliyini qorumaq və siyasətə uyğunluğunu izləmək;
* Bölmələrə və şöbələrə İTİS çərçivəsində məlumatlılığın artırılması, əlaqələrin təşkili və sənədləşmə tələblərinin müəyyənləşdirilməsi ilə bağlı işlər görmək;
* İTİS strukturunun davamlı olaraq qorunmasına və təkmilləşdirilməsinə cavabdeh olmaq, sistemin effektivliyinin artırılması üçün təşəbbüslər irəlilətmək.
  1. **Daxili Auditorun Məsuliyyəti**

Daxili auditor, İTİS-in effektivliyini və uyğunluğunu qiymətləndirmək, risklərin idarə olunmasını və təhlükəsizlik prosedurlarının tətbiqini yoxlamaq, İTİS-nin məqsədlərinə çatması üçün təkmilləşdirmə təklifləri vermək və təhlükəsizlik insidentlərinin və pozuntularının araşdırılmasına rəhbərlik etməkdən məsuldur.

* 1. **Bölmə/Şöbə Rəhbərlərinin Məsuliyyəti**

Bölmə/Şöbə rəhbərləri, İnformasiya Təhlükəsizliyi Siyasətinin tətbiqinə nəzarət etmək, işçilərin siyasətə uyğun fəaliyyət göstərmələrini təmin etmək, üçüncü tərəflərin siyasətdən məlumatlı olmalarını təmin etmək və təhlükəsizlik pozuntularının vaxtında və düzgün şəkildə bildirilməsini təşkil etməkdən cavabdehdir.

* 1. **Bütün İşçilərin Məsuliyyəti**

Bütün işçilər, İnformasiya Təhlükəsizliyi Siyasətinin və əlaqədar prosedurların tələblərinə riayət etməli, təhlükəsizlik tədbirlərinə uyğun fəaliyyət göstərməli və qarşılaşdıqları təhlükəsizlik pozuntuları barədə dərhal müvafiq şəxsləri məlumatlandırmalıdırlar.

* 1. **Üçüncü Tərəflərin Məsuliyyəti**

Üçüncü tərəflər, İnformasiya Təhlükəsizliyi Siyasətinin tələblərinə uyğunluğunu təmin etməli, İTİS çərçivəsində göstərilən davranış qaydalarına riayət etməli və siyasətin tətbiqi ilə əlaqədar hər hansı bir pozuntuya dair məlumat verməlidirlər.

# TƏTBİQ

* 1. **Risk İdarəetmə Çərçivəsi**

İnformasiya təhlükəsizliyi siyasətində risk idarəetmə çərçivəsi, qurumun informasiya təhlükəsizliyini qorumaq və riskləri idarə etmək məqsədilə nəzərdə tutulan bir yanaşmadır. Bu çərçivə, risklərin müəyyən edilməsi, qiymətləndirilməsi, azaldılması və izlənməsi proseslərini əhatə edir. İlk növbədə, qurumun informasiya resurslarına aid risklər tanınır və onların təsirləri qiymətləndirilir. Risklərin qiymətləndirilməsi əsasında ən yüksək təhlükə və zərər potensialı olan risklər prioritetləşdirilir. Növbəti mərhələdə, risklərin idarə edilməsi üçün uyğun texniki və təşkilati tədbirlər görülür və bu tədbirlər mütəmadi olaraq qiymətləndirilir və təkmilləşdirilir.

Risk idarəetmə çərçivəsi həmçinin, qurum daxilində və xarici tərəflərlə düzgün kommunikasiya və əlaqələndirmə vasitəsilə risklərlə bağlı məlumat mübadiləsini təmin edir. Risk idarəetmə prosesləri mütəmadi olaraq izlənir və yeni yaranan təhlükəsizlik təhdidlərinə qarşı uyğun tədbirlər görülür. Bu çərçivənin əsas məqsədi təhlükəsizlik tədbirlərinin səmərəliliyini artırmaq və qurumun informasiya təhlükəsizliyi mühitini davamlı olaraq gücləndirməkdir.

# İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏŞKİLİ

## Daxili Nizamlama

Qurumun bütün işçiləri üçün informasiya təhlükəsizliyinin təmin edilməsi ilə bağlı konkret vəzifələr müəyyən edilməli və bu vəzifələrin icrasını dəstəkləyən səriştə tələbləri nəzərə alınmalıdır. Aktivlərin qorunması üçün ziddiyyətli vəzifə və məsuliyyətlər bir-birindən ayrılmalı, bu isə icazəsiz dəyişiklik və sui-istifadə imkanlarını minimuma endirməlidir. Həmçinin, təhlükəsizlik pozuntularının aşkarlanması, qeydə alınması və müvafiq səlahiyyətli şəxslərlə vaxtında əlaqə saxlanılmasını təmin edən prosedurlar tətbiq edilməlidir.

# İNSAN RESURSLARININ TƏHLÜKƏSİZLİYİ

## İşə Başlamadan Əvvəl

* + 1. İşə qəbul ediləcək şəxslərin və ya üçüncü tərəflərin uyğunluğu yoxlanılmalı, onların təcrübəsi, bilikləri və səriştələri müəyyən edilməlidir. Yoxlama prosesi işin xarakterinə uyğun olaraq həyata keçirilməlidir.Yoxlamanın dərinliyi və əhatəliliyi işçinin vəzifəsi, ona təklif olunan işin xüsusiyyətləri və onun hansı informasiya resurslarına giriş hüququnun verilməsi ilə müəyyənləşdirilməlidir.
    2. Namizədlərlə bağlanacaq müqavilələrdə onların informasiya təhlükəsizliyinə dair öhdəlikləri dəqiq şəkildə göstərilməli və onların bu öhdəlikləri tam başa düşməsi təmin edilməlidir.
    3. İşə başlamazdan əvvəl bütün işçilər və ya podratçılar, informasiya təhlükəsizliyinə və məxfiçilik tələblərinə riayət edəcəklərini təsdiqləyən sənəd imzalamalıdırlar.

## İş Müddətində

* + 1. İşçilər qurumun informasiya təhlükəsizliyi siyasətinə tam şəkildə əməl etməli və vəzifələrini yerinə yetirərkən bu qaydaları rəhbər tutmalıdırlar.
    2. İşçilər informasiya təhlükəsizliyinə dair hər hansı pozuntunu və ya şübhəli vəziyyəti dərhal müvafiq məsul şəxsə bildirmək üçün məsuliyyət daşıyır.
    3. İş müddətində işçilərin informasiya aktivlərinə və sistemlərə giriş hüquqları müntəzəm olaraq nəzərdən keçirilməli və yalnız zəruri səviyyədə saxlanılmalıdır.

## İşə Xitam Verilməsi Və Dəyişdirilməsi

* + 1. İşçinin qurumla əmək münasibətləri başa çatdıqda və ya vəzifəsi dəyişdirildikdə, ona verilmiş bütün fiziki və elektron resurslar (şəxsi kompüterlər, cihazlar, identifikasiya kartları, parollar və s.) geri alınmalı və ya istifadəsi dayandırılmalıdır.
    2. İşçinin informasiya aktivlərinə giriş hüquqları dərhal ləğv edilməli, giriş sistemlərindən istifadə qeydləri nəzərdən keçirilməli və lazımi dəyişikliklər aparılmalıdır.

# AKTİVLƏRİN İDARƏOLUNMASI

## Aktivlərə Görə Məsuliyyət

Aktivlərin idarəolunması çərçivəsində qurumun informasiya və məlumatların emalı ilə əlaqəli aktivləri, obyektləri müəyyən edilməli və onların inventarizasiyası aparılmalıdır. Aktivlərin idarə edilməsinə məsul şəxslər təyin olunmalı, bu şəxslər aktivlərlə bağlı bütün səlahiyyətləri və məsuliyyətləri daşımalıdırlar.

Aktivlərin istifadəsi ilə bağlı qaydalar tərtib edilməli, sənədləşdirilməli və bütün işçilər, eləcə də üçüncü tərəflər üçün tətbiq edilməlidir. Qurum aktivlərinin düzgün istifadəsini təmin etmək məqsədilə əməkdaşlar və kontragentlər əməkdaşlıq bitdikdən sonra bütün aktivləri təhvil vermək öhdəliyini yerinə yetirməlidirlər.

## İnformasiyanın Təsnifatı

* + 1. Bütün informasiya növləri onların həssaslıq səviyyəsinə və təhlükəsizlik tələblərinə əsaslanaraq təsnif edilməlidir. Ümumi kateqoriyalar olaraq məxfi, məhdud, daxili istifadə, ictimai kimi səviyyələr müəyyən edilə bilər.
    2. Təsnif edilmiş informasiya müvafiq təhlükəsizlik tələblərinə uyğun etiketlənməli və qorunmalıdır. Elektron və fiziki mühitlərdə informasiyanın saxlanması və ötürülməsi zamanı onların məxfiliyini təmin etmək üçün uyğun texnoloji həllər və nəzarət mexanizmləri tətbiq olunmalıdır.
    3. Aktivlərin idarə edilməsi prosedurları qurum tərəfindən qəbul edilən informasiya təsnifat sxeminə əsasən hazırlanmalı və həyata keçirilməlidir.

## İnformasiya Daşıyıcıları İlə İşləmə

* + 1. İnformasiya daşıyıcılarının idarə olunması qurumun təhlükəsizlik tələblərinə uyğun həyata keçirilməlidir.
    2. Daşıyıcıların təyin edilməsi, istifadə qaydalarının müəyyənləşdirilməsi və qorunması üçün müvafiq prosedurlar hazırlanmalıdır. İnformasiya daşıyıcılarının icazəsiz istifadəsi və məzmununun sızması risklərini azaltmaq üçün nəzarət mexanizmləri tətbiq edilməli, həmçinin məlumatların daşınması, saxlanması və məhv edilməsi zamanı təhlükəsizlik tədbirləri görülməlidir.
    3. Daşıyıcıların itirilməsi, zədələnməsi və ya yanlış şəxslərin əlinə keçməsi hallarında tətbiq olunacaq tədbirlər əvvəlcədən müəyyən edilməlidir.

# GİRİŞ NƏZARƏTİ

## Giriş Nəzarətində Biznes Tələbləri

* + 1. Qurumun məlumatlarının və sistemlərinin məxfiliyini, bütövlüyünü və əlçatanlığını qorumaq üçün giriş nəzarəti tədbirləri biznes tələbləri ilə uzlaşdırılmalıdır. İcazə hüquqları yalnız işçinin və ya üçüncü tərəfin iş funksiyalarına uyğun olaraq verilməli və lazımsız giriş hüquqları məhdudlaşdırılmalıdır.
    2. Hər bir informasiya sisteminə giriş üçün biznes məqsədinə əsaslanan tələblər müəyyən edilməli və bu tələblərə uyğun siyasət və prosedurlar tətbiq edilməlidir. Giriş hüquqlarının təyin edilməsi, icazələrin verilməsi və istifadəsinin monitorinqi sistematik şəkildə həyata keçirilməlidir.
    3. Biznes tələblərinə uyğunluğun təmin olunması üçün müntəzəm olaraq giriş hüquqları nəzərdən keçirilməli, dəyişikliklər və xitam hallarına operativ nəzarət edilməlidir.

## İstifadəçi Girişinin İdarə Edilməsi

* + 1. İnsan resursları departamenti ilə birgə əməkdaşlıq çərçivəsində, istifadəçilərin giriş hüquqları iş vəzifələrinə uyğun olaraq müəyyən edilməli və nəzarət altında saxlanılmalıdır. İşə qəbul, departamentlərarası keçid və ya işdən çıxma hallarında giriş hüquqlarının təyin edilməsi, dəyişdirilməsi və ləğvi İnsan resursları departamentinin təqdim etdiyi məlumatlar əsasında həyata keçirilməlidir.
    2. Yeni istifadəçilər üçün giriş icazələri İnsan resursları departamentinin təsdiq etdiyi səlahiyyətlərə uyğun olaraq təyin olunmalı və təsdiq edilməlidir. İşçilərin giriş hüquqları və hesablarının aktivliyi mütəmadi olaraq yenidən yoxlanılmalı və artıq zəruri olmayan icazələrin ləğvi təmin edilməlidir.
    3. İT Komitəsi informasiya sistemlərinə və resurslarına giriş hüquqlarının razılaşdırılması, verilməsi, dəyişdirilməsi, bağlanması prosedurlarının bu təlimatın tələblərinə uyğunluğunu yoxlamalıdır.

## İstifadəçinin Məsuliyyətləri

İstifadəçilər giriş hüquqlarından yalnız iş məqsədləri üçün istifadə etməyə, giriş məlumatlarının məxfiliyini qorumağa və informasiya təhlükəsizliyi siyasətinin tələblərinə riayət etməyə məsuliyyət daşıyırlar.

## Sistem Və Proqram Girişinə Nəzarət

* + 1. İnformasiya sistemlərinə və tətbiqlərinə çıxışı məhdudlaşdırmaq və nəzarət etmək üçün bütün giriş tələbləri, tətbiq olunan təhlükəsizlik qaydalarına uyğun olaraq müəyyən edilməli və sənədləşdirilməlidir.
    2. İstifadəçilərin sistemlərə və resurslara giriş hüquqları yalnız düzgün sənədləşdirildikdən sonra verilə bilər.
    3. Giriş hüquqlarının verilməsi, istifadəçilərin kimliyini təsdiqləyən prosedurlardan keçməsini tələb etməlidir. Bu, identifikasiya, autentifikasiya və avtorizasiya proseslərinin düzgün yerinə yetirilməsi ilə təmin edilə bilər.
    4. İstifadəçiyə şifrə veriləndən sonra, istifadəçi ilk dəfə sistemi işə salarkən şifrəni dəyişdirməlidir. Həmçinin, şifrənin təhlükəsiz şəkildə təqdim edilməsi və istifadəçi tərəfindən dəyişdirilməsinin təmin edilməsi vacibdir.
    5. İstifadəçi tərəfindən təyin edilən şifrənin minimum uzunluğu istifadəçinin şifrəsi 8 simvoldan (inzibatçılar üçün – 12 simvoldan) az olmamalı, kiçik və böyük hərflərdən, rəqəm və ya digər simvollardan (məsələn, !, $, #, %) ibarət olmalı, rübdə bir dəfədən az olmayaraq vaxtaşırı mütləq dəyişdirilməlidir.
    6. Şəbəkə və tətbiq səviyyəsindəki təhlükəsizlik nəzarətlərini aşan və ya bypass edən proqramların istifadəsi qadağan olunmalı və bu proqramlara ciddi nəzarət edilməlidir.
    7. Proqramların mənbə koduna yalnız təyin edilmiş icazələrə malik şəxslər tərəfindən giriş təmin edilməlidir.

# KRİPTOQRAFİYA

## Kriptoqrafik Nəzarət

* + 1. İnformasiyanın qorunması məqsədilə kriptoqrafik vasitələrdən istifadənin təşkili ilə əlaqədar olaraq, xüsusi sənəd hazırlanmalı və tətbiq edilməlidir. Bu sənəd aşağıdakıları əhatə etməlidir:
* Hansı informasiya növlərinin kriptoqrafik alətlər ilə qorunacağı müəyyən edilməlidir;
* İnformasiyanın şifrələnməsi üçün kriptoqrafik alqoritmlərin təhlükəsizlik səviyyəsi, risk analizinə əsaslanaraq müəyyən olunmalıdır;
* Kriptoqrafik alətlərin istifadəsi ilə bağlı məsuliyyətlər, öhdəliklər və səlahiyyətlər təyin edilməlidir.
  + 1. Kriptoqrafik açarların idarə edilməsi üçün ayrıca sənəd hazırlanmalı və tətbiq edilməlidir. Bu sənəd aşağıdakı məsələləri əhatə etməlidir:
* Kriptoqrafik açarların yaradılması, müvafiq təhlükəsizlik standartlarına uyğun olaraq həyata keçirilməlidir;
* Kriptoqrafik açarların paylanması və təhlükəsiz şəkildə idarə olunması prosedurları müəyyən edilməlidir;
* Kriptoqrafik açarların zamanla yenilənməsi və ehtiyatlı şəkildə saxlanılması təmin edilməlidir;
* Kriptoqrafik açarların istifadədən çıxarılması, geri çağırılması və ya deaktiv edilməsi prosedurları təyin edilməlidir;
* Kriptoqrafik açarların ehtiyat nüsxələrinin saxlanması və məhv edilməsi qaydaları müəyyən edilməlidir;
* Kriptoqrafik açarların idarə edilməsi ilə bağlı əməliyyatların izlənməsi üçün loqların qeydiyyatı aparılmalıdır.

# FİZİKİ VƏ ƏTRAF MÜHİT TƏHLÜKƏSİZLİYİ

## Təhlükəsiz Ərazilər

* + 1. İnformasiya təhlükəsizliyinin təmin edilməsi məqsədilə, qurum informasiya resurslarının yerləşdiyi və məlumatların emal edildiyi sahələrin planını dəqiq müəyyən etməli və bu planı rəsmi olaraq sənədləşdirməlidir. Bu sənəd həmçinin ofisin ümumi perimetrini və təhlükəsizlik sərhədlərini əhatə etməlidir.
    2. Qurumun fiziki təhlükəsizliyi üçün, ofisin girişlərində mühafizə tədbirləri gücləndirilməli, kənar şəxslərin icazəsiz daxil olmasının qarşısını almaq üçün perimetr divarları, işıqlandırma və videomüşahidə sistemləri qurulmalıdır.
    3. Mühafizə və siqnalizasiya sistemlərinin düzgün işləməsini təmin etmək üçün, bu sistemlərin periodik olaraq test edilməsi və təkmilləşdirilməsini həyata keçirməlidir.
    4. Quruma daxil olan kənar şəxslərin, ərazidə və binalarda hərəkət etməsi yalnız əvvəlcədən müəyyən olunmuş vəzifəli şəxslərin razılığı ilə, təhlükəsizlik qaydalarına uyğun şəkildə müşayiət olunmalıdır.
    5. Quruma daxil olan kənar şəxslərin, ərazidə və binalarda hərəkət etməsi yalnız əvvəlcədən müəyyən olunmuş vəzifəli şəxslərin razılığı ilə, təhlükəsizlik qaydalarına uyğun şəkildə müşayiət olunmalıdır.
    6. Server otaqlarında fiziki təhlükəsizlik təmin edilməli, su və kanalizasiya borularının keçirilməsi qadağan edilməlidir.
    7. Server otaqları və kritik məlumatların işlənildiyi sahələrdə, temperatur və yanğın sensörlərinin quraşdırılması təmin edilməlidir.
    8. Qurum rəhbərliyi, server otaqları və məlumatların təhlükəsiz saxlanıldığı sahələr, müvafiq videomüşahidə sistemləri ilə izlənməli və təhlükəsizlik tədbirləri ilə təchiz edilməlidir.

## Avadanlıq Və Cihazlar

* + 1. Avadanlıqların düzgün yerləşdirilməsi və qorunması, ekoloji və fiziki risklərin qarşısını almaq məqsədilə həyata keçirilməlidir.
    2. Kompüter və periferiya qurğuları mütəmadi olaraq diaqnostika və profilaktik yoxlamalardan keçirilməli, bu proseslər hər altı aydan bir dəfə olmalıdır.
    3. Hər hansı bir nasazlıq və ya yeni proqram təminatına ehtiyac yarandıqda, müvafiq avadanlıq və proqram təminatları üzrə dəyişikliklər barədə İT şöbəsinə məlumat verilməlidir.
    4. Məlumat daşıyan avadanlıqlar, kabellər və digər müvafiq infrastruktur, fiziki müdaxilədən qorunmalı və zədələnmənin qarşısı alınmalıdır.
    5. Daşınan məlumat daşıyıcılarının təhlükəsizliyi üçün, daşınan avadanlıqlara müdaxilənin qarşısını almaq üçün təhlükəsizlik tədbirləri həyata keçirilməlidir.
    6. Yaddaş daşıyıcıları və digər informasiya daşıyıcıları üzərindəki məlumatların təhlükəsiz silinməsi və ya yenidən yazılması, məlumatın təkrar istifadəsi və ya məhv edilməsi təmin edilməlidir.
    7. Kağız sənədləri və çıxarıla bilən yaddaş daşıyıcıları ilə bağlı bütün təhlükəsizlik tələbləri sənədləşdirilməli və tətbiq edilməlidir.

# ƏMƏLİYYAT TƏHLÜKƏSİZLİYİ

## Əməliyyat Prosedurları Və Məsuliyyətlər

* + 1. Əməliyyat prosedurları strukturlaşdırılmış şəkildə tərtib edilməli, sənədləşdirilməli və yalnız məsul şəxslərin istifadəsinə açıq olmalıdır. Bu prosedurlara proqram təminatının yüklənməsi, məlumat ehtiyatlarının təhlükəsiz surətdə saxlanılması, səhvlərin idarə edilməsi və fövqəladə hallarda cavab tədbirləri və s. daxildir.
    2. Qurumun informasiya sistemləri və biznes proseslərindəki dəyişikliklər təhlükəsizlik baxımından dəyərləndirilməli, təsirləri idarə etmək üçün uyğun nəzarət mexanizmləri tətbiq edilməlidir.
    3. Resurs istifadəsi, sistem performansı və fəaliyyət tələbləri davamlı olaraq monitorinq edilməli, analitik vasitələrlə proqnozlaşdırılmalı və planlama tədbirləri həyata keçirilməlidir.
    4. Əməliyyat mühiti, sınaq və inkişaf mühitlərindən ayrılmalı və bu ayrılıq kiberhücum və ya icazəsiz dəyişikliklərin qarşısını almaq üçün sərt nəzarətlə dəstəklənməlidir.

## Zərərli Proqramlardan Qorunma

* + 1. Qurum sistemlərinin zərərli proqramlardan qorunması üçün profilaktik tədbirlər görülür. Bunun üçün yalnız təhlükəsizlik tələblərinə cavab verən lisenziyalı proqram təminatlarından istifadə edilir.
    2. Zərərli proqramlara qarşı çoxsəviyyəli qorunma sistemi tətbiq edilir və bu tədbirlər aşağıdakı sahələri əhatə edir:
* Əsas kompüter sistemləri və serverlərin daxili müdafiəsi;
* Elektron poçt və internet trafiki üzərində nəzarət.
  + 1. İstifadə olunacaq hər bir proqram təminatı və cihaz ilkin olaraq zərərverici proqramların olub-olmaması baxımından yoxlanılır. Yalnız yoxlamadan keçmiş tətbiqlər sistemlərə inteqrasiya edilir.
    2. Zərərli proqram təhlükələrinin aşkar edilməsi halları dərhal qeyd olunur. Bu hallar analiz edilir və zərərli proqramların mənbəyi, növü və yayılma üsulları müəyyən edilir.
    3. Avadanlıqların təhlükəsizliyini təmin etmək üçün mütəmadi olaraq yoxlama və texniki profilaktika həyata keçirilir. Bütün yeniləmələr və təhlükəsizlik tədbirləri standartlara uyğun şəkildə tətbiq olunur.

## Ehtiyat Nüsxələrinin Yaradılması Və Bərpası

* + 1. Qurum məlumatlarının qorunması üçün bütün zəruri ehtiyat nüsxələrin mütəmadi şəkildə yaradılması və təhlükəsizlik tələblərinə uyğun saxlanılması təmin edilməlidir. Ehtiyat nüsxələr hazırlanan plan əsasında sınaqdan keçirilməli və nəticələr sənədləşdirilməlidir.
    2. Ehtiyat nüsxə götürülməsi və bərpası üzrə aşağıdakı əsas prinsiplər tətbiq olunmalıdır:
* Məlumatların ehtiyat nüsxələrinin götürülməsi və bərpası ilə bağlı məsuliyyətlər dəqiq müəyyən edilməlidir.
* Nüsxələrin şifrələnməsi və yalnız səlahiyyətləndirilmiş şəxslər üçün əlçatan olması təmin edilməlidir.
* Müxtəlif dövrlər üçün (gündəlik, həftəlik, aylıq) nüsxə götürmə qaydaları müəyyən edilməli və yerinə yetirilməlidir.
* Sınaq məqsədli bərpa prosesləri planlı şəkildə həyata keçirilməli, prosedurun effektivliyi yoxlanılmalı və nəticələr qeydə alınmalıdır.
* Ehtiyat nüsxələrin yaradılması üzrə əməliyyatların qeydiyyatı aparılmalı və müntəzəm təhlil edilməlidir.
  + 1. Ehtiyat nüsxələrin saxlanılması zamanı məlumatların oğurlanması, məhv edilməsi və ya icazəsiz müdaxilə kimi risklərin qarşısını almaq üçün təhlükəsizlik tədbirləri görülməlidir. Ehtiyat nüsxələr hər hansı fiziki və kiber təhlükələrdən uzaq mühitdə saxlanılmalıdır.
    2. Təbii fəlakətlər, texnogen qəzalar və digər gözlənilməz hallar zamanı məlumatların qorunmasını təmin etmək üçün ehtiyat nüsxələr alternativ coğrafi məkanda və ya xüsusi mühafizə olunan obyektlərdə saxlanılmalıdır.
    3. Yaddaş daşıyıcıları, serverlər və digər məlumat saxlama vasitələrinin tələblərinə uyğun olaraq, ehtiyat nüsxələrin saxlanma şərtləri istehsalçının təlimatlarına əsasən tənzimlənməlidir.
    4. Ehtiyat nüsxələrin istifadəsi, bərpası və ya məhv edilməsi yalnız müvafiq səlahiyyətə malik şəxslərin nəzarəti altında həyata keçirilməlidir və bu proseslərin hər biri sənədləşdirilməlidir.

## Loqlaşdırma Və Monitorinq

* + 1. İstifadəçi fəaliyyətləri, nasazlıqlar, istisnalar və təhlükəsizlik hadisələri ilə bağlı bütün loqlar mütəmadi olaraq yaradılmalı, saxlanılmalı və audit üçün nəzərdən keçirilməlidir. Hadisə loqlarında qeydə alınan məlumatlar, potensial təhlükəsizlik risklərinin erkən aşkarlanmasına və sistemin etibarlılığının təmin edilməsinə xidmət etməlidir.
    2. Loqlama sistemləri və onların qeydləri, məlumatların təhlükəsizliyini təmin etmək üçün şifrələnməli və qeyri-qanuni müdaxilələrdən qorunmalıdır. Loqlara yalnız müvafiq icazəyə malik şəxslərin giriş imkanı olmalıdır. Həmçinin, loqların manipulyasiya edilməsi və silinməsi qadağan edilməlidir.
    3. Sistem inzibatçılarının və operatorlarının fəaliyyətləri diqqətlə loqlanmalı, onların hərəkətləri müntəzəm olaraq monitorinq edilməlidir. Hər hansı şübhəli və ya qeyri-adi fəaliyyət aşkar olunduqda dərhal araşdırma aparılmalı və müvafiq tədbirlər görülməlidir.
    4. Qurumdakı bütün informasiya emal sistemlərinin saatları vahid istinad vaxtına uyğun olaraq sinxronlaşdırılmalıdır. Bu, loq məlumatlarının təhlilinin dəqiqliyini təmin edəcək və hadisələrin ardıcıllığını izləməyə kömək edəcəkdir.

## Proqram Təminatına Nəzarət

* + 1. Əməliyyat sistemlərində proqram təminatının quraşdırılmasına və dəyişdirilməsinə nəzarət etmək üçün hərtərəfli prosedurlar hazırlanmalı və tətbiq edilməlidir. Bu prosedurlar vasitəsilə yalnız müvafiq təhlükəsizlik tələblərinə cavab verən və qurumun ehtiyaclarına uyğun olan proqram təminatlarının istifadəsinə icazə verilməlidir.
    2. Qurumda yalnız hüquqi olaraq lisenziyalı və təhlükəsiz açıq mənbəli proqram təminatları istifadə edilməlidir. Proqram təminatının lisenziyası və hüquqi vəziyyəti mütəmadi olaraq yoxlanılmalı, hər hansı qanunsuz proqram təminatının istifadəsinin qarşısı alınmalıdır.
    3. Qurum daxilində və ya sifarişlə hazırlanan bütün proqram təminatlarının ilkin kodları, müvafiq təhlükəsizlik tələblərinə uyğun olaraq saxlanmalı və müntəzəm olaraq yenilənməlidir. Proqram təminatının hər hansı bir versiyası və ya çıxış kodunda dəyişikliklər zamanı, İT Departamenti tərəfindən təhlil və yoxlama aparılmalıdır.
    4. İstifadəçilər və İT əməkdaşları tərəfindən qeyri-lisenziyalı və ya təhlükəsizlik riskləri yaradan proqram təminatlarının quraşdırılması və istifadəsi qəti şəkildə qadağan edilməlidir. Bu cür proqram təminatlarının aşkar edilməsi halında, dərhal müvafiq tədbirlər görülməlidir.
    5. Qurum daxilində bütün iş stansiyalarında quraşdırılmış proqram təminatları müntəzəm olaraq yoxlanılmalı, təhlil edilməli və zəruri təkmilləşdirmələr və yeniləmələr tətbiq olunmalıdır. Hər hansı bir zəiflik və ya nasazlıq aşkar edildikdə, dərhal düzəlişlər edilməli və təhlükəsizlik tədbirləri gücləndirilməlidir.

## Texniki Zəifliyin İdarə Edilməsi

* + 1. Qurum daxilində istifadə olunan informasiya sistemlərinin hər birindəki texniki zəifliklər mütəmadi olaraq izlənməli və qiymətləndirilməlidir. Hər hansı bir zəiflik aşkar edildikdə, bu zəifliyin qurumun infrastrukturu və məlumatları üzərində yaradacağı təsir təhlil edilməli və uyğun risk qiymətləndirilməsi aparılmalıdır. Zəifliyin aradan qaldırılması üçün dərhal tədbirlər görülməli, zərər potensialı minimuma endirilməli və mümkün olan təmir və yeniləmələr sürətlə həyata keçirilməlidir.
    2. İstifadəçilər tərəfindən yeni proqram təminatlarının quraşdırılması ilə bağlı aydın və sərt qaydalar müəyyən edilməli, bu qaydalar qurumun təhlükəsizlik siyasətinə uyğun olmalıdır. Proqram təminatının yalnız rəsmi lisenziyalı və təhlükəsiz mənbələrdən quraşdırılması tələb edilməli, qeyri-qanuni və ya təsdiq edilməmiş proqramların quraşdırılması qadağan edilməlidir. Bütün proqram təminatları quraşdırılmadan əvvəl müvafiq İT şöbəsinin təsdiqindən keçməlidir.

## İnformasiya Sistemlərinin Audit Tələbləri

* + 1. Audit tələbləri və əməliyyat sistemlərinin yoxlanılması ilə bağlı fəaliyyətlər mütəmadi olaraq planlaşdırılmalı və həyata keçirilməlidir. Bu fəaliyyətlər qurumun informasiya təhlükəsizliyi və əməliyyat mühitinin effektivliyini təmin etmək məqsədilə biznes proseslərində mümkün olan pozuntuları və təhlükəsizlik boşluqlarını aşkar etmək üçün nəzərdə tutulmuşdur. Audit və yoxlama fəaliyyətləri, əməliyyat sistemlərinin və proseslərin təkmilləşdirilməsi üçün strateji olaraq razılaşdırılmalı və istənilən pozuntunun yaranmasının qarşısını almaq üçün müvafiq tədbirlər planı hazırlanmalıdır.

# KOMMUNİKASİYA TƏHLÜKƏSİZLİYİ

## Şəbəkə Təhlükəsizliyinin İdarəolunması

* + 1. Quruma məxsus şəbəkələrin təhlükəsizliyini təmin etmək üçün şəbəkə infrastrukturu və onun idarə olunması üçün müvafiq siyasətlər, prosedurlar və texnologiyalar tətbiq edilməlidir.
    2. Şəbəkə vasitəsilə məlumatların ötürülməsi zamanı məlumatların məxfiliyi, bütövlüyü və mövcudluğu təmin edilməlidir. Bu məqsədlə məlumatların şifrələnməsi, girişin məhdudlaşdırılması və monitorinq texnologiyalarından istifadə edilməlidir.
    3. Daxili şəbəkə sistemləri ilə xarici şəbəkələr arasında təhlükəsizlik divarları (firewall) və digər müdafiə tədbirləri tətbiq edilməli, şəbəkə zonalarının düzgün şəkildə ayrılması təmin olunmalıdır.
    4. Şəbəkəyə giriş hüquqları yalnız müvafiq səlahiyyətə malik şəxslərə verilməlidir. Bütün şəbəkə istifadəçiləri üçün autentifikasiya sistemlərindən və şifrə idarəetmə mexanizmlərindən istifadə edilməlidir.
    5. Şəbəkə avadanlıqlarının və onların konfiqurasiyalarının müntəzəm olaraq yoxlanılması və yenilənməsi həyata keçirilməlidir. Potensial zəifliklərin qarşısını almaq üçün təhlükəsizlik yamalarının (patch) tətbiqi təmin edilməlidir.
    6. Şəbəkə fəaliyyətinə dair bütün hadisələr loqlaşdırılmalı və təhlükəsizlik pozuntularını aşkar etmək üçün analiz edilməlidir. Loq qeydləri icazəsiz girişdən qorunmalı və müəyyən edilmiş dövr ərzində saxlanılmalıdır.
    7. Xarici əlaqələr üçün, o cümlədən İnternet, bulud xidmətləri və qurumlarla şəbəkə əlaqələri üçün xüsusi təhlükəsizlik tədbirləri tətbiq edilməli, məlumat axınları təhlükəsizlik siyasətlərinə uyğun idarə edilməlidir.
    8. Şəbəkə təhlükəsizliyini təhdid edən istənilən riskin operativ şəkildə həll olunması üçün fövqəladə hallara dair tədbirlər planı hazırlanmalı və tətbiq edilməlidir.

# SİSTEMİN ƏLDƏ EDİLMƏSİ, İNKİŞAFI VƏ SAXLANMASI

## İnformasiya Sistemlərinin Təhlükəsizlik Tələbləri

* + 1. İnformasiya sistemlərinin yaradılması və ya mövcud sistemlərin yenilənməsi zamanı təhlükəsizlik tələbləri ilkin mərhələdən etibarən müəyyən edilməli və layihə planına daxil edilməlidir.
    2. Tətbiq xidmətlərində istifadə edilən məlumatlar düzgün ötürülməsi, yalnız təyinatına uyğun olaraq istifadəsi və icazəsiz girişlərdən müdafiə olunması üçün lazımi tədbirlər həyata keçirilməlidir.

## İnkişaf Və Dəstək Proseslərində Təhlükəsizlik

* + 1. Proqram təminatı və sistemlərin inkişafı üçün təhlükəsizlik tələbləri inteqrasiya edilməli və bu tələblər bütün inkişaf fəaliyyətləri boyunca tətbiq edilməlidir.
    2. İnkişaf prosesində edilən dəyişikliklər təsdiqlənmiş prosedurlara uyğun sənədləşdirilməli və dəyişikliklərin riskləri əvvəlcədən qiymətləndirilməlidir.
    3. Yeni və ya dəyişdirilmiş əməliyyat platformaları istifadəyə verilməzdən əvvəl, onların qurumun əməliyyatlarına və təhlükəsizlik tədbirlərinə mənfi təsirinin olmaması təmin edilməlidir.
    4. Sistemlərdə və proqram təminatında aparılan hər hansı dəyişikliklər yalnız zəruri hallarda həyata keçirilməli və dəyişikliklərə uyğun icazələr alınmalıdır.
    5. Təhlükəsizlik baxımından mühüm olan sistemlərin inkişafı zamanı universal təhlükəsizlik prinsiplərinə uyğun mühəndislik yanaşmaları tətbiq edilməli və sənədləşdirilməlidir.
    6. İnkişaf və dəstək fəaliyyətləri üçün təhlükəsiz infrastruktur təmin edilməli, həmin mühitlər qorunmalı və yalnız müəyyən edilmiş işçilərin çıxışına icazə verilməlidir.
    7. Qurum tərəfindən autsorsinq yolu ilə həyata keçirilən proqram təminatı inkişafı proseslərinə nəzarət edilməli və bu fəaliyyətlər üçün təhlükəsizlik tələbləri dəqiq müəyyən edilməlidir.
    8. İnkişaf mərhələsində proqram təminatının təhlükəsizlik komponentləri və funksiyaları sınaqdan keçirilməli və bu sınaqların nəticələri əsasında təhlükəsizlik zəiflikləri aradan qaldırılmalıdır.

## Test Məlumatları

* + 1. Test prosesində istifadə olunan məlumatların məxfiliyinin təmin edilməsi üçün real məlumatlardan mümkün qədər istifadə edilməməli və anonimləşdirilmiş məlumatlar tətbiq edilməlidir.
    2. Test məlumatlarının əldə edilməsi, saxlanılması və istifadəsi səlahiyyətli şəxslərin nəzarəti altında həyata keçirilməlidir.
    3. Real məlumatlardan istifadə zərurəti yarandıqda, onların təhlükəsizliyini təmin etmək üçün şifrələmə və digər təhlükəsizlik tədbirləri tətbiq edilməlidir.
    4. Test məlumatlarının istifadəsindən sonra onların saxlanılması ilə bağlı xüsusi tələblər olmasa, həmin məlumatlar etibarlı şəkildə silinməlidir.
    5. Test prosesində iştirak edən şəxslər məlumatların məxfiliyinə riayət etməli və məlumatlardan yalnız səlahiyyətli məqsədlər üçün istifadə etməlidirlər.

# XARİCİ TƏRƏFLƏRLƏ ƏLAQƏLƏR

## Xarici Tərəflərlə Əlaqədə İnformasiya Təhlükəsizliyi

* + 1. Qurumun informasiya resurslarına xarici tərəflərin çıxışı yalnız əvvəlcədən təsdiqlənmiş, hüquqi və texniki əsasları təmin edən müqavilələr əsasında həyata keçirilməlidir.
    2. Xarici tərəflərə məxfi məlumatlara giriş imkanı verilməzdən öncə, onlar məxfi məlumatların qorunması üzrə öhdəliklərini rəsmiləşdirən razılaşma sənədini imzalamalıdırlar. Bu razılaşma qurumun məxfi məlumatlarının icazəsiz istifadə edilməsinə və ya açıqlanmasına görə məsuliyyət tədbirlərini əhatə etməlidir.
    3. Xarici tərəflərlə əməkdaşlıq zamanı məlumatların ötürülməsi və işlənməsi prosesində baş verə biləcək təhlükəsizlik riskləri müəyyən edilməli və onların qarşısını almaq üçün xüsusi nəzarət mexanizmləri tətbiq olunmalıdır.
    4. Xarici tərəflərlə müqavilələrdə informasiya təhlükəsizliyi ilə bağlı tələblər, o cümlədən məlumatların məxfiliyi, bütövlüyü və mövcudluğu prinsiplərinə uyğunluq təmin edilməli, bu tələblər tədarük zəncirinin bütün mərhələlərinə tətbiq edilməlidir.
    5. Hər hansı təhlükəsizlik tələblərinin pozulması aşkar edildikdə, qurum rəhbərliyinin razılığı ilə pozuntu hallarını aradan qaldırmaq üçün həmin tərəfin çıxış hüquqları dayandırılmalı və fəaliyyətlər müvəqqəti olaraq saxlanılmalıdır.

## Xarici Tərəf Xidmətlərinin İdarə Edilməsi

* + 1. Xarici tərəflər tərəfindən təqdim olunan xidmətlərin təhlükəsizliyi təmin edilməli və bu xidmətlərin icrası zamanı həyata keçirilən əməliyyatlar mütəmadi olaraq monitorinq edilməli, qeydə alınmalı və nəzərdən keçirilməlidir.
    2. Xarici tərəflərin təqdim etdiyi xidmətlərdə edilən dəyişikliklər qurumun informasiya təhlükəsizliyi siyasətinə uyğun şəkildə idarə olunmalı və bu dəyişikliklərə başlamazdan əvvəl risklər, biznes proseslərinin təsiri və təhlükəsizlik aspektləri qiymətləndirilməlidir.
    3. Xarici xidmət təminatçıları ilə bağlanmış razılaşmalarda təhlükəsizlik tələbləri, xidmət səviyyəsi və performans göstəriciləri dəqiq şəkildə müəyyən edilməli, bu göstəricilərin yerinə yetirilməsi davamlı olaraq izlənilməlidir.
    4. Xarici tərəflərin xidmətlərində baş verə biləcək təhlükəsizlik insidentləri dərhal aşkar edilməli, bu insidentlərin təsirlərini minimuma endirmək üçün operativ tədbirlər görülməli və gələcəkdə təkrarlanmaması üçün təkmilləşdirmə işləri aparılmalıdır.

# İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİNİN İDARƏ EDİLMƏSİ

## İnformasiya Təhlükəsizliyi İnsidentlərinin İdarə Edilməsi Və Təkmilləşdirilməsi

* + 1. İnformasiya təhlükəsizliyi insidentlərinin vaxtında aşkarlanması, araşdırılması və həll edilməsi üçün standart prosedurlar hazırlanmalı, təsdiqlənməli və tətbiq edilməlidir.
    2. İnsidentlərin aşkarlanması və bildirilməsi üçün əməkdaşlar arasında məlumatlılıq artırılmalı və insidentlərin bildirilə biləcəyi mərkəzləşdirilmiş mexanizm yaradılmalıdır.
    3. Hər bir insident üçün prioritetlər müəyyən edilməli və təsir dərəcəsindən asılı olaraq uyğun təcili cavab tədbirləri görülməlidir.
    4. İnsidentlər zamanı toplanan məlumatlar analiz edilməli və onların kök səbəbləri müəyyən olunaraq gələcəkdə bu cür halların qarşısını almaq üçün qabaqlayıcı tədbirlər həyata keçirilməlidir.
    5. İnsidentlərin təkrar baş verməməsini təmin etmək üçün korrektiv tədbirlər sənədləşdirilməli, izlənilməli və müvafiq təhlükəsizlik prosedurlarında yeniliklər tətbiq edilməlidir.
    6. İnsidentlərin idarə edilməsi prosesi çərçivəsində hər bir insidentlə bağlı təfərrüatlar, təhlil və həyata keçirilmiş tədbirlər barədə hesabat hazırlanmalı və rəhbərliyə təqdim edilməlidir.
    7. Təhlükəsizlik insidentləri zamanı müvafiq hüquqi və tənzimləyici tələblərə uyğunluq təmin edilməli və zərurət yarandıqda aidiyyəti orqanlara məlumat verilməlidir.
    8. İnsidentlərin idarə edilməsi təcrübələri davamlı olaraq nəzərdən keçirilməli və yeni təhlükələrə uyğun şəkildə təkmilləşdirilməlidir.

# FƏALİYYƏT DAVAMLILIĞININ İDARƏ EDİLMƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

## İnformasiya Təhlükəsizliyinin Davamlılığının Təmin Edilməsi

* + 1. Qurumun biznes-proseslərinin və İT xidmətlərinin fövqəladə hallar və qəza vəziyyətlərində bərpasını təmin etmək məqsədilə xüsusi tədbirlər hazırlanmalı və fəaliyyət davamlılığı planında əks etdirilməlidir.
    2. Fasiləsiz fəaliyyətin təmin olunması və əlaqələndirilməsi İT şöbəsinin səlahiyyətində olmalıdır. Məlumat sistemlərinin bərpası isə müəyyən olunmuş müddət çərçivəsində qurumun İT rəhbəri tərəfindən təmin edilməlidir.
    3. Proseslərin dayanıqlığını qorumaq üçün təhlükələrin və risklərin qiymətləndirilməsinə əsaslanan idarəetmə strategiyaları planlaşdırılmalı və sənədləşdirilməlidir.
    4. Fəaliyyət davamlılığı planının dəstəklənməsi üçün zəruri prosedurlar, o cümlədən işçi heyətinin yerləşdirilməsi, sistemlərin bərpası və digər mühüm addımlar üçün əlavə sənədlər hazırlanmalıdır.
    5. Fövqəladə hallar zamanı fəaliyyət planının vaxtında icrasını təmin etmək üçün operativ iş mexanizmləri yaradılmalı və tətbiq edilməlidir.
    6. Fəaliyyət davamlılığı planı mütəmadi olaraq yenilənməli və təsdiqlənməlidir. Hər il bu planın test olunması üçün prosedurlar həyata keçirilməli, nəticələr təhlil olunmalı və təkmilləşdirilməlidir.
    7. Planın icrası zamanı ortaya çıxan hər hansı uyğunsuzluqların aradan qaldırılması üçün nəticələrə əsaslanaraq düzəlişlər edilməlidir.
    8. Ən mühüm əməliyyatların ehtiyat mərkəzdə bərpasını təmin etmək məqsədilə hər iki ildən bir tam miqyaslı sınaqlar həyata keçirilməlidir.
    9. Qurum məlumat sistemlərinin fasiləsiz işləməsi üçün texniki və inzibati tədbirləri mütəmadi olaraq tətbiq etməlidir.

# UYĞUNLUQ

## Qanun Və Müqavilə Tələblərinə Uyğunluq

* + 1. Qurumun informasiya təhlükəsizliyi ilə bağlı fəaliyyətləri yerli qanunvericilik aktları, beynəlxalq standartlar, müqavilə öhdəlikləri və digər tənzimləyici tələblərə uyğun həyata keçirilməlidir.
    2. Qanunvericiliyə və müqavilə tələblərinə uyğunluğun təmin edilməsi məqsədilə hüquqi tələblər və qurumun fəaliyyətinə təsir edə biləcək müqavilə öhdəlikləri müəyyənləşdirilməli və mütəmadi olaraq yenilənməlidir.
    3. Qurum tərəfindən istifadə edilən bütün informasiya resurslarının qanuni əsaslarla əldə olunması və istifadəsi təmin edilməli, müəllif hüquqları və lisenziyalaşdırma şərtləri pozulmamalıdır.
    4. Müqavilə tərəfləri ilə bağlanan bütün razılaşmalarda informasiya təhlükəsizliyinin qorunmasına dair konkret müddəalar əks etdirilməlidir.
    5. İnformasiya təhlükəsizliyi üzrə qanunvericiliyə, müqavilə öhdəliklərinə və standartlara əməl olunmaması hallarında nəticələrin minimuma endirilməsi və uyğunluğun bərpası üçün xüsusi prosedurlar hazırlanmalı və tətbiq edilməlidir.
    6. Qanun və müqavilə tələblərinə uyğunluğun yoxlanılması üçün dövri auditlər və müvafiq yoxlama tədbirləri həyata keçirilməlidir.

## İnformasiya Təhlükəsizliyi Rəyləri

* + 1. Qurum, informasiya təhlükəsizliyinin idarə edilməsi yanaşmasının, o cümlədən tətbiq olunan nəzarət məqsədlərinin, vasitələrinin, proseslərin və müvafiq sənədlərin müstəqil qiymətləndirilməsini həyata keçirməlidir. Bu qiymətləndirmələr planlaşdırılmış dövrlərdə və ya əhəmiyyətli dəyişikliklər baş verdikdə icra edilməlidir.
    2. İnformasiya sistemlərinin qurumun informasiya təhlükəsizliyi siyasəti və standartlarına uyğunluğu müntəzəm olaraq qiymətləndirilməlidir. Bu, sistemlərin təhlükəsizlik tələblərinə cavab verməsini təmin etmək üçün vacibdir.

# 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.

# İNTİZAM TƏDBİRLƏRİ

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

# ƏLAQƏLİ SƏNƏDLƏR

* ISO 27001:2022 Standartı

# TƏSDİQETMƏ

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

[vəzifə məlumatları]

[adı soyadı və ata adı]

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

[İmza] [Tarix]