“Təsdiq edilmişdir”

Azərbaycan Respublikasının
Milli Depozit Mərkəzinin
Müşahidə Şurasının

14 avqust 2017**-ci il tarixli qərarı**

(14 **№-li protokol)**

Sədr _____ B.Əzizov

İnformasiya təhlükəsizliyinə dair
Azərbaycan Respublikasının Milli Depozit Mərkəzinin daxili Qaydaları

1. Ümumi müddəalar

1.1. Bu Qaydalar «Qiymətli kağızlar bazarı haqqında» Azərbaycan Respublikasının Qanuna, «İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında» Azərbaycan Respublikasının Qanuna və digər Azərbaycan Respublikasının qüvvədə olan informasiya təhlükəsizliyinin təmin edilməsi üzrə tədbirlər haqqında normativ hüquqi aktlarına uyğun olaraq hazırlanmışdır.

1.2. Bu Qaydalar Azərbaycan Respublikasının Milli Depozit Mərkəzində (bundan sonra - MDM) informasiya sistemlərinin təhlükəsizliyinə dair minimal tələbləri müəyyən edir.

1.3. MDM-in əməkdaşları və informasiya resurslarına daxilolma hüquqlarına malik olan bütün şəxslər məlumatların təhlükəsizliyinin təmin olunması məqsədi ilə bu qaydalara riayət etməlidir.

1.4. Bu Qaydaların tələbləri MDM-in bütün təşkilati strukturunu və biznes prosesləri əhatə edir. Qaydaların tələbləri MDM-in bütün rəhbər işçilərinə və əməkdaşlarına, biznes proseslərinin iştirakçısı olan əlaqəli tərəflərə, habelə prosesin təşkilatdankənar iştirakçılarına da şamil edilir.

2. Anlayışlar

2.1. **İnformasiya sistemləri** – informasiya texnologiyaları və sənədlərinin təşkilati və texniki qaydada, o cümlədən hesablama texnikasından istifadə edilməklə, nizamlanmış məcmusudur.

2.2. **İT infrastruktur** – server, kompüter və şəbəkə avadanlıqları və onların əməliyyat sistemləri, kommunikasiya xətləri, idarəetmə sistemlərinin məcmusudur.

2.3. **İT resurslar** – İnformasiya sistemləri və İT infrastrukturun məcmusudur.

2.4. **Elektron sənədlər** –informasiya sistemlərində rəqəmsal saxlanılan informasiyadır

2.5. **Kompüter avadanlığı** – daxili şəbəkəyə qoşulmuş stasionar və ya daşınan qurğulardır.

2.6. **Sistem inzibatçısı** – informasiya sistemlərində dəyişiklikləri tətbiq edən, sistemlərin ehtiyat surətlərinin yaradılması və sistemin fəaliyyətinin monitorinqini, habelə səlahiyyət bölgüsünə əsasən informasiya sistemi üzrə digər funksiyaları həyata keçirən əməkdaşdır.

2.7. **Təhlükəsizlik inzibatçısı** – informasiya sistemlərinin mühafizəsinə və məlumatlara sanksiya edilməmiş müdaxilələrə nəzarət edən və informasiya texnologiyalarının tətbiqinə cavabdeh olan struktur bölməyə tabeçiliyi olmayan əməkdaşdır.

2.8. **İnformasiyanın bütövlüyü** – İnformasiyanın icazəsiz dəyişilməməsinin və tamlığının qorunmasıdır.

2.9. **İstifadəçi** – İT resurslara giriş səlahiyyəti verilmiş şəxsdir.

2.10. **İstifadəçi adı**- istifadəçilərə verilmiş unikal təyinedicidir.

2.11. **Parol** – İT resurlara giriş üçün istifadə olunan, istifadəçilərin yalnız özlərinin bildiyi simvollar toplusudur.

2.12. **İdentifikasiya**− sistemin müəyyən komponentlərinin tanınması prosesi; unikal, sistem tərəfindən qavranılan identifikatorların (adların) köməyi ilə aparılır və identifikasiya istifadəçiyə (və ya istifadəçinin adından fəaliyyət göstərən prosesə) öz adını sistemə bildirməyə imkan verir.

2.13. **Autentifikasiya**– paroldan istifadə edilməklə istifadəçinin identifikasiyaya uyğunluğunun yoxlanılmasıdır.

2.14. **İstifadəçi sessiyası** – autentifikasiya prosesindən sonra müvafiq İT resurslardan istifadə etmək üçün işlədilən, öz adından əməliyyatlar edə bilən əməliyyat sistemi, proqram təminatı interfeysi və ya rəqəmsal əlaqədir.

2.15. **İmtiyazlı giriş hüquqları**– informasiya sistemlərində idarəetmə hüquqlarıdır.

2.16. **Zərərli proqram** – İT resurslarda çoxalmağa cəhd edən, İT resurslara, elektron sənədlərə, fayllara ziyan vuran, konfidensial məlumatların əldə edilməsinə, məlumatların korlanmasına (dəyişdirilməsinə, silinməsinə) səbəb olan və istifadəçilərin işinə mane olan və sistemə adətən gizli daxil edilən hər hansı proqram təminatıdır.

2.17. **Antivirus mühafizəsi** – zərərli proqramların aşkar və məhv edilməsinə yönəldilmiş tədbirlər kompleksi və proqramdır.

3. Qaydaların məqsədi

3.1. İnformasiya təhlükəsizliyinin təmin olunması sahəsində tarazlaşdırılmış kompleks təşkilati və texniki tədbirlərə əsaslanan informasiya təhlükəsizliyinin idarə olunması üzrə səmərəli sistemin yaradılması, dəstəklənməsi, ona nəzarət edilməsi və bu sistemin inkişaf etdirilməsi.

3.2. İnformasiya sahəsində MDM-in, onun kontragentlərinin, habelə əməkdaşlarının mənafeyinin hərtərəfli qorunmasının təmin edilməsi

3.3. MDM daxilində istifadə olunan informasiyaların bütövlüyünün təmin edilməsi ilə bağlı konkret vəzifələrin bölüşdürülməsi.

3.4. İnformasiyanın məhvi, modifikasiyası, surətinin çıxarılması, təcrid edilməsi ilə bağlı sanksiyalaşdırılmamış hərəkətlərin qarşısının alınması.

3.5. Daxili şəbəkənin hər bir xidmət sahəsinin təhlükəsizliyinin təmin edilməsi.

3.6. Bütün sistemin fövqəladə hallarda fasiləsiz fəaliyyətini təmin edən planın hazırlanması.

3.7. İnformasiya təhlükəsizliyi kompleks zəruri proseslərin və tədbirlərin həyata keçirilməsi, həmçinin hər bir əməkdaşın informasiya təhlükəsizliyinin təmin olunmasına dair daxili rəsmləşmələrin tələbləri səviyyəsində yerinə yetirilməsi ilə müəyyən edilmiş zəruri köməyi sayəsində təmin olunur.

4. İnformasiyanın təsnifatlaşdırılması

4.1. MDM-də yaradılan, dövriyyədə olan, ötürülən və yaxud saxlanılan bütün informasiyaya sahiblik hüququ MDM-ə məxsusdur.

4.2. MDM ona məxsus informasiyanın təhlükəsizliyi onların təsnifat dərəcələrinə uyğun olaraq qanunvericilikdə müəyyən edilmiş qaydada təmin edilməlidir.

4.3. MDM-in biznes struktur bölmələrinin fəaliyyət istiqamətlərinə görə onlar tərəfindən istifadə olunan informasiyalar müəyyən edilir.

4.4. İnformasiyalar həssaslıq dərəcələrinə görə aşağıdakı siniflər üzrə təsnifatlaşdırılır:

4.4.1. Açıq informasiya – əldə olunması, işlənməsi, verilməsi və ya istifadəsi qanunvericiliklə məhdudlaşdırılmayan və ümumi istifadə üçün təyin olunmuş informasiyadır;

4.4.2. Xidməti informasiya – daxili iş proseslərində yaranan və MDM daxilində xidməti istifadə üçün nəzərdə tutulan informasiyadır;

4.4.3. Konfidensial informasiya – əldə olunması, işlənməsi, verilməsi və ya istifadəsinə qanunla məhdudiyyət qoyulan, həmçinin kommersiya sirrini təşkil edən informasiyadır.

4.5. MDM-ə məxsus informasiyaların təsnifatlaşdırılması nəticəsində struktur bölmələr üzrə hazırlanmış informasiyaların müvafiq həssaslıq sinfi üzrə bölünməsinin siyahısı MDM rəhbərliyi tərəfindən təsdiq edilir.

4.6. MDM-də informasiyanın təsnifatlaşdırılması və onlara sahiblik müvafiq struktur bölmənin rəhbəri tərəfindən müəyyən edilir və rəhbərlik tərəfindən təsdiq edilir.

4.7. MDM-ə məxsus bütün informasiyalar müvafiq həssaslıq sinfinin nişanları ilə nişanlanır.

4.8. Əgər MDM-ə məxsus informasiyasını əldə edən şəxs informasiyanın təsnifat nişanının düzgün olmadığını hesab edirsə, bu halda informasiya mümkün siniflərdən daha yuxarı qorunma səviyyəsinə aid edilməli və Təhlükəsizlik departamentinə (bundan sonra - TD) bu barədə məlumat verilməlidir.

4.9. MDM-də kənar təşkilatlardan daxil olan informasiyanı qəbul edən şəxs və ya sistem informasiyanı MDM-in informasiya təsnifat sinfinə uyğun olaraq nişanlamalıdır.

4.10. İnformasiya sistemlərinin istifadəçiləri yaratdıqları hər bir elektron sənədə və ya kağız daşıyıcıya informasiyanın müvafiq təsnifat nişanını verməlidirlər.

4.11. Bütün informasiyaların saxlandığı avadanlıq, qurğu və daşıyıcıların üzərində müvafiq həssaslıq sinfinə uyğun olan nişanlar qoyulmalıdır.

4.12. Həssas informasiya çap edilmiş və ya əllə yazılmış kağız daşıyıcılarının üzərində müvafiq həssaslıq sinfinin nişanı qoyulmalıdır.

4.13. Həssas informasiyanı özündə saxlayan tikilmiş sənədlərin üz qabığında, titul səhifəsində və arxa qabığında müvafiq həssaslıq sinfinin nişanı qoyulmalıdır.

4.14. Bütün məlumatlar onların həssaslıq dərəcəsindən asılı olaraq qorunmalı və saxlanılmalıdır.

4.15. MDM-ə məxsus İnformasiyadan istifadə hüquqları MDM rəhbərliyi tərəfindən təsdiq edilmiş səlahiyyət bölgüsünə müvafiq aparılır.

4.16. Bu uyğunluğa riayət olunmasına TD tərəfindən nəzarət olunur.

5. MDM əməkdaşlarının informasiya təhlükəsizliyi üzrə məlumatlandırılması

5.1. İşə qəbul zamanı təhlükəsizlik üzrə müvafiq struktur bölmə tərəfindən əməkdaşların məlumatların qorunması və informasiya təhlükəsizliyinin təmin olunması məqsədi ilə aşağıdakı istiqamətlərdə məlumatlandırılması təmin olunmalıdır:

5.1.1. İT resurslara giriş hüquqları haqqında;

5.1.2. Hər bir əməkdaşın məxsusi istifadəçi adından aparılan bütün əməliyyatlara görə fərdi məsuliyyət daşıması haqqında;

5.1.3. Parolların və digər identifikasiya və ya autentifikasiya vasitələrindən istifadə edilməsi və onların məxfiliyinin saxlanılması haqqında;

5.1.4. Elektron və kağız daşıyıcılarda olan konfidensial məlumatlardan ibarət sənədlərin kənar şəxslər üçün əlçatmaz olan yerdə saxlanması haqqında.

5.2. İnformasiya təhlükəsizliyinə dair bütün məsələlərlə bağlı ardıcıl olaraq TD-yə məlumat verilməlidir.

6. MDM əməkdaşlarının informasiya təhlükəsizliyi üzrə məsuliyyəti

6.1. MDM-in əməkdaşları göstərilən müvafiq informasiya təhlükəsizliyi sahələrinə görə məsuliyyət dərəcələri aşağıdakı qaydada müəyyənləşdirilir:

6.1.1. MDM-in struktur bölmə rəhbərləri informasiya təhlükəsizliyi siyasəti ilə bütün işçi və istifadəçilərin tanış edilməsi və nəzarət edilməsi üzrə;

6.1.2. Sistem inzibatçıları sistemin fasiləsiz fəaliyyətinin informasiya təhlükəsizliyi siyasətinə uyğun (olmaqla) təşkil edilməsi üzrə;

6.1.3. İstifadəçilər daxili şəbəkədə və fərdi kompüterlərin işlənməsində təhlükəsizlik qaydalarının, rəhbərliyin və informasiya təhlükəsizliyi işçilərinin tələblərinə riayət edilməsi üzrə.

6.2. Əməkdaşlar sənədləri stol üstündə nəzarətsiz qoymamalı və onları bağlı saxladırlar.

6.3. Fərdi kompüterlər nəzarətsiz qalmamalı, otaqdan çıxanda onun ekranı bağlanmalı, istifadəçi sessiyasından çıxmalı və ya kilitə salınmalıdır.

6.4. Məlumatlar mütəmadi olaraq fərdi kompüterlərdən fayl serverində müvafiq ayrılmış qovluqlarda saxlanmalıdır.

6.5. Zərərli proqramlardan (viruslardan) şübhə olduğu təqdirdə icazəsiz heç bir iş görməməli və TD-nin əməkdaşına müraciət edilməlidir.

6.6. Elektron məktubların əlavələri ilə ehtiyatlı rəftar etmək, əgər onların tərkibi şübhəlidirsə onları açmadan TD-yə xəbər vermək lazımdır.

6.7. İnternetdən MDM-in sisteminə və fərdi kompüterlərə lazımsız məlumatlar yüklənməməlidir.

6.8. MDM-in elektron xidmətlərindən şəxsi məqsədlər üçün istifadə edilməməlidir.

7. İT resurslara daxil olma hüquqlarının idarə olunması

7.1. İT resurslarına daxil olma hüquqlarının verilməsi üçün aşağıdakı vahid qayda tətbiq edilir:

7.1.1. Əməkdaşın birbaşa rəhbəri lazımi strukturlardan icazə almaq üçün doldurulmuş "İT resurslarında hüquqların verilməsi forması"nı təqdim edir (Əlavə №1);

7.1.2. "İT resurslarında hüquqların verilməsi forması" MDM rəhbərliyi və təhükəsizlik üzrə məsul bölmənin rəhbəri tərəfindən təsdiq edildikdən sonra ərizə sistem inzibatçılarına təqdim edilməlidir.

7.2. Hər bir istifadəçi üçün "İT resurslarında hüquqların verilməsi forması"nın mövcud olmasına təhükəsizlik üzrə struktur bölmənin rəhbəri nəzarət edir.

7.3. İstifadəçiyə İT resurslarda imtiyazlı giriş hüquqları informasiya təhlükəsizliyi və təhlükəsizlik üzrə müvafiq struktur bölmənin rəhbərləri ilə razılaşdırmaqla MDM-in rəhbərliyinin razılığı ilə verilə bilər.

7.4. İnzibatçı tərəfindən "İT resurslarında hüquqların verilməsi forması"ndakı məlumatlar əsasında əməkdaşa istifadəçi adı və birdəfəlik şifrə verilir.

7.5. MDM-in əməkdaşı bölmələr arasında köçürüldüyü və ya funksional vəzifələr dəyişdiyi zaman əməkdaşın yeni rəhbəri tərəfindən "İT Resurslarında hüquqların verilməsi forması" hazırlanmalıdır.

7.6. Daxil olma hüquqları "İT resurslarında hüquqların verilməsi forması" əməkdaş işdən azad edildiyi halda və ya hər hansısa şübhəli məqam əsasında geri götürülə bilər.

7.7. Məlumatların təhlükəsizliyi vəziyyətinin müntəzəm yoxlanılması çərçivəsində informasiyanın təhlükəsizliyi üzrə müvafiq struktur bölmə daxil olma hüquqlarının geri alınmasına müntəzəm nəzarət etməlidir.

7.8. Əməkdaş işdən azad edildiyi halda onun birbaşa rəhbəri istifadəçi hüquqlarının geri alınmasını təmin etməlidir.

7.9. TD-nin əməkdaşları uçot yazıları və İT resurslara giriş hüquqlarını vaxtaşırı yoxlamalı və yenidən nəzərdən keçirilməlidir.

7.10. İT resurslarına günün vaxtından asılı olaraq qoşulmanın məhdudlaşdırılması nəzərdə tutulmalıdır.

7.11. MDM əməkdaşları qeyri iş saatlarında İT resurslara daxil olmaq üçün "Qeyri-iş saatlarıda istifadəçilərin İT resurslarına qoşulmasına icazə forması"nı doldurmalıdır (Əlavə №2).

7.12. İstifadəçilərin və sistem inzibatçılarının sistemdə uçotunun yaradılması, dəyişdirilməsi və ləğv edilməsi, habelə onların informasiya sistemlərinə daxilolma qaydalarını müəyyən edən prosedurlar mövcud olmalıdır.

7.13. İnformasiya sistemlərində istifadəçilərin yaradılması sistem inzibatçısı tərəfindən, səlahiyyətlərin təyin edilməsi, dəyişdirilməsi və istifadəçilərin fəaliyyətinin dayandırılması isə təhlükəsizlik inzibatçısının nəzarəti ilə həyata keçirilməlidir.

8. İT resurslarda istifadəçi adı və parollardan istifadə

8.1. İstifadəçi adı və parol hər bir əməkdaş üçün şəxsidir.

8.2. İstifadəçilər parolları açıq şəkildə yazmamalı, sistem inzibatçıları parolları proqramların ilkin mətnlərində, paket fayllarında (batch files, scripts) saxlamamalı və yazmamalıdır.

8.3. İT resursların inzibatçılarının, ödəniş sistemlərinin istifadəçi adı, parolları və identifikasiya qurğuları möhürlənmiş zərflərdə yerləşdirilməklə TD-də seyflərdə saxlanılmalıdır.

8.4. İstifadəçi adı, parolları və identifikasiya qurğuları qəbul və ya təhvil verilən zaman TD tərəfindən xüsusi jurnallarda qeydiyyat aparılmalıdır.

8.5. Zərfin açılması MDM-in rəhbərliyinin icazəsi ilə işçinin birbaşa rəhbərinin və TD-nin rəhbərinin iştirakı ilə həyata keçirilməlidir.

9. İnformasiya təhlükəsizliyi sisteminin idarə olunması

9.1. İnformasiya təhlükəsizliyinin idarə olunması sistemi MDM-in ümumi korporativ idarəetmə sisteminin ayrılmaz tərkib hissəsidir.

9.2. İdarəetmə sisteminin məqsədi informasiya təhlükəsizliyinin təmin olunması üzrə proseslərin, təşkilati və texniki tədbirlərin müəyyənləşdirilməsi, planlaşdırılması, tətbiqi, fəaliyyəti, monitorinqi, nəticələrin və səmərəliyin qiymətləndirilməsi, həmin proseslərin və tədbirlərin dəstəklənməsi və təkmilləşdirilməsi yolu ilə MDM-in informasiya təhlükəsizliyi siyasətinin və ona dəstək sənədlərin tam və səmərəli surətdə həyata keçirilməsidir.

9.3. İnformasiya təhlükəsizliyinin idarəetmə sisteminin vəzifələrinə aşağıdakılar daxildir:

9.3.1. Beynəlxalq standartların və ən yaxşı təcrübələrin tövsiyələrini nəzərə alaraq İT risklərinin idarə olunmasına vahid yanaşmanın tətbiq edilməsi;

9.3.2. İnformasiya təhlükəsizliyinin təmin olunması proseslərinin səmərəli idarə edilməsi və təkmilləşdirilməsi;

9.3.3. İnformasiya təhlükəsizliyinin təmin olunmasına dair sənədlər sisteminin yaradılması və dəstəklənməsi;

9.3.4. MDM rəhbərliyi üçün informasiya təhlükəsizliyinin idarə olunması prosesinin şəffaflığının təmin edilməsi;

9.3.5. İnformasiya təhlükəsizliyinin təmin olunması üzrə proseslərin və tədbirlərin nəticəliliyinin və səmərəliliyinin qiymətləndirilməsi və onların təkmilləşdirilməsinə və inkişaf etdirilməsinə dair rəhbərlik tərəfindən qərarlar qəbul edilməsi üçün meyarların hazırlanması;

9.3.6. Təhlükəsizlik hadisəsi baş verdikdə informasiya sistemlərinin fasiləsiz fəaliyyətinin təmin edilməsi.

9.4. İnformasiya təhlükəsizliyinin təmin olunması sahəsində MDM-in bütün təşkilati strukturu üzrə aşağıdakı qaydada funksiya və məsuliyyətin bölüşdürülməsi həyata keçirilir:

9.4.1. MDM-in rəhbərliyi:

- informasiya təhlükəsizliyi sahəsində strateji məqsəd və vəzifələri müəyyən edir, informasiya təhlükəsizliyinə dair əsas sənədləri təsdiq edir;
- informasiya təhlükəsizliyinin təmin olunması sahəsində struktur bölmələrin və əməkdaşlarının əsas funksiyaları və məsuliyyətini müəyyənləşdirir;

- informasiya təhlükəsizliyi sahəsində risklərin qiymətləndirilməsi nəticələrini, bu risklərin azaldılmasına yönəldilmiş proseslərin və tədbirlərin tətbiqi planlarını, o cümlədən həmin planların həyata keçirilməsinə ayrılan resursların həcmini təsdiq edir;
- informasiya təhlükəsizliyinin təmin olunmasına resurs ayrılması barədə qərar qəbul edir və ondan səmərəli istifadə olunmasına nəzarət edir;
- informasiya təhlükəsizliyinin xarici auditinin keçirilməsi haqqında qərar qəbul edir.

9.4.2. Təhlükəsizlik departamenti:

- MDM-in informasiya sahəsində təhlükəsizliyinin təmin olunmasına yönəldilmiş fəaliyyəti həyata keçirir;
- İnformasiya sahəsində risklərin idarə olunması prosesi üzrə informasiya təhlükəsizliyi ilə əlaqədar işlərdə iştirak edir;
- İnformasiya təhlükəsizliyini idarəetmə sistemi proseslərinin və informasiya təhlükəsizliyinin təmin olunması üzrə risklərə cavab verilməsinə yönəldilmiş kompleks təşkilati və texniki tədbirlərin planlaşdırılması, habelə planlaşdırılan tədbirlərin MDM-in rəhbərliyi səviyyəsində razılaşdırılmasın; təmin edir;
- Biznes proseslərin fasiləsizliyinin idarə olunması işlərində iştirak edir;
- İnformasiya təhlükəsizliyinin təmin olunması proseslərinə və tədbirlərinə yenidən baxılması, onların təkmilləşdirilməsinə və inkişaf etdirilməsinə dair təkliflərin və planların, informasiya təhlükəsizliyinə dair sənədlərin işlənib hazırlanmasını təmin edir;
- İnformasiya təhlükəsizliyinin təmin olunması mexanizmlərinin və vasitələrinin seçilməsi, tətbiq edilməsi və müşayiət olunması, habelə mühafizə mexanizmlərinin və vasitələrinin tətbiqi və müşayiəti zamanı qarşılıqlı fəaliyyəti və nəzarəti təmin edir;
- İnformasiya təhlükəsizliyi hadisələrinin monitorinqi üzrə işlərə rəhbərlik və bu işlərin əlaqələndirilməsini təmin edir;
- İnformasiya təhlükəsizliyinin təmin olunması proseslərinin və tədbirlərinin nəticəliliyi və səmərililiyi meyarlarını işləyib hazırlayır;
- İnformasiya təhlükəsizliyinin təmin olunması proseslərinin və tədbirlərinin müntəzəm monitorinqinin keçirilməsi, onların yerinə yetirilməsi tamlığının və keyfiyyətinin, mövcud sənədlərin tələblərinə uyğunluğunun qiymətləndirilməsi,

informasiya resurslarının və biznes proseslərinin informasiya təhlükəsizliyi üçün təhlükələrdən qorunması vəziyyətini qiymətləndirir;

- İnzibati İşlər Departamenti ilə birlikdə əməkdaşların informasiya təhlükəsizliyi məsələlərinə dair tədris proqramlarının planlaşdırılması, hazırlanması və həyata keçirilməsi, təlimatlandırma və treyninqlərin keçirilməsi, əməkdaşların bu sahədə biliklərinə nəzarət edilməsi işlərini həyata keçirir.

9.4.3. İnfromasiya texnologiyaları infrastrukturu departamenti (İTİD) və İnformasiya sistemləri və xüsusi proqram təminatı departamenti (İSXPTD):

- Təhlükəsizlik departamentinə həvalə edilmiş informasiya təhlükəsizliyinin təmin olunması mexanizmləri və vasitələri istisna olmaqla MDM-in bütün informasiya infrastrukturunun dəstəklənməsini, istismarını və inkişafını təmin edir;
- informasiya sahəsində risklərin idarə olunması, habelə informasiya texnologiyaları xidmətlərinin bərpa edilməsi və biznes proseslərin fasiləsizliyinin təmin olunması prosesində iştirak edır;
- İnformasiya sahəsində risklərinin idarə olunması üzrə informasiya texnologiyaları üçün təhlükələrlə və digər pozuntularla əlaqədar işlərə yardım edir;
- İnformasiya təhlükəsizliyinin təmin olunması üzrə Təhlükəsizlik departamenti tərəfindən planlaşdırılan proseslərin və tədbirlərin informasiya texnologiyaları xidmətlərinə təsirinin qiymətləndirilməsini, bu proseslərin və tədbirlərin tətbiqinə razılaşdırılmış yanaşmanın təmin edilməsini həyata keçirir;
- MDM-in informasiya texnologiyaları xidmətlərinin bərpası işlərinə yardım edir;
- İnformasiya təhlükəsizliyi tələblərinə uyğun olaraq informasiya sistemlərin alınmasının planlaşdırılması, tətbiqi, istismarı, dəstəklənməsi və monitorinqi proseslərində iştirak edir;
- İnformasiya sistemlərində dəyişikliklərin edilməsi qaydasına uyğun olaraq, yeni yaradılan yaxud mövcud proqram təminatlarında dəyişikliklər zamanı proqram təminatının yeləşdiyi və tətbiq edildiyi avadanlıqlarla uyğunluğunun yoxlanmasını təmin edir;
- Münaqişələrin idarə olunması üzrə bütün proseslərdə - identifikasiya, cavabvermə, araşdırma, nəticələrin və səbəblərin aradan qaldırılması proseslərində İnformasiya təhlükəsizliyi departamentinə yardım edir;

- İnformasiya təhlükəsizliyi üzrə tələblərə uyğunluğun qiymətləndirilməsi, informasiya resurslarının qorunması vəziyyətinin qiymətləndirilməsi və daxili auditlərin keçirilməsi zamanı İnformasiya təhlükəsizliyi departamentinə və daxili audit əməkdaşlarına yardım göstərir.

9.4.4. Daxili auditor:

- marağı olan bütün tərəflərə və ilk növbədə MDM-in rəhbərliyinə informasiya təhlükəsizliyinin təmin olunması üzrə həyata keçirilən proseslərin və tədbirlərin informasiya təhlükəsizliyinə dair sənədlərdə əks etdirilmiş tələblərə uyğunluğunun düzgün, obyektiv və müstəqil qiymətini verir;
- informasiya təhlükəsizliyi proseslərinin öz üstünlüklərinə müvafiq surətdə planlaşdırılması və onların daxili auditlərinin keçirilməsi, proseslərin və tədbirlərin sənədləşdirilmiş tələblərə uyğunluğunun qiymətləndirilməsini təmin edir.

9.4.5. Hüquq departamenti:

- Azərbaycan Respublikası qanunvericiliyinin normalarına uyğunluq baxımından informasiya təhlükəsizliyinə dair bütün daxili sənədlərə baxılmasını təmin edir;
- İnformasiya təhlükəsizliyi münaqişələrinin araşdırılması zamanı İnformasiya təhlükəsizliyi departamentinə hüquqi yardımın göstərilməsini təmin edir;
- İnformasiya təhlükəsizliyinə aid ola bilən qanunvericilik aktlarının öyrənilməsi və İnformasiya təhlükəsizliyi departamentinə informasiya təhlükəsizliyinin təmin olunması ilə əlaqədar qanunvericilik normaları barədə məlumat verir.

9.4.6. Biznes struktur bölmə rəhbərləri:

- biznes proseslərin və informasiya resurslarının əhəmiyyətinin obyektiv qiymətləndirilməsi yolu ilə onların qiymətləndirilməsində və təsnifləşdirilməsində iştirak edir;
- informasiya resurslarının məxfiliyi, tamlığı və ya onlara giriş qaydası üzrə tələbləri, habelə biznes prosesləri və informasiya resursları barəsində informasiya təhlükəsizliyi üzrə digər tələblərin müəyyənləşdirilməsində iştirak edir;

- əməkdaşların informasiya resurslarına giriş hüquqlarının müəyyənləşdirilməsi və bu hüquqlara müntəzəm surətdə yenidən baxılması, giriş hüququnun və müvafiq səlahiyyətlərin verilməsi barədə qərar qəbul edir.

9.4.7. Əməkdaşlar:

- informasiya təhlükəsizliyi üzrə əmək müqavilələrində, vəzifə təlimatlarında, informasiya təhlükəsizliyinə dair digər sənədlərdə ifadə olunmuş bütün tələbləri yerinə yetirir;
- öhdəsinə düşən vəzifələrin və informasiya təhlükəsizliyi üzrə onlara aid tələblərin yerinə yetirilməsi üçün lazımi səviyyədə bilik və vərdişlərə malik olmalıdır.

9.5. Hər hansı informasiya təhlükəsizliyi hadisəsi nəticəsində yaranmış informasiya təhlükəsizliyi risklərinin təsnifatı, ölçülməsi, qiymətləndirilməsi, təhlili və müvafiq tədbirlərin görülməsi Risklərin idarə edilməsi qaydalarına uyğun olaraq həyata keçirilməlidir.

9.6. İnformasiya təhlükəsizliyi hadisəsi nəticəsində yaranmış risk risklərin təsnifatına uyğun olaraq sistem riski kimi qiymətləndirildikdə, bu hadisə barədə dərhal bütün mümkün kanallardan istifadə etməklə maliyyə bazaralrına nəzarət orqanına məlumat verilməlidir.

10. Avadanlıqların təhlükəsizliyinin təmin edilməsi

10.1. Bütün server avadanlıqları onların texniki istifadəsinə uyğun olaraq xüsusi təchiz olunmuş server otaqlarında yerləşdirilməli, bu otaqlara yalnız icazəsi olan şəxslərin girişi təmin edilməlidir (TD-nin əməkdaşının iştirakı ilə) və giriş qapısı qıfıldan əlavə xüsusi identifikasiya vasitələri ilə təchiz edilir.

10.2. Server otaqları odadavamlı mebellər ilə təchiz edilməli, dayanıqlı materiallardan inşa edilməli, döşəməsi və tavanı antistatik örtüklə təmin edilməlidir.

10.3. Server otaqlarında avadanlığın quraşdırılması, əvəz edilməsi, təmiri, otaqlardan çıxarılması, habelə kənar təşkilatların mütəxəssislərinin server otağında işi sistem inzibatçısı və təhlükəsizlik inzibatçısının nəzarəti altında həyata keçirilməlidir.

10.4. Server otaqları yanğınsöndürmə vasitələri, yanğın və mühafizə siqnalizasiya sistemləri, müşahidə kameraları, havalandırma (kondisioner) sistemləri və istiliyin tənzimlənməsi üçün termometrlə təchiz edilməlidir.

10.5. TD-nin əməkdaşları mütəmadi olaraq server otaqlarına baxış keçirməli, yuxarıda qeyd olunan tələblərin yeinə yetirilməsinə nəzarət etməlidir.

10.6. Bütün kompüter və telekommunikasiya avadanlığı elektrik cərəyanı xətlərinə həmin avadanlıqların istehsalçılarının tələblərinə uyğun olaraq qoşulmalıdır.

10.7. Kompüter avadanlıqlarının MDM-ə gətirilməsi və buradan çıxarılması üçün sifarişlər rəsmiləşdirilməli və məlumatlar TD-yə təqdim edilməlidir.

10.8. Bütün kompüter və telekommunikasiya avadanlıqları təftiş edilməli və kompüter avadanlıqlarının korpuslarına icazəsiz müdaxilələrin qarşısının alınması məqsədilə müvafiq nəzarət mexanizmi tətbiq edilməlidir.

10.9. Kompüter və ya server avadanlığı sıradan çıxdıqda, avadanlığın təyinatı dəyişdikdə və ya onun təmiri zamanı informasiya daşıyıcıları MDM-dən çıxarıldıqda həmin daşıyıcılardakı informasiya etibarlı şəkildə silinməlidir.

10.10. Daşınan kompüterlərdə konfidensial məlumatlar saxlanılmamalıdır.

10.11. Əmək fəaliyyətinə xitam verilən əməkdaşlardan istifadə etdikləri avadanlıqlar TD-nin nəzarəti altında təhvil alınmalıdır.

10.12. Kompüter avadanlıqlarının cari vəziyyəti TD tərəfindən vaxtaşırı yoxlanılmalıdır.

10.13. Avadanlıqlarda edilən dəyişikliklər TD-nin əməkdaşının iştirakı ilə aktlaşdlırılmalıdır.

11. Xarici informasiya daşıyıcılarından istifadə

11.1. Xarici informasiya daşıyıcılarının İT infrastruktura aid avadanlıqlara qoşulmasının məhdudlaşdırılması nəzərdə tutulmalıdır.

11.2. Xarici informasiya daşıyıcılarından yalnız biznes ehtiyacları ödəmək zərurəti yarandıqda istifadə oluna bilər və bu halda köçürülən informasiyaya nəzarət olunmalıdır.

11.3. Xarici infromasiya daşıyıcılarının uçotu aparılmalı, onların hamısı identifikasiya olunmalıdır.

11.4. Xarici infromasiya daşıyıcılarında olan məlumatdan istifadə edilməsi zərurəti olmadığı halda həmin informasiya etibarlı şəkildə silinməlidir (bərpa imkanı olmamaq şərti ilə) yaxud daşıyıcının özü məhv edilməlidir.

11.5. İnformasiyanın surətinin xarici informasiya daşıyıcılarına və xarici informasiya daşıyıcılarından İT infrastruktura aid avadanlıqlara köçürülməsi ilə əlaqədar bütün faktlar qeydə alınmalı, daşıyıcının identifikatoru, surəti çıxarılan obyektin adı və surətin çıxarıldığı vaxt göstərilməlidir.

11.6. Xarici infromasiya daçıyıcılarlnda saxlanan və daşınan məlumatlara informasiyanın təsnifləşdirilməsi və nişanlanması prosedurları tətbiq edilməlidir.

11.7. Hər hansı xarici informasiya daşıyıcısının tətbiqi və onların kompüter və digər avadanlıqlara qoşulması istifadəçilərin bilavasitə rəhbəri və TD ilə razılaşdırılmalıdır.

11.8. Konfidensial informasiya daşıyan xarici daşıyıcıların daşınması zamanı onlara icazəsiz baxılması və dəyişikliklər edilməsi imkanını istisna edən tədbirlər (möhürlənmiş və plomblanmış qeyri-şəffaf paket/konteynerdən istifadə) tətbiq olunmalı və xarici daşıyıcıdakı informasiya etibarlı şəkildə şifrələnməlidir.

12. Şəbəkə infrastrukturunun təşkili

12.1. Şəbəkə infrastrukturunun bütün elementlərini, şəbəkə birləşmələrini (məntiqi və fiziki), avadanlıq və protokolları əks etdirən məntiqi və fiziki sxemlər tərtib edilməlidir.

12.2. Cari kabel infrastrukturunun sxeminin, birləşmələrin və qoşulmaların cədvəli tərtib edilməlidir.

12.3. Şəbəkə avadanlıqlarına qoşulma və dəyişikliklərin edilməsi imkanı məhdudlaşdırılmalıdır.

12.4. Bütün kütləvi şəbəkə xidmətləri (İnternet, elektron poçt, DNS, məsafədən giriş sistemləri) ayrılmış şəbəkə seqmentlərində - şəbəkələrarası ekranlarla ayrılmış zonalarda yerləşdirilməlidir.

12.5. Naqilsiz şəbəkələrdən istifadə edilməsi zamanı aşağıdakı tələblər yerinə yetirilməlidir:

12.5.1. Mütləq mühafizə olunmuş protokollardan (məsələn, WPA, WPA2) istifadə edilməlidir;

12.5.2. Naqilsiz rabitəyə zərurət olmadıqda kompüterlərdəki bütün naqilsiz adapterlər söndürülməlidir.

12.6. Serverlərdə, telekommunikasiya avadanlıqlarında istifadə olunan şəbəkə servislərinin və xidmətlərin aktuallığı yoxlanılmalı, lokal şəbəkənin skan olunması təşkil edilməlidir.

12.7. İstifadə olunmayan bütün şəbəkə servisləri və xidmətləri ləğv edilməlidir.

12.8. Müxtəlif şəbəkələrdə əməkdaşların istifadə etdikləri mobil kompüterlər istisna olmaqla istifadəçilərin fərdi kompüterlərində şəbəkə sazlamalarında dəyişikliklər etmək imkanı bağlanılmalıdır.

13. Konfidensial məlumatlarla davranış və nəzarət sisteminin təşkili

13.1. MDM-in informasiya sistemlərində olan məlumatın qorunması məqsədilə konfidensial məlumatlarla işləmək üçün aşağıda göstərilən qaydalara riayət olunmalıdır:

13.1.1. MDM-ə aid məlumatın müəyyən bölməsinə daxil olması haqda qərar rəhbərlik tərəfindən qəbul olunur və təhlükəsizlik üzrə müvafiq struktur bölmə tərəfindən nəzarət olunur;

13.1.2. Elektron sənədlərin və tətbiqi proqramların icazəsi olmayan şəxslər tərəfindən oxunması, dəyişdirilməsi, silinməsi, surətinin çıxarılmasının qarşısının alınması təmin edilir;

13.1.3. Konfidensial məlumatların məzmununun kənar şəxslərə açıqlanması qadağandır.

13.2. Kağız daşıyıcılarda olan məlumatlarla davranış zamanı aşağıdakılara əməl olunmalıdır:

13.2.1. Açıq olmayan məlumatlar aid olduğu struktur bölmə rəhbəri ilə məlumatların kimlər tərəfindən əlavə nüsxələrinin yaradılması və ya çap edilməsi razılaşdırılmalıdır;

13.2.2. Açıq olmayan məlumatların əlavə nüsxələri yaradıldıqda nüsxələrin sayı və ünvan sahibləri haqqında informasiya qeyd edilməlidir;

13.2.3. Açıq olmayan məlumatların üzərində aparılan bütün əməliyyatların (çap etmək, surətini çıxarma, daşıma, göndərmə və s.) uçotu aparılmalıdır;

13.2.4. Kağız üzərində açıq olmayan məlumatlardan ibarət sənədlərin məhv edilməsi kağız doğrayan xüsusi qurğulardan istifadə edilməklə aparılmalıdır;

13.2.5. Çap edilmiş açıq olmayan məlumatlar şəxsən ünvan sahiblərinə çatdırılmalı, boş otaqda nəzarətsiz qoyulmamalıdır;

13.2.6. Açıq olmayan məlumatların çatdırılması ünvan sahibinin məlumatın əldə etməsi barədə təsdiqi ilə müşayiət olunmalıdır;

13.2.7. Açıq olmayan məlumatların ixtiyarsız olaraq kənar şəxslər tərəfindən əldə edilməməsi üçün məsuliyyətlə davranılmalıdır.

13.3. Konfidensial məlumatların həmin məlumatlara hüquqi icazəsi olan şəxslər və ya onların qanuni təmsilçilərinin razılığı olmadan yalnız maliyyə bazarlarına nəzarət orqanının və məhkəmənin sorğusu əsasında onlara təqdim olunmasına yol verilir.

13.4. Konfidensial məlumatlar üzrə yaranan risklər və bununla bağlı müvafiq tədbirlərin görülməsi Risklərin idarə edilməsinə dair müvqfiq qaydalarla tənzimlənir.

14. İnformasiyanın arxivləşdirilməsi və saxlanması

14.1. Aidiyyatı struktur tərəfindən ehtiyat surəti çıxarılan informasiya resurslarının siyahısı müəyyən edilməli, müntəzəm olaraq ehtiyat köçürülmə proseduru tətbiq edilməlidir.

14.2. Ehtiyat surətçıxarmanın yerinə yetirilməsi və ona nəzarət üçün məsul olan əməkdaşın və ya əməkdaşların siyahısı MDM rəhbərliyi tərəfindən təsdiq edilməlidir.

14.3. Ehtiyat surətlərin çıxarılmasının tezliyi məlumatların nə qədər tez dəyişməsinə, bu dəyişikliklərin nə qədər zəruri olmasına və əməliyyatların həcminə uyğun olmalıdır.

14.4. Ehtiyat surətlər qeyri-iş vaxtlarında çıxarılmalıdır.

14.5. Ehtiyat surətlər onların istifadəyə yararlı olduğuna əmin olmaq məqsədilə mütəmadi sınaqdan keçirilməlidir.

14.6. Ehtiyat surətçıxarma tapşırıqlarının müvəffəqiyyətlə yerinə yetirilməsinə nəzarət etmək üçün ehtiyat surətçıxarma sistemi proseslərinin qeydiyyatı jurnallarının yoxlanması həyata keçirilməlidir.

14.7. Ehtiyat surətləri MDM-in binasından kənarda saxlanmalıdır.

14.8. Ehtiyat surətlərinin çıxarılması, köçürülməsi və saxlanması proseslərinə təhlükəsizlik inzibatçısı tərəfindən nəzarət olunmalıdır.

15. İnternet resurslarından istifadə qaydaları

15.1. Zərər verici proqram təminatının, icazəsiz birləşmələrin və tunellərin aşkara çıxarılması məqsədi ilə bütün İnternet trafiki (daxil olan və çıxan) inzibatçılar tərəfindən xüsusi proqram təminatı ilə süzgəcdən keçirilməlidir.

15.2. MDM rəhbərliyi tərəfindən struktur bölmələr üzrə əməkdaşların internet resurslarından istifadə hüquqları müəyyənləşdirilməli və təsdiq edilməlidir.

15.3. İnternetlə məlumat mübadiləsi üzərində məhdudiyyətlər müəyyən edilməli, habelə əməkdaşların müxtəlif kateqoriyaları (qrupları) üçün internet ünvanlarının məzmunu təyin edilməlidir.

15.4. İnformasiya təhlükəsizliyi üzrə mütəxəssis tərəfindən internet resurslarından istifadə nəzarətdə saxlanmalı və məlumatların təhlili aparılmalıdır.

16. Elektron poçtdan istifadə qaydaları

16.1. İstifadəçilərin poçt qutusunun ölçüsü, habelə xarici və daxili məktubun maksimum həcmi təyin edilməlidir.

16.2. Elektron məlumatların kütləvi surətdə göndərilməsindən mühafizə sistemləri (antispam sistemləri) tətbiq edilməlidir.

16.3. Kənar ünvanlara göndərilən elektron məktublara məlumatın məzmunundan düzgün istifadə edilməməsinə görə məsuliyyət barədə xəbərdarlıq (məxvilik bildirişi) əlavə edilməlidir.

17. Yekun Müddəalar

17.1. Bu Qaydalar Müşahidə Şurasının qərarı ilə təsdiq edildiyi gündən qüvvəyə minir.

17.2. Qaydalara aşağıdakı hallarda yenidən baxılır:

17.2.1. MDM-in təşkilati strukturunda, biznes proseslərində və ya İT resurslarında ciddi dəyişikliklər olduqda;

17.2.2. İnformasiya təhlükəsizliyi sahəsində MDM-in rəhbərliyi tərəfindən müəyyən edilən məqsəd və vəzifələr dəyişdirildikdə;

17.2.3. MDM-in iş şərtləri, o cümlədən qanunvericiliyin və ya tənzimləyici orqanların tələbləri dəyişdikdə;

17.2.4. MDM-in informasiya təhlükəsizliyinin idarə olunmasına yanaşmalar dəyişdikdə.

17.3. Qaydalara dəyişikliklər yalnız Müşahidə Şurasının qərarı ilə təsdiq edildikdən sonra qüvvəyə minir.

“İnformasiya təhlükəsizliyinə dair
Azərbaycan Respublikasının Milli Depozit Mərkəzinin daxili Qaydaları”na
ƏLAVƏ №1

İT resurslarında hüquqların verilməsi forması

Tərtib etmə tarixi: (gün/ay/il)_____

☐Hüquqların verilməsi ☐ Hüquqların dəyişdirilməsi ☐Hüquqların alınması

İşçinin adı,soyadı, atasının adı:

İşə başlama tarixi (gün/ay/il):
Departamentin adı və vəzifəsi:
İT resursun adı:
Hüquqların təsviri:

1 2 3 4 5	6 7 8 9 10

Birbaşa rəhbər

_____
(adı, soyadı)

MDM-in rəhbəri

_____
(adı, soyadı)

_____
(imza, tarix)

İnzibatçı

_____
(adı, soyadı)

_____
(imza, tarix)

Təyin edilmiş istifadəçi adı:

İstifadəçi adını və ilkin şifrəni qəbul etdim. İstifadəçi adının və şifrəsinin məsuliyyəti mənə izah olundu.

Hüquq veriləcək şəxs _____ _____
(adı, soyadı) (imza, tarix)

“İnformasiya təhlükəsizliyinə dair
Azərbaycan Respublikasının Milli Depozit Mərkəzinin daxili Qaydaları”na
ƏLAVƏ №2

Qeyri-iş saatlarıda istifadəçilərin İT resurslarına qoşulmasına icazə forması

Tərtib etmə tarixi: (gün/ay/il)_____

İşçinin adı,soyadı, atasının adı:
Struktur bölməsinin adı və vəzifəsi:
İT resursunun adı:
İstifadəçi adı:
Qoşulma vaxtının tarixi: ____ _____ _____ (gün/ay/il)
Qoşulma vaxtının saat aralığı: saat: ___ ___dan ___ ___ dək
Görəcəyi işlərin təsviri:
1.
2.
3.
4.
5.
6.
7.
8
9.
10

Birbaşa rəhbər

_____
(adı, soyadı)

_____
(imza, tarix)

İnformasiya təhlükəsizliyi üzrə müvafiq struktur bölmənin rəhbəri

_____
(adı, soyadı)

_____
(imza, tarix)

İnzibatçı

_____
(adı, soyadı)

_____
(imza, tarix)