AZƏRBAYCAN RESPUBLİKASI MƏRKƏZİ BANKININ İDARƏ HEYƏTİNİN

Q Ə R A R I

№ 14/2

Bakı şəhəri **28 mart 2024-cü il**

"Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər"in təsdiq edilməsi barədə

Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair tələblərin beynəlxalq standartlara uyğun olaraq gücləndirilməsi məqsədilə "Azərbaycan Respublikasının Mərkəzi Bankı haqqında" Azərbaycan Respublikası Qanununun 22.1.17-ci və 48.3.4-cü maddələrinə, habelə "İcbari sığortalar haqqında" Azərbaycan Respublikası Qanununun 34-1.4-cü maddəsinə əsasən Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyəti

QƏRARA ALIR:

1. "Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər" (bundan sonra – Tələblər) təsdiq edilsin (əlavə olunur).

2. Bu Qərarın 1-ci hissəsi ilə təsdiq edilmiş Tələblər dərc edildiyi gündən bir il sonra qüvvəyə minsin və həmin tarixdən "Banklarda informasiya təhlükəsizliyinin idarə edilməsi Qaydası"nın təsdiq edilməsi barədə" Azərbaycan Respublikası Mərkəzi Bankının İdarə Heyətinin 2021-ci il 14 iyul tarixli 20/1 nömrəli Qərarının 1-ci hissəsi ləğv edilsin.

3. Hüquq departamentinə tapşırılsın ki, bu Qərarın 3 gün müddətində Azərbaycan Respublikasının Hüquqi Aktların Dövlət Reyestrinə daxil edilməsi üçün Azərbaycan Respublikasının Ədliyyə Nazirliyinə təqdim edilməsini təmin etsin.

Mərkəzi Bankın sədri **Taleh Kazımov**

"Təsdiq edilmişdir"
Azərbaycan Respublikasının
Mərkəzi Bankı
Qərar № 14/2
28 mart 2024-cü il

Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər

1. Ümumi müddəalar

1.1. Bu Tələblər "Azərbaycan Respublikasının Mərkəzi Bankı haqqında" Azərbaycan Respublikası Qanununun 48.3.4-cü maddəsinə, habelə "İcbari sığortalar haqqında" Azərbaycan Respublikası Qanununun 34-1.4-cü maddəsinə əsasən hazırlanmışdır və banklarda, kredit ittifaqları istisna olmaqla, bank olmayan kredit təşkilatlarında, sığortaçılarda, qiymətli kağızlar bazarında lisenziyalaşdırılan şəxslərdə, səhmdar investisiya fondları və investisiya fondlarının idarəçilərində, poçt rabitəsinin milli operatorunda, ödəniş təşkilatlarında, elektron pul təşkilatlarında, ödəniş sistemlərinin operatorlarında, kredit bürolarında, mərkəzi depozitarda informasiya təhlükəsizliyinə dair minimum tələbləri müəyyən edir.

1.2. Bu Tələblər İcbari Sığorta Bürosunun icbari sığortalar üzrə informasiya sistemi və əlaqəli aktivlərinə münasibətdə tətbiq edilir.

1.3. Bu Tələblərin 1.1-ci və 1.2-ci bəndlərində nəzərdə tutulan şəxslər birlikdə bu Tələblərdə nəzarət subyektləri adlandırılır.

1.4. Bu Tələblərin 4.12-4.16-cı və 6.5-ci bəndləri bu Tələblərin 2.1.35-ci yarımbəndində nəzərdə tutulan II kateqoriya nəzarət subyektlərinə tətbiq edilmir.

1.5. Bu Tələblərin 4.4-cü, 4.5-ci, 4.12- 4.16-cı, 6.5-ci, 6.9-cu, 6.10-cu, 6.12-ci, 7.17-ci, 7.19-cu, 7.21 - 7.23-cü bəndləri bu Tələblərin 2.1.36-cı yarımbəndində nəzərdə tutulan III kateqoriya nəzarət subyektlərinə tətbiq edilmir.

1.6. Nəzarət subyektlərində fərdi məlumatların mühafizəsinə dair tələblər bu Tələblər ilə yanaşı "Fərdi məlumatlar haqqında" Azərbaycan Respublikasının Qanunu ilə tənzimlənir.

2. Anlayışlar

2.1. Bu Tələblərdə istifadə edilən əsas anlayışlar aşağıdakı mənaları ifadə edir:

2.1.1. **aktiv** – nəzarət subyektləri üçün dəyəri olan əsas (biznes proseslər və informasiya) və dəstəkləyici (şəbəkə və texniki infrastruktur, proqram təminatları, personal, bina, təşkilati struktur) aktivlər;

2.1.2. **aktiv sahibi** – aktivin bütün fəaliyyət dövrü ərzində idarə edilməsinə və mühafizəsinə məsul olan şəxs;

2.1.3. **audit** – audit sübutlarının əldə edilməsi və onların audit meyarlarının yerinə yetirmə səviyyəsini müəyyənləşdirmək məqsədilə obyektiv olaraq qiymətləndirilməsi üçün həyata keçirilən sistematik, müstəqil və sənədləşdirilmiş proses;

2.1.4. **autentikasiya** – xidmət istifadəçisinin kimliyini və fərdiləşdirilmiş təhlükəsizlik məlumatlarının istifadəsinin etibarlılığını yoxlamağa imkan verən nəzarət tədbiri;

2.1.5. **dərindən müdafiə (defence in depth**) – aktivlərin mühafizəsi üçün çoxsəviyyəli nəzarət tədbirlərinin müəyyən edilməsi;

2.1.6. **emulyator** – əməliyyat sistemini imitasiya etməklə həmin əməliyyat sistemində çalışan proqramları çalışdıran proqram təminatı;

2.1.7. **etiketlənmə** – informasiyanın təsnifatına uyğun olaraq informasiya və əlaqəli aktivlərin müxtəlif üsullarla (məsələn, fiziki nişan, başlıq və altlıq, metadata, su nişanı, ştamp vasitəsilə) işarələnməsi;

2.1.8. **əməliyyat mühiti** – informasiya sisteminin istifadəçiyə açıq real istismar mühiti;

2.1.9. **həssas informasiya** – fiziki və hüquqi şəxslərə, habelə milli təhlükəsizliyə potensial mənfi təsirləri səbəbilə icazəsiz işlənmədən, o cümlədən daxil olmadan, dəyişdirilmədən və ya açıqlanmadan mühafizə edilməli informasiya (məsələn, həssas ödəniş məlumatları, fərdi məlumatlar, dövlət sirri, kommersiya sirri, bank sirri, sığorta sirri və digər konfidensial məlumatlar);

2.1.10. **informasiya** – yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlar;

2.1.11. **informasiyanın əlçatanlığı** – tələb olunduğu halda informasiyanın əldə edilə və istifadə oluna bilməsi xüsusiyyəti;

2.1.12. **informasiyanın konfidensiallığı** – informasiyanın səlahiyyətli olmayan girişlər üçün əlçatan və açıq olmama xüsusiyyəti;

2.1.13. **informasiya prosesi** – informasiyanın yaradılması, yığılması, işlənməsi, saxlanması, axtarışı, yayılması;

2.1.14. **informasiya sistemi** – informasiya texnologiyaları və sənədlərinin təşkilati və texniki qaydada, o cümlədən hesablama texnikasından istifadə edilməklə, nizamlanmış məcmusu;

2.1.15. **informasiyanın tamlığı** – informasiyanın dəqiqlik və bütünlük xüsusiyyəti;

2.1.16. **informasiya təhlükəsizliyi** – informasiyanın konfidensiallığının, tamlığının və əlçatanlığının mühafizə olunması;

2.1.17. **informasiya təhlükəsizliyinin idarə edilməsi sistemi (bundan sonra - İTİS) –** fəaliyyət məqsədlərinə nail olmaq üçün nəzarət subyektinin informasiya təhlükəsizliyinin yaradılması, tətbiq edilməsi, dəstəklənməsi və davamlı inkişaf etdirilməsinə istiqamətlənən fəaliyyət və prosedurlar toplusu;

2.1.18. **informasiya texnologiyaları** – informasiya proseslərinin avtomatlaşdırılmış qaydada icrası üçün istifadə edilən proqramlar, sistemlər və ya avadanlıqlar;

2.1.19. **informasiya təhlükəsizliyi hadisəsi** – informasiya təhlükəsizliyi siyasətinin mümkün pozuntusu və ya idarəetmənin uğursuzluğunu göstərən sistem, xidmət və ya şəbəkə vəziyyətinin meydana gəlməsi və ya təhlükəsizliklə əlaqəli ola biləcək əvvəllər bilinməyən bir vəziyyət;

2.1.20. **informasiya təhlükəsizliyi insidenti** – biznes proseslərin pozulması və informasiya təhlükəsizliyi təhdidi yaratma ehtimalı əhəmiyyətli olan bir və ya bir neçə arzuolunmaz və ya gözlənilməz informasiya təhlükəsizliyi hadisəsi;

2.1.21. **inkişaf mühiti** – informasiya sisteminin proqram təminatlarının işlənib hazırlanması mühiti;

2.1.22. **istifadəçi** – informasiya sistemində giriş hüququ olan personal və müştərilər;

2.1.23. **kriptoqrafik vasitələr** – informasiyanın kriptoqrafik çevrilməsindən istifadə etməklə informasiya təhlükəsizliyinin təmin edilməsi üçün tətbiq olunan üsullar (avadanlıqlar, tətbiqi proqram təminatları və s.);

2.1.24. **kritik informasiya sistemi** – həssas informasiya üzrə informasiya proseslərini icra edən, nəzarət subyektlərinin əsas fəaliyyətinin həyata keçirilməsi zamanı istifadə edilən və (və ya) nəzarət subyektlərində risklərin qiymətləndirilməsinə əsasən yüksək təsir səviyyəsinə malik olan informasiya sistemləri;

2.1.25. **mobil cihaz** – fərdi istifadə üçün nəzərdə tutulmuş portativ elektron cihaz (noutbuk, planşet, smartfon və s.);

2.1.26. **personal** – nəzarət subyektində fəaliyyət göstərən mütəxəssislər, o cümlədən əmək müqavilələri və digər müqavilələrə əsasən çalışan fiziki şəxslər və təcrübəçilər;

2.1.27. **personalizasiya** – ödəniş kartlarının hazırlanması zamanı ödəniş kartının istifadəçisi haqqında məlumatların elektron daşıyıcıya (çipə) və (və ya) maqnit lentə yüklənməsi və ödəniş kartı üzərində eyniləşdirmə məlumatlarının çap olunması;

2.1.28. **sıfır etibar (zero trust**) – ilkin olaraq bütün istifadəçilər, cihazlar və şəbəkələrə etibar edilməməsi və giriş icazəsi verilməzdən əvvəl yoxlanmasının zəruriliyini ehtiva edən təhlükəsizlik modeli;

2.1.29. **sınaq mühiti** – informasiya sisteminin real istismara verilməzdən əvvəl test edildiyi mühit;

2.1.30. **sistem inzibatçısı** – informasiya sistemində dəyişiklikləri tətbiq edən, onun ehtiyat nüsxələrinin yaradılmasını, fəaliyyətinin monitorinqini və fasiləsiz fəaliyyətini təmin edən, habelə səlahiyyət bölgüsünə əsasən sistem üzrə digər funksiyaları həyata keçirən nəzarət subyektinin personalı;

2.1.31. **son istifadəçi cihazı** – şəbəkəyə qoşulmuş informasiya və kommunikasiya texnologiyaları avadanlıqları (məsələn, masaüstü kompüterlər, mobil cihaz, əşyaların interneti və s.);

2.1.32. **təchizatçı** – müqavilə əsasında nəzarət subyektinə mal (iş, xidmət) təqdim edən şəxs;

2.1.33. **yuxarı idarəetmə orqanı** – nəzarət subyektinin daxili nəzarət orqanı (müvafiq olaraq müşahidə (direktorlar) şurası, himayəçilik şurası və ya digər səlahiyyətli idarəetmə orqanı);

2.1.34**. I kateqoriya nəzarət subyektləri** – banklar, sığortaçılar, mərkəzi depozitar, İcbari Sığorta Bürosu, kredit büroları, elektron pul təşkilatları və ödəniş sistemlərinin operatorları;

2.1.35. **II kateqoriya nəzarət subyektləri** – qiymətli kağızlar bazarında lisenziyalaşdırılan şəxslər, poçt rabitəsinin milli operatoru, ödəniş təşkilatları, səhmdar investisiya fondları və investisiya fondlarının idarəçiləri;

2.1.36. **III kateqoriya nəzarət subyektləri** – kredit ittifaqları istisna olmaqla, bank olmayan kredit təşkilatları.

3. İnformasiya təhlükəsizliyinin idarə edilməsi sistemi

3.1. İTİS nəzarət subyektlərində bu Tələblərin və Azərbaycan Respublikası Mərkəzi Bankının (bundan sonra – Mərkəzi Bank) digər normativ xarakterli aktlarının tələbləri nəzərə alınmaqla nəzarət subyektinin yuxarı idarəetmə orqanının ümumi rəhbərliyi altında nəzarət subyektinin biznes prosesləri və ümumi idarəetmə sisteminin ayrılmaz hissəsi kimi formalaşdırılır, fəaliyyəti təmin edilir və davamlı olaraq təkmilləşdirilir.

3.2. İTİS-in formalaşdırılması ilə bağlı nəzarət subyektinin ümumi strategiyasına uyğun olan informasiya təhlükəsizliyi siyasəti hazırlanır və yuxarı idarəetmə orqanı tərəfindən təsdiq edilir.

3.3. İTİS-ə bilavasitə nəzarətin həyata keçirilməsi üçün nəzarət subyekti tərəfindən informasiya təhlükəsizliyi üzrə məsul şəxs təyin edilir. İnformasiya təhlükəsizliyi üzrə məsul şəxsin əsas vəzifələri aşağıdakılardır:

3.3.1. informasiya təhlükəsizliyi siyasətini, əlaqəli qaydaları hazırlayır və rəhbərliyə təqdim edir;

3.3.2. İTİS-i təşkil edir və təkmilləşdirilməsi üçün təkliflər hazırlayır;

3.3.3. İTİS üzrə nəzarət subyektinin struktur bölmələrinin fəaliyyətini əlaqələndirir;

3.3.4. rüblük əsasda nəzarət subyektində informasiya təhlükəsizliyi vəziyyəti və informasiya təhlükəsizliyi riskləri ilə bağlı rəhbərliyə hesabat təqdim edir;

3.3.5. informasiya təhlükəsizliyi tələblərindən kənarlaşmalar baş verdikdə səbəbləri göstərilməklə bu barədə rəhbərliyi dərhal məlumatlandırır;

3.3.6. personalın, o cümlədən informasiya təhlükəsizliyinin təmin edilməsi funksiyasını həyata keçirən struktur bölmələrin əməkdaşlarının məlumatlandırılması, təlimlərə cəlb edilməsi, habelə müştərilərin maarifləndirilməsi işini təşkil edir.

3.4. İnformasiya təhlükəsizliyi siyasəti müvafiq informasiya risklərini və nəzarət sahələrini kompleks və əsaslı şəkildə əhatə edərək aydın və anlaşılan formada hazırlanır, təsdiqlənir və təsdiq edilmiş redaksiya personalla kommunikasiya edilir.

3.5. İnformasiya təhlükəsizliyi siyasəti azı bu Tələblərin 4-7-ci hissələri ilə müəyyən edilən tədbirləri əhatə edir və İTİS-in davamlı təkmilləşdirilməsi öhdəliyini müəyyənləşdirir.

3.6. İnformasiya təhlükəsizliyi siyasəti azı ildə 1 (bir) dəfə ayrıca, habelə nəzarət subyektinin risklərin idarə edilməsi sisteminə baxılarkən yenidən nəzərdən keçirilir və tələb edildikdə müvafiq dəyişikliklər edilir. İTİS-in davamlılığının, adekvatlığının və effektivliyinin təmin edilməsi üçün dəyişikliklər edildikdə informasiya təhlükəsizliyi siyasətinə növbədənkənar qaydada yenidən baxılır.

3.7. Bu Tələblərə uyğunluğun qiymətləndirilməsi üçün nəzarət subyektində İTİS informasiya təhlükəsizliyinin yoxlanılması sahəsində beynəlxalq səviyyədə akkreditasiya edilmiş və maliyyə bazarlarında informasiya təhlükəsizliyinin yoxlanılması üzrə azı 3 (üç) il təcrübəyə malik kənar auditor tərəfindən aşağıdakı dövriliklə yoxlanılır:

3.7.1. I kateqoriya nəzarət subyektlərində ildə 1 (bir) dəfədən az olmayaraq;

3.7.2. II və III kateqoriya nəzarət subyektlərində 2 (iki) ildə bir dəfədən az olmayaraq.

3.8. Ödəniş kartları vasitəsilə aparılmış əməliyyatlar haqqında məlumatların toplanması, emalı və ötürülməsinə, həmçinin kart emissiyasına və ekvayrinqinə texniki xidmət göstərilməsi üzrə fəaliyyəti həyata keçirən ödəniş sistemlərinin operatorları və banklar əlavə olaraq bu sahə üzrə informasiya təhlükəsizliyi standartlarına uyğunluğun

yoxlanılması sahəsində beynəlxalq səviyyədə akkreditasiya edilmiş kənar auditor tərəfindən ildə 1 (bir) dəfədən az olmayaraq yoxlanılır.

4. Təşkilati nəzarət tədbirləri

4.1. Nəzarət subyektində informasiya təhlükəsizliyinə cavabdeh müstəqil struktur bölmə formalaşdırılır, bu struktur bölmənin, habelə digər personalın informasiya təhlükəsizliyi ilə bağlı vəzifələri və bu vəzifələr üzrə öhdəlik və səlahiyyətləri müəyyən edilir. Maraqlar münaqişəsinin qarşısını almaq məqsədilə informasiya təhlükəsizliyinə cavabdeh struktur bölmənin informasiya texnologiyalarına cavabdeh struktur bölmədən ayrı yaradılması və fərqli kuratorlara tabe olması təmin edilir.

4.2. İnformasiya və digər əlaqəli aktivlərin icazəsiz, qeyri-ixtiyari dəyişdirilməsi və ya sui-istifadəsi hallarının məhdudlaşdırılması üçün nəzarət subyekti toqquşan vəzifələrin və öhdəlik sahələrinin bir-birindən ayrılmasını təmin edir.

4.3. Nəzarət subyekti tərəfindən informasiya təhlükəsizliyinin təmin edilməsi məqsədilə Mərkəzi Bankla, habelə səlahiyyətli dövlət orqanları (qurumları) ilə qarşılıqlı əlaqələrin yaradılması və qarşılıqlı fəaliyyət üzrə informasiyanın, habelə informasiya təhlükəsizliyi insidentləri barədə məlumatların vaxtında mübadiləsi ilə bağlı müvafiq prosedurlar formalaşdırılır.

4.4. Nəzarət subyekti tərəfindən informasiya təhlükəsizliyi təhdidlərinin vaxtında müəyyənləşdirilməsi məqsədilə müvafiq məlumatlar toplanılır və təhlili aparılır.

4.5. Layihələrin növündən asılı olmayaraq layihə idarəetməsinin bütün mərhələlərində nəzarət subyekti tərəfindən informasiya təhlükəsizliyi təmin edilir və davamlı monitorinqi aparılır.

4.6. Nəzarət subyektində informasiya və digər əlaqəli aktivlərin mühafizəsi üzrə aşağıdakı tədbirlər həyata keçirilir:

4.6.1. informasiya və digər əlaqəli aktivlər müəyyənləşdirilir və inventarizasiyası aparılmaqla aktuallığı təmin edilir;

4.6.2. inventarizasiya edilmiş aktivlər üzrə onların bütün istifadə dövründə düzgün idarə edilməsinə məsul olan aktiv sahibləri müəyyən edilir;

4.6.3. informasiya və digər əlaqəli aktivlərdən məqbul istifadə qaydaları müəyyən edilir və təsdiq edilməklə sənədləşdirilir;

4.6.4. əmək və xidmət müqavilələri dəyişdiyi, habelə müddətləri bitdiyi zaman aktivlərin mühafizəsi təmin edilir, həmçinin personalın istifadəsində olan müvafiq aktivlər nəzarət subyektinə geri qaytarılır;

4.6.5. informasiyanın tamlıq, konfidensiallıq, əlçatanlıq xüsusiyyətləri, dəyəri, əhəmiyyətliliyi, icazəsiz açıqlanma və ya dəyişikliyə qarşı həssaslığı, maraqlı tərəflərin tələbləri, habelə qanunvericiliyin tələbləri nəzərə alınmaqla informasiyanın təsnifatı həyata keçirilir;

4.6.6. qəbul edilmiş informasiya təsnifatına uyğun olaraq informasiyanın və əlaqəli aktivlərin etiketlənməsi qaydaları müəyyən edilir və təsdiq edilməklə sənədləşdirilir;

4.6.7. daxili və kənara bütün növ informasiya ötürmə üsulları üçün aşağıdakılar nəzərə alınmaqla informasiyanın ötürülməsi tələbləri müəyyənləşdirilir, habelə həmin tələblər müvafiq qaydalarda və müqavilələrdə nəzərə alınır:

4.6.7.1. ötürülən informasiyanın ələ keçirilməsi, icazəsiz daxil olma, surətinin çıxarılması, dəyişdirilməsi, yanlış istiqamətləndirilməsi, məhv edilmə kimi hallar üzrə nəzarət tədbirləri, o cümlədən ötürülən informasiyanın təsnifatına uyğun olaraq həssas informasiyanın qorunması üçün kriptoqrafik üsullar;

4.6.7.2. ötürülmə zamanı informasiyanın etibarlılığı qorunmaqla izlənəbilənliyinin və inkaredilməzliyinin təmin edilməsi üçün nəzarət tədbirləri;

4.6.7.3. informasiya ötürmə vasitələrinin etibarlılığının və əlçatanlığının təmin edilməsi;

4.6.7.4. informasiyanın saxlanılması, emalı, istifadəsi, arxivləşdirilməsi və silinməsi üzrə prosedurların müəyyən edilməsi;

4.6.7.5. informasiyanın müvafiq qaydada mühafizəsini təmin etmək üçün qarşı tərəflə razılaşdırılmış etiketlənmə sisteminin istifadəsi.

4.7. Biznes və informasiya təhlükəsizliyi tələbləri əsasında informasiya və digər əlaqəli aktivlərə girişlər üzrə azı aşağıdakılar nəzərə alınmaqla qaydalar hazırlanır və təsdiq edilir:

4.7.1. informasiya və digər əlaqəli aktivlərə giriş hüquqlarının bütün həyat dövrü üzrə qeydiyyatının və mütəmadi monitorinqinin aparılması;

4.7.2. giriş hüquqları verilmiş hesabların istifadəçi, imtiyazlı və servis hesabları olaraq təsnifatının aparılması və aktuallığının təmin edilməsi;

4.7.3. nəzarət subyekti tərəfindən müəyyən edilmiş müddət ərzində istifadə edilməyən, habelə aktuallığını itirmiş giriş hesablarının bloklanması;

4.7.4. müvafiq informasiya və digər əlaqəli aktivlər üzrə giriş hüquqlarının yalnız həvalə edilmiş vəzifələrin icrası üçün zəruri olan hədlərdə verilməsi;

4.7.5. personal və təchizatçılarla müqavilə münasibətlərinə xitam verildikdə və ya dəyişdirildikdə müvafiq olaraq onların informasiya və digər əlaqəli aktivlərə giriş hüquqlarının dərhal ləğv edilməsi və ya dəyişikliyə uyğunlaşdırılması;

4.7.6. sistem və proqram təminatlarının mənbə kodlarına giriş hüquqlarının məhdudlaşdırılması.

4.8. Nəzarət subyektində autentikasiya məlumatlarının idarə edilməsi üzrə azı aşağıdakı tələbləri nəzərə alan qaydalar hazırlanır və təsdiq edilir:

4.8.1. əvvəlcədən təyin edilmiş (susmaya görə) autentikasiya məlumatlarının sistemlərin və ya proqram təminatlarının quraşdırılmasından dərhal sonra dəyişdirilməsi;

4.8.2. autentikasiya məlumatı kimi müəyyən edilən şifrələrin azı aşağıdakı tələblərə cavab verməsi:

4.8.2.1. şifrələr üçüncü şəxslər tərəfindən asanlıqla təxmin edilə bilən və ya şifrə sahibi ilə əlaqəli məlumatlardan (məsələn, adlar, telefon nömrələri və doğum tarixləri və s.) ibarət olmaması;

4.8.2.2. sistemə ilk giriş zamanı və ya şifrə sistem inzibatçısı tərəfindən yeniləndikdən sonra informasiya sistemində personaldan şifrə yenilənməsinin tələb edilməsi və tələbin inkar edilməsinə imkan verilməməsi;

4.8.2.3. şifrə təyin edilərkən minimum uzunluq, hərf-rəqəm və xüsusi simvollardan istifadə tələblərinin müəyyən edilməsi;

4.8.2.4. şifrələrin qüvvədə olma müddətinin müəyyən edilməsi;

4.8.2.5. əvvəl istifadə edilən şifrələrdən təkrar istifadənin məhdudlaşdırılması;

4.8.3. personalı özlərinin autentikasiya məlumatlarını qorumağa cavabdeh etmək məqsədilə nəzarət subyekti tərəfindən müəyyən edilən qaydalara riayət etmələrinin tələb edilməsi və nəzarətin təmin edilməsi.

4.9. Təchizatçılarla münasibətlərdə bu Tələblər ilə müəyyən edilmiş informasiya təhlükəsizliyi tələbləri gözlənilir, o cümlədən aşağıda qeyd edilən tədbirlərin icrası təmin edilir:

4.9.1. nəzarət subyektinin aktivlərinə giriş hüququ olan təchizatçılarla münasibətdə risklərin minimallaşdırılması məqsədilə informasiya təhlükəsizliyi tələblərinin tərəflər arasında razılaşdırılması və sənədləşdirilməsi;

4.9.2. təchizatçıların reyestrinin tərtib edilməsi və təchizatçıların göstərdikləri xidmətlərin nəzarət subyekti tərəfindən mütəmadi monitorinqinin aparılması;

4.9.3. təchizatçılar tərəfindən göstərilən xidmətlərdə edilən dəyişikliklərin informasiya, informasiya sistemləri və proseslərin kritikliyi nəzərə alınmaqla informasiya təhlükəsizliyi üzrə mövcud siyasətə və qaydalara uyğun olaraq aparılması və risk qiymətləndirilməsinin həyata keçirilməsi;

4.9.4. nəzarət subyektinin aktivlərinə giriş hüququ olan təchizatçılarla bağlanılan müqavilələrdə informasiya təhlükəsizliyi üzrə əlaqələndirici şəxs(lər)in müəyyən edilməsi;

4.9.5. nəzarət subyekti xidmətləri kənardan aldığı zaman belə xidmət göstərən təchizatçılara və onlar tərəfindən təqdim edilən xidmətlərə münasibətdə aparılan risk qiymətləndirilməsinə, habelə qanunvericiliyin tələblərinə əsasən həssas informasiyaya çıxışın məhdudlaşdırması və təchizatçının birbaşa xidmət göstərən personalına dair müvafiq peşəkarlıq tələblərinin müəyyən edilməsi.

4.10. "Bulud" xidmətlərinin əldə edilməsi, istifadəsi, idarə edilməsi və xidmətlərdən çıxışla bağlı nəzarət subyekti tərəfindən aşağıdakı tədbirlər görülür:

4.10.1. azı aşağıdakılar nəzərə alınmaqla qaydalar hazırlanır və təsdiq edilir:

4.10.1.1. "bulud" xidmətlərindən istifadə üzrə informasiya təhlükəsizliyi tələbləri;

4.10.1.2. "bulud" xidmətinin seçim meyarlarının (müvafiq sahə üzrə ISO/IEC, PCI DSS, Uptime Tier və (və ya) digər beynəlxalq standartlara uyğunluq) və bulud xidmətindən istifadənin əhatə dairəsi;

4.10.1.3. "bulud" xidmətlərinin istifadəsi və idarə edilməsi üzrə vəzifə və öhdəliklər;

4.10.1.4. "bulud" xidməti təchizatçısı və nəzarət subyekti tərəfindən ayrılıqda tətbiq edilən nəzarət tədbirləri;

4.10.1.5. "bulud" xidmətlərindən istifadə ilə bağlı informasiya təhlükəsizliyi insidentlərinin idarə edilməsi tədbirləri;

4.10.1.6. informasiya təhlükəsizliyi risklərinin idarə edilməsi məqsədilə istifadə edilən "bulud" xidmətlərinin monitorinqi və qiymətləndirilməsi ilə bağlı tədbirlər;

4.10.1.7. "bulud" xidmətlərindən istifadə zamanı baş verən fövqəladə hallarda fəaliyyətin davamlılığı ilə bağlı tədbirlər;

4.10.1.8. çıxış strategiyası da daxil olmaqla "bulud" xidmətlərindən imtina və ya xidmətin dəyişdirilməsi (dayandırılması) qaydası.

4.10.2. "bulud" xidməti müqavilələri nəzarət subyektinin informasiyanın təhlükəsizliyi siyasətinin tələblərinə cavab verməlidir. Nəzarət subyektinin sahib olduğu informasiyanın və xidmətlərinin əlçatanlığının qorunması üçün "bulud" xidməti müqavilələrində aşağıdakı şərtlər gözlənilməlidir:

4.10.2.1. “bulud” xidməti üzrə həllərin arxitektura və infrastruktur üzrə müvafiq sahədə beynəlxalq standartlara əsaslanması;

4.10.2.2. “bulud” xidməti üzrə girişlərə nəzarət mexanizmlərinin nəzarət subyektinin tələblərinə uyğun olması;

4.10.2.3. zərərli proqram təminatlarından mühafizə və monitorinqi həllərinin tətbiq edilməsi;

4.10.2.4. nəzarət subyektinin sahib olduğu həssas informasiyanın bu Tələblərin 4.10.2.5-ci yarımbəndinin tələbi nəzərə alınmaqla yalnız məlumat ötürmə kanallarının tam şifrlənməsi (end-to-end encryption) təmin edilməklə işlənməsi;

4.10.2.5. nəzarət subyektinin sahib olduğu həssas informasiyanın yalnız Azərbaycan Respublikasının ərazisində saxlanması;

4.10.2.6. “bulud” xidməti təchizatçısı tərəfindən nəzarət subyektinə məxsus informasiyadan digər məqsədlər üçün istifadə edilməməsi, həmçinin xidmət göstərilən digər təşkilatların məlumatlarından ayrı saxlanılması;

4.10.2.7. “bulud” xidməti çərçivəsində informasiya təhlükəsizliyi hadisəsi baş verdikdə “bulud” xidməti təchizatçısı tərəfindən müvafiq dəstəyin göstərilməsi;

4.10.2.8. “bulud” xidmətlərinin “bulud” xidməti təchizatçısı tərəfindən submüqavilə əsasında üçüncü tərəf vasitəsilə təqdim edilməsinin qadağan edilməsi;

4.10.2.9. rəqəmsal sübutların toplanılmasında nəzarət subyektinə dəstəyin göstərilməsi;

4.10.2.10. nəzarət subyektinin “bulud” xidmətindən imtina etməsi halında tərəflər arasında razılaşdırılmış vaxt çərçivəsində müvafiq dəstəyin və xidmətlərin əlçatanlığının təmin edilməsi;

4.10.2.11. “bulud” xidməti təchizatçısı tərəfindən informasiyanın nəzarət subyekti tərəfindən tələb edilən ehtiyat nüsxələrinin yaradılması, həmçinin təhlükəsizliyinin təmin edilməsi;

4.10.2.12. xidmətin göstərilməsi və ya xidmət istifadəsindən imtina zamanı nəzarət subyektinə məxsus olan konfiqurasiya fayllarının, ehtiyat nüsxələrin, mənbə kodu və digər həssas informasiyanın təqdim edilməsi, geri qaytarılması və “bulud” xidməti təchizatçısındakı informasiyanın bərpa edilmək imkanı olmadan silinməsi;

4.10.2.13. “bulud” xidməti təchizatçısı tərəfindən həyata keçirilən dəyişikliklər (məsələn, informasiya sistemləri və infrastruktur komponentləri üzrə dəyişikliklərin edilməsi, digər ölkə və ya regionda informasiyanın emalı və ya saxlanılması, submüqavilə çərçivəsində digər “bulud” xidməti təchizatçılarının xidmətlərindən istifadə edilməsi) barədə nəzarət subyektinə əvvəlcədən məlumat verilməsi;

4.10.2.14. fövqəladə hallarda “bulud” xidməti təchizatçısı tərəfindən tətbiq edilən fəaliyyətinin davamlılığı tədbirlərinin nəzarət subyektinin fəaliyyətinin davamlılığı qaydalarına uyğun olması.

4.11. İnformasiya təhlükəsizliyi hadisələrinin kommunikasiyası daxil olmaqla informasiya təhlükəsizliyi insidentlərinin çevik, davamlı və effektiv idarə edilməsi məqsədilə nəzarət subyekti tərəfindən azı aşağıdakılar nəzərə alınmaqla informasiya təhlükəsizliyi insidentlərinin idarə edilməsi qaydaları hazırlanır və təsdiq edilir:

4.11.1. informasiya təhlükəsizliyi hadisələrinin idarə edilməsi prosesləri, müvafiq vəzifə və öhdəliklər, əlaqələndirici şəxs(lər) və zəruri kommunikasiya kanallarının müəyyən edilməsi;

4.11.2. informasiya təhlükəsizliyi hadisələrinin qiymətləndirilməsi və hadisənin informasiya təhlükəsizliyi insidenti olub-olmaması haqqında qərarın qəbul edilməsi;

4.11.3. informasiya təhlükəsizliyi insidentlərinə reaksiya çərçivəsində insidentlərin təsirinə məruz qalan bütün aktivlərin əhatə edilməsi, zəruri sübutların əldə edilməsi, maraqlı tərəflərin ehtiyaclarına uyğun kommunikasiyanın və kök-səbəb təhlilinə əsaslanan sənədləşdirilmiş prosedurların tətbiq edilməsi;

4.11.4. informasiya təhlükəsizliyi hadisələri və insidentlər barədə məlumatlandırmanın müvafiq kommunikasiya kanalları vasitəsilə dərhal həyata keçirilməsi;

4.11.5. personal və təchizatçılar tərəfindən aşkar edilən və ya şübhələnilən informasiya təhlükəsizliyi hadisələri barədə əlaqələndirici şəxs(lər)ə məlumatın verilməsi və əldə edilən məlumatların qeydiyyatı prosesinin müəyyən edilməsi;

4.11.6. informasiya təhlükəsizliyi insidentləri üzrə azı aşağıdakıları əhatə edən tədbirlərin görülməsi:

4.11.6.1. insident baş verdiyi andan dəlillərin yığılması;

4.11.6.2. insidentin qeydiyyatının aparılması və kommunikasiyası;

4.11.6.3. insidentin risk əsaslı qiymətləndirilməsi, azı aşağıdakı meyarlar üzrə prioritetləşdirilməsi və kateqoriyalaşdırılması:

4.11.6.3.1. aşağı - insident nəticəsində nəzarət subyekti bir biznes proses üzrə fəaliyyətini qeyri-effektiv şəkildə həyata keçirməyə davam edir;

4.11.6.3.2. orta - insident nəticəsində nəzarət subyekti bir neçə biznes proses üzrə fəaliyyətini həyata keçirə bilmir;

4.11.6.3.3. yüksək - insident nəticəsində nəzarət subyekti hər hansı kritik biznes proses üzrə fəaliyyətini həyata keçirə bilmir;

4.11.6.4. insidentin aradan qaldırılması məqsədilə görüləcək tədbirlərin siyahısının formalaşdırılması və icrasına nəzarət edilməsi;

4.11.6.5. insident aradan qaldırıldıqdan sonra insidentin bağlanması və hesabatlılığının aparılması;

4.11.6.6. insidentlər barədə məlumatlandırma vasitələrinin (elektron poçt, xüsusi təyinatlı informasiya sistemi, telefon zəngi və s.) təyin edilməsi;

4.11.7. insidentlərin analizi və həll edilməsi nəticəsində insidentlərin gələcəkdə baş vermə ehtimalının və təsirinin azaldılması məqsədilə bilik bazasının formalaşdırılması və istifadə edilməsi;

4.11.8. insidentlərin idarə edilməsinə cəlb edilən əməkdaşların bu sahədə zəruri bilik və bacarıqlarının artırılması.

4.12. Nəzarət subyektində informasiya sistemlərinin və informasiya texnologiyalarının zədələndiyi, sıradan çıxdığı və ya təhlükəyə məruz qaldığı hallarda informasiya təhlükəsizliyi və fəaliyyətin davamlılığı təmin edilir. Kritik informasiya sisteminin fəaliyyətinin davamlılığını təmin etmək üçün azı aşağıdakı tədbirlər görülür:

4.12.1. biznesə təsir analizi aparılır, biznes prosesləri kritiklik səviyyəsi üzrə təsnifləşdirilir, kritik informasiya sistemi və əlaqəli aktivlər müəyyən edilir;

4.12.2. müəyyən edilmiş kritik informasiya sistemi üzrə baş vermiş fövqəladə hallar zamanı informasiya təhlükəsizliyi və fəaliyyətinin davamlılığının lazımi səviyyəsini təmin etmək məqsədilə proseslər təyin edilir, sənədləşdirilir, tətbiq edilir və aktuallığı təmin edilir;

4.12.3. fəaliyyətin davamlılığına təsir edən risklərə adekvat reaksiyanın verilməsi üzrə zəruri bilik və bacarığa malik personalın mövcudluğu təmin edilməklə zəruri planlama həyata keçirilir;

4.12.4. fəaliyyətin davamlılığını təmin etmək məqsədilə nəzarət subyektinin Azərbaycan Respublikasının bir-biri ilə qonşu olmayan iqtisadi rayonlarında yerləşən 2 (iki) informasiyanın işlənməsi mərkəzinin (əsas və ehtiyat mərkəz) olması təmin edilir;

4.12.5. azı aşağıdakıları nəzərdə tutan fövqəladə hallarda fəaliyyətin davamlılığı və bərpası plan(lar)ı hazırlanır və sənədləşdirilir:

4.12.5.1. fövqəladə halların biznes proseslərə təsir səviyyəsi üzrə təsnifləşdirilməsi;

4.12.5.2. fövqəladə hallar zamanı fəaliyyətin bərpa edilməsi üçün məsul şəxslərin siyahısı və səlahiyyətləri;

4.12.5.3. fövqəladə hallarda informasiya mübadiləsinin təşkilində istifadə olunan kritik informasiya sistemləri və texnologiyalarının siyahısı, onlar arasında əlaqə üzrə məntiqi və fiziki topoloji diaqramlar;

4.12.5.4. fövqəladə halın baş verməsi nəticəsində informasiya sistemində bərpa edilməsi mümkün olmayan məlumat itkisinin məqbul hesab edilən zaman göstəricisi;

4.12.5.5. fövqəladə halın baş verməsindən sonra biznes prosesə xidmət edən informasiya sisteminin bərpa edilməsi üçün tələb olunan müddət;

4.12.5.6. mümkün ssenarilər əsasında fövqəladə hallarda yarana biləcək dayanma zamanı mövcud olacaq risklərin qarşısının alınması üzrə tədbirlər;

4.12.5.7. fövqəladə hallar zamanı kommunikasiya tədbirləri;

4.12.5.8. informasiya sistemləri və (və ya) ehtiyatlarının saxlanılması üçün üçüncü tərəf xidmət təchizatçılarının xidmətlərindən istifadə edildiyi halda fəaliyyətin davamlılığının təmin edilməsi üzrə tədbirlər.

4.13. Nəzarət subyekti fövqəlaqə hallarda fəaliyyətinin davamlılığını təmin etmək məqsədilə kritik informasiya sistemlərinin və əlaqəli aktivlərin etibarlı, təhlükəsiz və davamlı fəaliyyətini ehtiyat mərkəzdən təmin edir.

4.14. Fövqəladə hallarda fəaliyyətin davamlılığı və bərpası planı ehtiyat mərkəz üzərindən müxtəlif ssenarilər əsasında ildə azı 2 (iki) dəfə sınaqdan keçirilir, nəticələri sənədləşdirilir və sınağın nəticəsi uğursuz olduqda nəzarət subyekti növbəti 2 (iki) ay ərzində yenidən ehtiyat mərkəz vasitəsilə sınaq yoxlaması aparır və nəticəsi sənədləşdirilir.

4.15. Nəzarət subyekti fövqəladə hallarda fəaliyyətin davamlılığını təmin etmək üçün sorğuların cavablandırılması və məlumat mübadiləsinin aparılmasına məsul əməkdaşları (əsas və əvəzedici şəxslər) təyin edərək onları təlimatlandırır.

4.16. Fövqəladə hallarda fəaliyyətin davamlılığını və bərpasını təmin etmək məqsədilə əlaqədar işçilər üçün ildə 2 (iki) dəfədən az olmayaraq təlimlər keçirilir və nəticələri sənədləşdirilir.

4.17. Əqli mülkiyyət hüquqlarının mühafizəsi məqsədilə qanunvericiliyin tələbləri nəzərə alınaraq düzgün istifadə qaydaları tətbiq edilir, informasiya sistemləri və proqram

təminatları lisenziya şərtlərinə uyğun olaraq istismar edilərək nüsxələrinin icazəsiz yayımlanması məhdudlaşdırılır.

4.18. Məlumatların saxlanılması, arxivləşdirilməsi, itirilməsinin qarşısının alınması, məhv edilməsi, həmçinin icazəsiz dəyişdirilməsi ilə əlaqədar qanunvericiliyin tələbləri və informasiyanın təsnifatı nəzərə alınaraq məlumatların saxlanılması, arxivləşdirilməsi və məhv edilməsini əhatə edən nəzarət tədbirləri müəyyən edilir.

4.19. Nəzarət subyektinin kritik informasiya sistemində planlaşdırılmamış fasilələr və (və ya) əhəmiyyətli dəyişikliklər baş verdikdə, habelə yüksək kateqoriyalı insidentin baş verməsi halında müvafiq sistem üzrə daxili və ya kənar audit həyata keçirilərək nəticələri sənədləşdirilir.

4.20. İnformasiya texnologiyalarının düzgün və təhlükəsiz fəaliyyətini təmin etmək məqsədilə əməliyyat prosedurları azı aşağıdakıları əhatə edərək sənədləşdirilir və müvafiq işçilər üçün əlçatanlığı təmin edilir:

4.20.1. proqram təminatlarının yüklənməsi və quraşdırılması;

4.20.2. digər proqram təminatları ilə qarşılıqlı inteqrasiya əlaqələri;

4.20.3. xətaların idarə edilməsi;

4.20.4. proqram təminatlarının dəstəklənməsi üzrə əlaqələndirici şəxslərlə kommunikasiya planları;

4.20.5. fövqəladə hallar zamanı proqram təminatlarının bərpası;

4.20.6. audit izi və loqların qeydiyyatının həyata keçirilməsi;

4.20.7. monitorinq prosedurları.

5. İnsan resursları üzrə nəzarət tədbirləri

5.1. Nəzarət subyekti personalın və aktivlərə giriş hüququ olan təchizatçıların fəaliyyətə başlamazdan əvvəl informasiya təhlükəsizliyi sahəsində onlar üçün nəzərdə tutulmuş vəzifələrə uyğun olmalarını təmin etmək məqsədilə aşağıdakı tədbirləri həyata keçirir:

5.1.1. biznes tələblərinə, giriş əldə edilən informasiyanın təsnifatına və proqnozlaşdırılan risklərə adekvat olaraq namizədlərin uyğunluğunu müəyyən edir;

5.1.2. bağlanmış müqavilələr və nəzarət subyektinin daxili sənədləri ilə onların və nəzarət subyektinin informasiya təhlükəsizliyi üzrə öhdəliklərini müəyyənləşdirir.

5.2. Nəzarət subyekti personal və aktivlərə giriş hüququ olan təchizatçıların, habelə müştərilərin informasiya təhlükəsizliyi ilə bağlı öz öhdəliklərini bilməsini, yerinə yetirməsini, habelə maariflənməsini təmin etmək məqsədilə aşağıdakı tədbirləri həyata keçirir:

5.2.1. personalın və təchizatçıların informasiya təhlükəsizliyi siyasəti və müvafiq qaydalara uyğun olaraq informasiya təhlükəsizliyi tələblərinə riayət etməsini tələb edir;

5.2.2. personalı informasiya təhlükəsizliyi siyasəti və onların funksiyalarına uyğun olan qaydalarla bağlı azı ildə 2 (iki) dəfə və müvafiq sənədlərdə dəyişikliklər edildikdə növbədənkənar qaydada təlimlərə cəlb edir, habelə informasiya təhlükəsizliyi ilə əlaqədar azı ildə 4 (dörd) dəfə maarifləndirir;

5.2.3. təchizatçıları informasiya təhlükəsizliyi tələbləri ilə əlaqədar azı ildə 2 (iki) dəfə, habelə dəyişiklik edildikdə növbədənkənar qaydada məlumatlandırır;

5.2.4. müştəriləri informasiya təhlükəsizliyi ilə əlaqədar azı rübdə bir dəfə maarifləndirir;

5.2.5. informasiya təhlükəsizliyinə dair personal üçün təlim proqramları nəzarət subyektinin icra orqanının rəhbəri tərəfindən təsdiq edilir və icrasına nəzarət edilir;

5.2.6. nəzarət subyektinin qaydalarında informasiya təhlükəsizliyi tələblərini pozan personala qarşı qanunvericiliyə müvafiq qaydada məsuliyyət tədbirləri müəyyən edilir.

5.3. Personal və aktivlərə giriş hüququ olan təchizatçılarla müqavilə münasibətlərinə xitam verilməsindən və ya dəyişdirilməsindən sonrakı dövr üçün informasiya təhlükəsizliyi üzrə öhdəliklər müəyyən edilir.

5.4. Personal və təchizatçılara informasiya və digər əlaqəli aktivlərə giriş hüququ verilən zaman informasiyanın qorunması və icazəsiz kənar şəxslərə açıqlanmasının qarşısının alınması məqsədilə azı aşağıdakıları nəzərdə tutan razılaşma formaları hazırlanır və tərəflər arasında imzalanır:

5.4.1. həssas informasiyanın əhatə dairəsi;

5.4.2. razılaşmanın qüvvədə olma müddəti;

5.4.3. informasiyanın icazəsiz açıqlanmasına görə tərəflərin məsuliyyəti;

5.4.4. informasiya və digər əlaqəli aktivlər üzərində sahiblik hüquqları;

5.4.5. informasiya və digər əlaqəli aktivlərdən istifadənin monitorinqi və uyğunsuzluq hallarında görüləcək tədbirlər;

5.4.6. təqdim edilmiş informasiya və digər əlaqəli aktivlərin geri qaytarılması və ya məhv edilməsi qaydası.

5.5. Personalın məsafədən işləməsi zamanı nəzarət subyektinin olduğu yerdən kənarda giriş edilən, emal edilən və saxlanılan informasiyanın təhlükəsizliyinin təmin edilməsi üçün azı aşağıdakıları nəzərdə tutan qaydalar hazırlanır, təsdiq edilir və personalla kommunikasiya edilir:

5.5.1. məsafədən iş zamanı fiziki təhlükəsizlik tələbləri;

5.5.2. informasiya mübadiləsinin təhlükəsiz təşkili ilə bağlı tələblər;

5.5.3. məsafədən işi təmin edən texnologiyalardan təhlükəsiz istifadə tələbləri;

5.5.4. ev və digər ictimai internet şəbəkələrindən istifadə ilə bağlı tələblər;

5.5.5. əməliyyat sistemi və proqram təminatları üzrə ən son yenilənmələrin tətbiqi ilə bağlı tələblər;

5.5.6. zərərverici proqram təminatlarına qarşı mühafizənin təşkili ilə bağlı tələblər.

5.6. Personal tərəfindən aşkarlanan və ya şübhələnilən informasiya təhlükəsizliyi hadisələri barədə vaxtında daxili məlumatlandırmanın təmin edilməsi üçün azı aşağıdakıları nəzərdə tutan mexanizm formalaşdırılır:

5.6.1. personalın mümkün olan ən qısa müddətdə informasiya təhlükəsizliyi hadisəsi barədə məlumat verməsi barədə öhdəliyinin mövcudluğu;

5.6.2. informasiya təhlükəsizliyi hadisələri barədə məlumatın təqdim edildiyi əlaqələndirici şəxs(lər)in müəyyən ediməsi;

5.6.3. informasiya təhlükəsizliyi hadisələri barədə məlumat vermə prosedurunun olması.

5.7. İnformasiya təhlükəsizliyi hadisəsi üzrə məlumatla bağlı nəzərə alınan hallara aşağıdakılar daxildir:

5.7.1. informasiyanın konfidensiallığı, tamlığı və əlçatanlığının pozulması halları;

5.7.2. qeyri-effektiv təhlükəsizlik tədbirləri;

5.7.3. insan xətaları;

5.7.4. informasiya təhlükəsizliyi siyasəti və müvafiq qaydalar ilə uyğunsuzluq halları;

5.7.5. avadanlıq və proqram təminatının funksiyasının pozulması və ya fəaliyyətində müşahidə edilən digər uyğunsuzluqlar və çatışmazlıqlar;

5.7.6. giriş pozuntuları;

5.7.7. zəifliklər və şübhələnilən zərərli proqram təminatlarına yoluxma halları.

6. Fiziki təhlükəsizlik üzrə nəzarət tədbirləri

6.1. Nəzarət subyektində informasiya və digər əlaqəli aktivlərə icazəsiz fiziki giriş, zədə və müdaxilənin qarşısının alınması məqsədilə onların saxlanıldığı məkanların mühafizəsi azı aşağıdakı tələblər nəzərə alınmaqla təmin edilir:

6.1.1. əhatə etdiyi aktivlərlə bağlı informasiya təhlükəsizliyi tələblərinə uyğun olaraq təhlükəsizlik perimetrləri və hər bir perimetrin yerləşdiyi məkan və dayanıqlılıq tələbləri müəyyən edilir;

6.1.2. təhlükəsizlik perimetrlərində işləmə üzrə müvafiq prosedurlar formalaşdırılır;

6.1.3. aktuallığı təmin edilməklə giriş icazəsi olan səlahiyyətli şəxslərin siyahısı tərtib edilir;

6.1.4. təhlükəsizlik perimetrlərinə yalnız icazəsi olan şəxslərin daxil olması üçün müvafiq giriş nəzarət mexanizmləri tətbiq edilir;

6.1.5. icazəsiz şəxslərin daxil ola biləcəyi giriş sahələri (yükləmə və boşaltma sahələri) və digər oxşar sahələrə nəzarət edilir, habelə mümkün olduqda icazəsiz giriş hallarının qarşısının alınması üçün həmin sahələr informasiya texnologiyalarından təcrid edilir.

6.2. Nəzarət subyektində informasiyaya və digər əlaqəli aktivlərə icazəsiz girişin, zədənin və müdaxilənin qarşısını almaq məqsədilə ofis, otaq və avadanlıqların mühafizəsi ilə bağlı qaydalar hazırlanır və təsdiq edilir.

6.3. İcazəsiz fiziki girişlərin aşkar edilməsi və qarşısının alınması məqsədilə sahələrin və binaların müşahidə kameraları vasitəsilə fasiləsiz monitorinqi təmin edilir.

6.4. Təbii fəlakətlər və digər fiziki təhdidlərlə bağlı risk qiymətləndirilməsi aparılır və ərazinin coğrafi xüsusiyyətləri, insan həyatına təhlükə yaradan amillər nəzərə alınmaqla mühafizə tədbirləri müəyyən edilir.

6.5. İnformasiyanın işlənməsi mərkəzinin (server otağının) bu Tələblərin 6.1-6.4-cü bəndlərinin tələblərinə əlavə olaraq azı aşağıdakı tələblərə də cavab verməsi təmin edilir:

6.5.1. müşahidə kameraları tərəfindən qeydə alınan görüntülər ən azı 6 (altı) ay müddətində qeydə alındığı binada, habelə bu görüntülərin ehtiyat nüsxələri qeydə alındığı binadan kənarda saxlanır;

6.5.2. pəncərəsiz olması təmin edilir, bu mümkün olmadıqda, pəncərə zirehli şüşə və dəmir barmaqlıqlarla təchiz edilir;

6.5.3. germetik olması təmin edilir;

6.5.4. qapıların zərbəyə, odadavamlı olması təmin edilir;

6.5.5. temperaturun tənzimlənməsi üçün termometr, havalandırma və soyutma sistemləri ilə təchiz edilir;

6.5.6. mühafizə və yanğın-siqnalizasiya sistemləri ilə təchiz edilir;

6.5.7. avtomatlaşdırılmış yanğınsöndürmə sistemləri ilə təchiz edilir;

6.5.8. rütubətliliyi ölçən və tənzimləyən avadanlıqlar ilə təchiz edilir;

6.5.9. hərəkət detektorları ilə təchiz edilir;

6.5.10. fasiləsiz elektrik enerjisi ilə təmin edən qida mənbəyi və generator ilə təchiz edilir.

6.6. Ödəniş kartları vasitəsilə aparılmış əməliyyatlar haqqında məlumatların toplanması, emalı və ötürülməsinə, həmçinin kart emissiyasına və ekvayrinqinə texniki xidmət göstərilməsi üzrə fəaliyyəti həyata keçirən ödəniş sistemlərinin operatorlarında və banklarda ödəniş kartının personalizasiyası, saxlanılması (anbar otağı), təhvil verilməsi, PİN-zərflərin çapı üçün nəzərdə tutulmuş iş sahələrinin (otaqların) bu Tələblərin 6.1-6.5-ci bəndlərinin tələblərinə uyğun olması və personalizasiya otaqlarında yalnız personalizasiya fəaliyyətinin həyata keçirilməsi təmin edilir.

6.7. Bankomatların və onların yerləşdiyi ərazilərin azı aşağıdakı tələblərə cavab verməsi təmin edilir:

6.7.1. bankomatda istifadəçinin üz təsvirini aydın çəkməyə imkan verən azı bir ədəd müşahidə kamerası quraşdırılır və qeydə alınan görüntülər müvafiq nəzarət subyektində azı 6 (altı) ay müddətində saxlanılır;

6.7.2. bankomat tərəfindən video müşahidənin aparılması barədə istifadəçinin görə biləcəyi yerdə asan oxunan və aydın şəkildə görünən xəbərdarlıq bildirişi yerləşdirilir;

6.7.3. bankomatın oxuyucu qurğusuna kənardan müdaxilə edilməsinin qarşısını alan xüsusi avadanlıq quraşdırılır;

6.7.4. daxili proqram təminatının bu Tələblərin 7-ci hissəsində nəzərdə tutulan müvafiq tələblərə cavab verməsi təmin edilir;

6.7.5. qlobal məsafədən mövqe təyinetmə (GPS) və mühafizə siqnalizasiya sistemi ilə təchiz edilir;

6.7.6. açıq ərazilərdə quraşdırılmış bankomatın qarşısındakı (və ya ətrafındakı) 2 (iki) metrdən az olmayan ərazinin sutkanın qaranlıq vaxtı aydın şəkildə işıqlandırılması təmin edilir.

6.8. Kağız və digər informasiya daşıyıcıları üçün azı aşağıdakılar nəzərə alınmaqla təmiz masa və təmiz ekran qaydası qəbul edilir və personalla kommunikasiya edilir:

6.8.1. həssas informasiya və əlaqəli informasiya texnologiyaları mühafizə edilən sahələrdə saxlanılır;

6.8.2. kompüter avadanlıqlarından istifadə başa çatdırıldıqda avadanlığa giriş məhdudlaşdırılır və yenidən istifadə üçün müvafiq şifrə, token və digər istifadəçi autentikasiya üsulu tətbiq edilir.

6.9. İnformasiya və digər əlaqəli aktivlərin nəzarət subyektinin ərazisindən kənarda istifadəsi ilə bağlı yarana biləcək risklər nəzərə alınmaqla müvafiq təhlükəsizlik tədbirləri tətbiq edilir.

6.10. Elektrik və telekommunikasiya xətlərinin kəsilməzliyi, bu xətlərin fərqli kanallarla aparılması, elektrik və telekommunikasiya xətləri qovşaqlarının mühafizə edilməsi, onların yerləşdiyi otaqlara girişə nəzarət edilməsi, habelə kənar müdaxilələrdən və zədələnmələrdən qorunması təmin edilir.

6.11. Avadanlıqların elektrik enerjisinin kəsilməsi və dəstəkləyici vasitələrdə (fasiləsiz qida mənbələri, elektrik enerjisi, havalandırma və s.) baş verə biləcək nasazlıqlar nəticəsində yaranan fasilələrdən azı aşağıdakılar nəzərə alınmaqla qorunması təmin edilir:

6.11.1. dəstəkləyici avadanlıqların istehsalçının təlimatlarına uyğun olaraq sazlanması, istifadəsi, dəstəklənməsi təmin edilir;

6.11.2. dəstəkləyici avadanlıqların mütəmadi olaraq nəzarət subyektinin tələbatına cavab verməsi təmin edilir;

6.11.3. düzgün işləməsinin yoxlanılması məqsədilə dəstəkləyici avadanlıqlar azı ildə 2 (iki) dəfə sınaqdan keçirilir və nəticələr sənədləşdirilir;

6.11.4. dəstəkləyici avadanlıqlar informasiya prosesini icra edən avadanlıqlardan fərqli şəbəkə seqmentində yerləşdirilir və yalnız zəruri hallarda internetə qoşulması təmin edilir.

6.12. Avadanlıqların etibarlı və davamlı fəaliyyəti üçün onlara adekvat dəstəkləmə xidməti göstərilir.

6.13. İnformasiya və digər əlaqəli aktivlərin razılaşdırılmadan nəzarət subyektinin ərazisindən kənara çıxarılmaması təmin edilir.

6.14. İnformasiya daşıyıcıları olan avadanlıqlar məhv edilməzdən və ya yenidən istifadəyə verilməzdən öncə saxlanılan həssas informasiya və lisenziyalı proqram təminatları bərpası mümkün olmayacaq qaydada silinir. Avadanlıqların fiziki məhv edilməsi qaydası qəbul edilir, məhvetmə xüsusi texnologiyalardan istifadə etməklə həyata keçirilərək sənədləşdirilir.

6.15. Personal istifadə etdiyi avadanlıqları nəzarətsiz saxladığı müddətdə onların adekvat təhlükəsizliyinin təmin edildiyinə əmin olur. Bütün personal mühafizənin təmin edilməsi ilə bağlı qaydalar, habelə öhdəlikləri barədə məlumatlandırılır.

7. Texnoloji nəzarət tədbirləri

7.1. Son istifadəçi cihazları vasitəsilə saxlanılan, emal edilən və əlçatan olan informasiyanın təhlükəsizliyini təmin etmək məqsədilə son istifadəçi cihazlarının təhlükəsiz konfiqurasiyası və idarə edilməsi üçün azı aşağıdakılar nəzərə alınmaqla qaydalar qəbul edilir və personalla kommunikasiya edilir:

7.1.1. son istifadəçi cihazlarının idarə edə, emal edə, saxlaya və ya dəstəkləyə biləcəyi informasiyanın növü və təsnifat səviyyəsi;

7.1.2. son istifadəçi cihazlarının qeydiyyatı;

7.1.3. fiziki mühafizə ilə bağlı tələblər;

7.1.4. proqram təminatlarının quraşdırılmasında məhdudiyyət;

7.1.5. son istifadəçi cihazlarında əməliyyat sistemləri, proqram təminatları və ən son yenilənmələrlə bağlı tələblər;

7.1.6. girişlərə nəzarət;

7.1.7. informasiyanın növü və təsnifat səviyyəsinə müvafiq olaraq son istifadəçi cihazlarının yaddaş qurğularının şifrələnməsi və ehtiyat nüsxələrinin formalaşdırılması;

7.1.8. zərərverici proqram təminatlarına qarşı mühafizə;

7.1.9. ev və digər ictimai internet şəbəkələrinə qoşulma qaydası.

7.2. İnformasiya və digər əlaqəli aktivlərə giriş icazələrinin azı aşağıdakılar nəzərə alınmaqla məhdudlaşdırılması təmin edilir:

7.2.1. həssas informasiyaya anonim girişlərin qarşısı alınması;

7.2.2. fərdin və ya fərdlər qruplarının xüsusi girişi olan (oxumaq, yazmaq, silmək, icra etmək və s.) informasiyanın müəyyən edilməsi, səlahiyyətlərin təyin edilməsi;

7.2.3. həssas informasiyanın izolyasiya edilməsi.

7.3. Mənbə koduna, inkişaf alətlərinə və proqram təminatı kitabxanalarına oxumaq və yazmaq giriş hüquqları azı aşağıdakılar nəzərə alınmaqla idarə edilir:

7.3.1. müəyyən edilmiş qaydalara uyğun olaraq proqramın mənbə koduna və proqram təminatı kitabxanalarına giriş hüquqlarının idarə edilməsi;

7.3.2. biznes ehtiyacları əsasında, habelə dəyişiklik və ya sui-istifadə risklərini idarə etmək məqsədilə müəyyən edilmiş qaydalara uyğun olaraq mənbə koduna oxumaq və yazmaq giriş hüququnun verilməsi;

7.3.3. dəyişikliklərə nəzarət qaydalarına uyğun olaraq mənbə kodunun və əlaqəli elementlərinin yenilənməsi və mənbə koduna giriş hüququnun verilməsi;

7.3.4. proqram siyahılarının oxumaq və yazmaq giriş hüquqlarının idarə edildiyi və təyin edildiyi təhlükəsiz mühitdə saxlanılması;

7.3.5. mənbə koduna edilən bütün giriş və dəyişikliklərin loqlanması.

7.4. İnformasiyaya giriş qaydaları əsasında azı aşağıdakılar nəzərə alınmaqla təhlükəsiz autentikasiya texnologiyaları və prosesləri tətbiq edilir:

7.4.1. autentikasiya prosesi uğurla yekunlaşana qədər giriş verilmiş həssas informasiyanın göstərilməməsi;

7.4.2. yalnız icazə verilmiş şəxslərin daxil ola biləcəyi barədə ümumi xəbərdarlığın göstərilməsi;

7.4.3. autentikasiya üçün yalnız bütün məlumatlar daxil edildikdən sonra onların etibarlılığının təsdiq edilməsi;

7.4.4. istifadəçi adları və şifrələrin "brute-force" hücumdan qorunma metodlarının tətbiq edilməsi;

7.4.5. uğurlu və uğursuz giriş cəhdlərinin loqlanması;

7.4.6. uğurlu giriş tamamlandıqdan sonra aşağıdakı məlumatların göstərilməsi:

7.4.6.1. əvvəlki uğurlu girişin tarixi və saatı;

7.4.6.2. son uğurlu girişdən sonra baş verən uğursuz giriş cəhdlərinin təfərrüatları.

7.4.7. daxil edilən şifrənin göstərilməməsi və şəbəkə üzərindən açıq mətn formasında ötürülməməsi;

7.4.8. müəyyən edilmiş müddət ərzində heç bir fəaliyyət olmadığı təqdirdə sistemlə qurulmuş əlaqələrin başa çatdırılması.

7.5. İmtiyazlı giriş hüquqları azı aşağıdakı mühafizə tədbirləri və 7.4-cü bəndin tələbləri nəzərə alınmaqla yalnız icazə verilmiş personala, proqram təminatı komponentlərinə və servislərə verilməlidir:

7.5.1. imtiyazlı giriş hüquqlarının yalnız ehtiyac yarandığı təqdirdə verilməsi və adi giriş hüquqlarından daha yüksək autentikasiya tələblərinin tətbiq edilməsi;

7.5.2. hər bir sistem və proses üçün imtiyazlı giriş hüququ tələb edən personalın müəyyənləşdirilməsi, qeydiyyatının aparılması və imtiyazlı giriş hüquqlarından istifadə müddətinin təyin edilməsi;

7.5.3. imtiyazlı istifadəçilərin yalnız onlara aid imtiyazlı hesablardan istifadə etməsinin, habelə imtiyazlı hesabların gündəlik istifadəçi hesablarından ayrılmasının təmin edilməsi;

7.5.4. imtiyazlı giriş hüququ olan personalın hərəkətlərinin monitorinqi və loqlanması.

7.6. İnformasiya və informasiya texnologiyalarının zərərverici proqram təminatlarından mühafizəsi personalın məlumatlandırılması ilə birgə həyata keçirilir və bu zaman azı aşağıdakılar nəzərə alınır:

7.6.1. icazə verilməmiş proqram təminatlarından istifadənin aşkarlanması və qarşısının alınması;

7.6.2. bilinən və şübhələnilən zərərverici internet səhifələrindən istifadənin müəyyən edilməsi və qarşısının alınması;

7.6.3. zərərverici proqram təminatından mühafizə vasitələrinin yalnız lisenziya əldə edilməklə tətbiq edilməsi;

7.6.4. zərərverici proqram təminatlarından mühafizə vasitələrinin tətbiq edilməsi;

7.6.5. zərərverici proqram təminatından mühafizə vasitələrinin mərkəzləşdirilmiş qaydada idarə edilməsi;

7.6.6. zərərverici proqram təminatından mühafizə vasitələrinin quraşdırılması, sazlanması, yoxlanılması, dəstəklənməsi və monitorinqinin icazə verilmiş şəxslər tərəfindən həyata keçirilməsi;

7.6.7. zərərverici proqram təminatından mühafizə vasitələrinin bazalarının avtomatik olaraq ən son yenilənmələrlə təmin edilməsi;

7.6.8. zərərverici proqram təminatından mühafizə vasitələri tərəfindən azı aşağıdakı yoxlamaların həyata keçirilməsi:

7.6.8.1. şəbəkə və ya istənilən yaddaş qurğuları vasitəsilə qəbul edilən informasiyanın istifadədən əvvəl yoxlanılması;

7.6.8.2. elektron məktublardakı və ani mesajlaşma proqram təminatlarındakı qoşmaların istifadədən əvvəl yoxlanılması;

7.6.8.3. internet səhifələrin yoxlanılması;

7.6.9. zərərverici proqram təminatlarına bütün yoluxma faktlarının qeydə alınması, habelə onların növləri və yoluxma mənbələri göstərilməklə hesabatlılığının aparılması.

7.7. Həssas informasiyanın silinməsi prosesi çərçivəsində müvafiq silinmə metodunun (məsələn, elektron şəkildə üzərinə yazılma, kriptoqrafik silinmə və s.) seçilməsi və silinmənin nəticələrinin sübut qismində saxlanılması təmin edilir, habelə kənar təchizatçıların, o cümlədən "bulud" xidməti təchizatçılarının xidmətlərindən istifadə edildikdə təchizatçı tərəfindən tətbiq edilən silinmə metodlarının məqsədəuyğunluğu yoxlanılır və silinmənin sübutları tələb edilir.

7.8. İnformasiya itkisinin qarşısının alınması məqsədilə kritik informasiya sistemlərinin ehtiyat nüsxələrinin yaradılması, həmçinin bərpa prosesinin testləşdirilməsi üzrə azı aşağıdakıları əhatə edən qaydalar qəbul edilir və tətbiqi təmin edilir:

7.8.1. ehtiyat nüsxələrin yaradılması və bərpası məqsədilə vəzifələr və bu vəzifələr üzrə öhdəlik və səlahiyyətlərin müəyyən edilməsi;

7.8.2. ehtiyat nüsxələrin yaradılması vasitələrinin mərkəzləşdirilmiş qaydada idarə edilməsi;

7.8.3. həssas informasiyanın ehtiyat nüsxələrinin şifrələnmiş şəkildə saxlanılmasının təmin edilməsi;

7.8.4. nəzarət subyektinin biznes ehtiyacları, informasiya təhlükəsizliyi tələbləri və informasiya sistemlərinin kritikliyi nəzərə alınmaqla ehtiyat nüsxələrinin əhatə dairəsi (məsələn, qismən, differensial və (və ya) tam ehtiyat nüsxə) və yaradılma tezliyinin müəyyən edilməsi;

7.8.5. ehtiyat nüsxələrin arxivləşdirilməsi ilə bağlı qanunvericiliklə müəyyən edilən müddətdə və qaydada saxlanılması və saxlanma müddəti başa çatdıqdan sonra silinməsinin təmin edilməsi;

7.8.6. ehtiyat nüsxələrin ildə 2 (iki) dəfədən az olmamaqla sınaq bərpasının həyata keçirilməsi və nəticələrinin sənədləşdirilməsi;

7.8.7. ehtiyat nüsxələrin yaradılması üzrə loqların qeydiyyatının aparılması.

7.9. Fəaliyyətlər, istisnalar, xətalar və digər hadisələr üzrə loqların yaradılması, saxlanılması, mühafizəsi və təhlilinin təmin edilməsi üçün qaydalar qəbul edilir. Kritik informasiya sistemləri və digər əlaqəli aktivlər üzrə hadisələrin loqlanması zamanı azı aşağıdakılar nəzərə alınır:

7.9.1. hadisə loqlarının qeydiyyatı aparılır və azı 1 (bir) il müddətinə saxlanılmaqla mütəmadi olaraq monitorinq edilir. Qeydiyyatı aparılan loqlara azı aşağıdakılar daxildir:

7.9.1.1. xəbərdarlıq loqları – qeyri-adi fəaliyyət və baş verə biləcək nasazlıqları özündə əks etdirən loqlar;

7.9.1.2. xətalar üzrə loqlar – dayanmaları və ya sıradan çıxmaları əks etdirən loqlar;

7.9.1.3. kritik loqlar – sistem uğursuzluğunun qarşısını almaq üçün müdaxilənin edilməsini tələb edən kritik hadisələri özündə əks etdirən loqlar;

7.9.2. hər bir hadisə loqu özündə azı aşağıdakı məlumatları saxlayır:

7.9.2.1. istifadəçi identifikatoru;

7.9.2.2. hadisənin baş vermə tarixi, vaxtı və təfərrüatları (giriş, çıxış və s.);

7.9.2.3. hadisənin statusu və (və ya) xətanın kodu;

7.9.2.4. uğurlu və uğursuz giriş cəhdləri;

7.9.2.5. sistem konfiqurasiyasına dəyişikliklər;

7.9.2.6. giriş edilmiş fayllar və giriş növü;

7.9.2.7. şəbəkə ünvanları və protokolları;

7.9.2.8. mühafizə sistemlərinin aktivləşdirilməsi və deaktivləşdirilməsi;

7.9.2.9. proqram təminatında həyata keçirilən əməliyyatlar;

7.9.3. loqların qeydiyyatı vasitələrinin və loq məlumatlarının dəyişdirilməyə və icazəsiz girişlərə qarşı müdafiəsi təmin edilir;

7.9.4. imtiyazlı giriş hüququna malik olanlar da daxil olmaqla istifadəçilərin öz fəaliyyətləri barədə loqları silməsi və ya deaktivasiya etməsi qadağan edilir.

7.10. İnformasiya sistemlərinin və digər əlaqəli aktivlərin vahid zaman mənbəyi ilə sinxronlaşdırılması təmin edilir və əlaqələndirmə üçün standart istinad vaxtı müəyyən edilir.

7.11. Şəbəkələrdə və şəbəkə avadanlıqlarında informasiyanın qorunması məqsədilə azı aşağıdakı tələblər nəzərə alınır:

7.11.1. şəbəkə infrastrukturunun idarə edilməsi üzrə öhdəliklərin müəyyən edilməsi;

7.11.2. simsiz, üçüncü tərəfə məxsus və ya qlobal şəbəkələrdə ötürülən informasiyanın konfidensiallığının və tamlığının mühafizəsinin təmin edilməsi;

7.11.3. şəbəkə infrastrukturu üzrə şəbəkə diaqramlarının hazırlanması, aktuallığının təmin edilməsi, həmçinin avadanlıqların konfiqurasiya fayllarının saxlanılmasının təmin edilməsi;

7.11.4. bütün şəbəkə xidmətləri üzrə təhlükəsizlik mexanizmləri, xidmət səviyyələri və idarəetmə tələblərinin müəyyən edilməsi və şəbəkə xidmətlərinin göstərilməsi müqavilələrinə daxil edilməsi;

7.11.5. şəbəkədə istifadəçilərin və informasiya sistemlərinin, habelə şəbəkə idarəetmə kanallarının seqmentlər üzrə ayrılmasının təmin edilməsi;

7.11.6. avadanlıqların şəbəkəyə qoşulmasının aşkarlanması, məhdudlaşdırılması və autentikasiyasının həyata keçirilməsi.

7.12. Şəbəkə xidmətlərinin təhlükəsizlik mexanizmləri, xidmət səviyyələri və idarəetmə tələbləri üzrə azı aşağıdakıları nəzərdə tutan qaydalar müəyyən edilir və tətbiqi təmin edilir:

7.12.1. giriş icazəsi verilən şəbəkələr və şəbəkə xidmətlərinin dairəsi;

7.12.2. fərqli şəbəkə xidmətlərinə girişlər üçün autentikasiya tələbləri;

7.12.3. şəbəkəyə girişin mühafizəsi üçün şəbəkə idarəetməsi və texnoloji nəzarət tədbirləri (məsələn, autentikasiya, şifrələmə və s.) və prosedurları;

7.12.4. şəbəkə və şəbəkə xidmətlərinə giriş üçün istifadə edilən vasitələr (məsələn, virtual şəxsi şəbəkədən (VPN) istifadə və ya simsiz şəbəkə);

7.12.5. istifadəçinin giriş zamanı vaxt, yer və digər atributları.

7.13. Arzuolunmaz internet resurslarına girişlərə məhdudiyyətlər tətbiq edilir, habelə azı aşağıdakılar nəzərə alınmaqla bu resurslardan təhlükəsiz və düzgün istifadə qaydaları formalaşdırılır:

7.13.1. personalın giriş hüququnun olduğu və ya qadağan edildiyi internet resursları növlərinin müəyyən edilməsi;

7.13.2. aşağıdakı internet resurslarına girişlərin bloklanması:

7.13.2.1. zəruri biznes ehtiyacları üçün icazə verilənlər istisna olmaqla, informasiyanın internetə yüklənməsi funksiyası olan internet resursları;

7.13.2.2. bilinən və ya şübhələnilən zərərverici internet resursları (məsələn, zərərverici proqram və fişinq məzmunları yayan internet resursları);

7.13.2.3. qanunazidd məzmun yayan internet resursları;

7.13.3. nəzarət subyektinin sosial media hesablarının azı aşağıdakılar nəzərə alınmaqla təhlükəsizliyinin təmin edilməsi:

7.13.3.1. hər bir sosial media hesabı üçün autentikasiya məlumatlarının idarə edilməsi qaydalarına uyğun şifrənin təyin edilməsi;

7.13.3.2. iki faktorlu autentikasiyanın tətbiq edilməsi;

7.13.3.3. şifrələrin dövrü olaraq yenilənməsi;

7.13.3.4. sosial media hesabında fərdi təhlükəsizlik tənzimlənmələrinə baxılması və yenilənməsi;

7.13.3.5. sosial media hesabında həssas informasiyanın paylaşılmamasının nəzarətdə saxlanılması;

7.13.3.6. sosial media hesabının fəaliyyətinin mütəmadi monitorinq edilməsi;

7.13.3.7. paylaşılan və ya ümumi istifadədə olan son istifadəçi cihazlarından istifadənin məhdudlaşdırılması;

7.13.3.8. sosial media proqram təminatlarının və onların quraşdırıldığı son istifadəçi cihazlarının ən son yeniləmələrlə təmin edilməsi;

7.13.3.9. sosial media hesabına bağlı elektron poçt hesabının təhlükəsizliyinin təmin edilməsi;

7.13.3.10. sosial media hesabına bağlanmış son istifadə cihazlarının siyahıya alınması və dövri olaraq nəzərdən keçirilməsi.

7.14. Təhlükəsiz sistemlərin mühəndisliyi prinsipləri azı aşağıda göstərilənlər nəzərə alınmaqla formalaşdırılır və istənilən informasiya sisteminin inkişafı fəaliyyətinə tətbiq edilir:

7.14.1. "dərindən müdafiə" prinsipinin tətbiq edilməsi;

7.14.2. azı aşağıdakıları əhatə edən "sıfır etibar" prinsipinin tətbiq edilməsi:

7.14.2.1. informasiya təhlükəsizliyinin təmin edilməsi üzrə yalnız şəbəkə perimetri təhlükəsizliyinə etibar edilməməsi;

7.14.2.2. informasiya sistemlərinə daxil olmaq üçün "heç vaxt etibar etmə və həmişə yoxla" yanaşmasından istifadə edilməsi;

7.14.2.3. məlumat ötürmə kanallarının tam şifrlənməsinin (end-to-end encryption) təmin edilməsi.

7.15. Sınaq yoxlamaları zamanı həssas informasiyanın adsızlaşdırılmadan istifadəsinə yol verilmir, sınaq mühitinin təhlükəsizliyi diqqətdə saxlanılır.

7.16. Kritik informasiya sistemləri və əlaqəli aktivləri əhatə edən audit zamanı nəzarət subyektinin biznes proseslərinə mənfi təsirləri minimallaşdırmaq məqsədilə audit testləri dəqiqliklə planlaşdırılır və nəzarət subyektinin rəhbərliyi ilə razılaşdırılır.

7.17. İnformasiya texnologiyalarının, insan resurslarının, digər təsisatların tələb edilən həcmdə olmasını təmin etmək məqsədilə resursların istifadəsi monitorinq edilir və azı aşağıdakılar nəzərə alınmaqla nəzarət subyektinin mövcud və gözlənilən ehtiyaclarına uyğunlaşdırılır:

7.17.1. yeni personalın cəlb edilməsi;

7.17.2. yeni təsisatların, o cümlədən daha güclü sistemlərin və komponentlərin (mərkəzi prosessor, operativ yaddaş qurğusu, digər yaddaş qurğuları və s.) əldə edilməsi;

7.17.3. köhnəlmiş məlumatların arxivləşdirilməsi və (və ya) silinməsi;

7.17.4. yararsız və istifadəsinə zərurət olmayan proqram təminatlarının, verilənlər bazasının idarəetmə sistemlərinin, texniki infrastrukturların istismardan çıxarılması;

7.17.5. proqram təminatı kodlarının və verilənlər bazası üzrə sorğuların optimallaşdırılması.

7.18. Kritik informasiya sistemi və digər əlaqəli aktivlərdə texniki zəifliklərin müəyyən edilməsi və onlardan sui-istifadənin qarşısının alınması məqsədilə azı aşağıdakı tədbirlər həyata keçirilir:

7.18.1. texniki zəifliklərin monitorinqi, zəifliklər üzrə risklərin qiymətləndirilməsi, tətbiq əlavələrinin və yenilənmələrin idarə edilməsi məqsədilə vəzifələr və bu vəzifələr üzrə öhdəlik və səlahiyyətlərin müəyyən edilməsi;

7.18.2. texniki zəifliklərin analizi və aradan qaldırılması məqsədilə ildə azı 1 (bir) dəfə müdaxilə sınaqlarının keçirilməsi üzrə ixtisaslaşmış kənar mütəxəssislər cəlb edilməklə daxili və xarici müdaxilə sınaqlarının həyata keçirilməsi və nəticələrinin sənədləşdirilməsi;

7.18.3. kritik informasiya sisteminin müdaxilə sınaqları keçirildikdən və aşkar edilmiş zəifliklər aradan qaldırıldıqdan sonra əməliyyat mühitinə keçirilməsi;

7.18.4. kritik informasiya sisteminə tətbiqi planlaşdırılan dəyişikliklərin sınaq mühitində testləşdirilməsi və aşkarlanmış zəifliklərin aradan qaldırılmasından sonra əməliyyat mühitində tətbiq edilməsi;

7.18.5. texniki zəiflik aşkar edildikdən sonra əlaqəli risklər və görüləcək tədbirlərin müəyyən edilməsi.

7.19. Texniki infrastrukturun və proqram təminatlarının tələb edilən təhlükəsizlik tənzimləmələri ilə düzgün işləməsini və konfiqurasiyalarının icazəsiz və ya yanlış dəyişikliklərdən mühafizəsini təmin etmək məqsədilə konfiqurasiyalar, o cümlədən təhlükəsizlik konfiqurasiyaları müəyyən edilir, sənədləşdirilir, tətbiq edilir və monitorinqi həyata keçirilir.

7.20. Qanunsuz açıqlanmasının qarşısının alınması məqsədilə qanunvericiliyin tələbləri və müqavilə şərtləri nəzərə alınmaqla giriş icazəsi olmayan şəxslərə münasibətdə həssas informasiyanın adsızlaşdırılması həyata keçirilir və informasiya təsnifatına uyğun olaraq giriş hüquqları müəyyən edilərək mühafizəsi təmin edilir.

7.21. İnformasiya sistemlərində, şəbəkə və digər infrastruktur elementlərində informasiya sızıntısının qarşısının alınması üçün informasiyanın təsnifatı nəzərə alınmaqla potensial informasiya sızıntısı baş verə biləcək kanalların monitorinqinin həyata keçirilməsi və sızıntının qarşısının alınması üçün müvafiq alətlərdən (nəzarət mexanizmləri, proqram təminatı, sistem və s.) istifadə edilməsi təmin edilir.

7.22. Əlçatanlıq tələblərini qarşılamaq məqsədilə kritik informasiya sistemləri üzrə azı aşağıdakılar müəyyən olunmaqla informasiya texnologiyalarının kifayət qədər olması təmin edilir:

7.22.1. azı 2 (iki) şəbəkə xidməti təchizatçısı və (və ya) internet xidməti təchizatçısı ilə müqavilə bağlanması;

7.22.2. informasiya sistemlərində fəaliyyətin fasiləsizliyi üçün yüklənmələrin tarazlaşdırılması və klasterizasiya texnologiyalarının tətbiq edilməsi;

7.22.3. informasiya texnologiyaları və kommunikasiya avadanlıqlarının dublikat komponentlərə (mərkəzi prosessor, operativ yaddaş qurğusu, digər yaddaş qurğuları və s.) malik olması.

7.23. Potensial informasiya təhlükəsizliyi insidentlərinin qiymətləndirilməsi məqsədilə şəbəkə, sistem və proqram təminatlarında baş verə biləcək qeyri-adi davranışların azı aşağıdakılar nəzərə alınmaqla davamlı monitorinqi mexanizmi yaradılır:

7.23.1. daxil olan və ötürülən şəbəkə, sistem və proqram təminatı trafikləri;

7.23.2. sistemlərə, informasiyanın işlənmə mərkəzlərinə, monitorinq sisteminə, şəbəkə avadanlıqları və şəbəkə konfiqurasiya fayllarına girişlər, o cümlədən imtiyazlı girişlər;

7.23.3. təhlükəsizlik alətləri (antivirus, şəbəkə təhlükəsizliyi avadanlıqları və sair) üzrə loqları;

7.23.4. resursların (mərkəzi prosessor, operativ yaddaş qurğusu, digər yaddaş qurğuları və s.) istifadə imkanları.

7.24. Əməliyyat sistemlərində proqram təminatlarının təhlükəsiz şəkildə quraşdırılması məqsədilə azı aşağıdakı tələblər nəzərə alınır:

7.24.1. istifadəsinə icazə verilən proqram təminatlarının siyahısının formalaşdırılması;

7.24.2. proqram təminatlarının quraşdırılmasının yalnız icazə verilmiş şəxslər tərəfindən həyata keçirilməsi;

7.24.3. proqram təminatlarının yalnız uğurlu sınaq testləşdirilməsindən sonra quraşdırılması və yenilənməsi;

7.24.4. dəyişikliklər tətbiq edilməzdən öncə geri qayıtma planının müəyyən edilməsi;

7.24.5. əməliyyat sistemi və proqram təminatları üzərində nəzarəti üstələyən utilit proqram təminatlarının istifadəsinin məhdudlaşdırılması və istifadəsinə nəzarətin tətbiq edilməsi.

7.25. İnformasiyanın konfidensiallığının və tamlığının qorunması üçün kriptoqrafiyanın düzgün seçilməsi və effektiv istifadəsinin təmin olunması məqsədilə aşağıdakı tədbirlər həyata keçirilir:

7.25.1. kriptoqrafik vasitələrlə təhlükəsizliyi təmin edilməli olan informasiya müəyyən edilir;

7.25.2. risklərin qiymətləndirilməsinə əsasən informasiyanın şifrlənməsi üçün istifadə edilən kriptoqrafik vasitələrin şifrləmə alqoritminin mürəkkəblik səviyyəsi müəyyən edilir;

7.25.3. kriptoqrafik vasitələrdən istifadə üzrə vəzifələr və bu vəzifələr üzrə öhdəlik və səlahiyyətlər müəyyənləşdirilir;

7.25.4. azı aşağıdakıları müəyyən edən kriptoqrafik açarların idarə edilməsi sistemi yaradılır:

7.25.4.1. kriptoqrafik açarların yaradılması;

7.25.4.2. kriptoqrafik açarların paylanılması;

7.25.4.3. kriptoqrafik açarların dəyişdirilməsi;

7.25.4.4. kriptoqrafik açarların geri çağırılması;

7.25.4.5. kriptoqrafik açarların qüvvəsinin dayandırılması və bərpa edilməsi;

7.25.4.6. kriptoqrafik açarların ehtiyat nüsxəsinin yaradılması və saxlanılması;

7.25.4.7. kriptoqrafik açarların məhv edilməsi;

7.25.4.8. kriptoqrafik açarların idarə edilməsi üzrə loqların qeydiyyatının aparılması.

7.26. Proqram təminatı və informasiya sistemlərinin bütün fəaliyyət dövrü ərzində təhlükəsiz inkişaf etdirilməsi azı aşağıdakılar nəzərə alınmaqla təmin edilir:

7.26.1. inkişaf, sınaq və əməliyyat mühitlərinin bir-birindən ayrılması;

7.26.2. təhlükəsiz inkişaf metodologiyasının və təhlükəsiz kodlaşdırma təlimatının formalaşdırılması;

7.26.3. layihələndirmə və dizayn mərhələləri üzrə təhlükəsizlik tələblərinin tətbiq edilməsi;

7.26.4. mütəmadi olaraq mənbə kodlarının yoxlanılması, müdaxilə sınaqlarının aparılması və mənbə kodlarında aşkarlanan təhlükəsizlik boşluqlarının aradan qaldırılması;

7.26.5. mənbə kodlarının təhlükəsiz saxlanması və konfiqurasiyası;

7.26.6. mənbə kodlarının versiyaları üzrə nəzarətin təmin edilməsi;

7.26.7. inkişaf etdirilmənin azı aşağıdakıları nəzərdə tutan kənar təchizatçıya ötürülməsi qaydasının qəbul edilməsi:

7.26.7.1. kənardan alınan xidmətlə bağlı lisenziya müqavilələrinin, kod sahibliyinin və əqli mülkiyyət hüquqlarının nəzərə alınması;

7.26.7.2. müqavilələrdə nəzarət subyektinin informasiya təhlükəsizliyi üzrə tələblərinin müəyyən edilməsi;

7.26.7.3. inkişaf mühitinə dair təhlükəsizlik tələblərinin müəyyən edilməsi;

7.26.7.4. xidmətin nəticələrinin qəbulu üzrə testlərin həyata keçirilməsi;

7.26.7.5. qanunvericiliyin tələblərinin (məsələn, fərdi məlumatların mühafizəsi ilə bağlı) gözlənilməsi.

7.27. Proqram təminatının hazırlanması və ya əldə edilməsi zamanı azı aşağıdakılar nəzərə alınmaqla informasiya təhlükəsizliyi tələbləri müəyyən edilir:

7.27.1. proqram təminatı tərəfindən işlənilən informasiyanın növü və təsnifat səviyyəsi;

7.27.2. proqram təminatında verilənlərə və funksiyalara giriş hüquqları;

7.27.3. zərərverici hücumlara və qeyri-ixtiyari pozulmalara qarşı dayanıqlılıq;

7.27.4. həssas informasiyanın mühafizəsi tələbləri;

7.27.5. informasiyanın işlənməsi, ötürülməsi və saxlanılması zamanı mühafizəsi tələbləri;

7.27.6. bütün əlaqəli tərəflər arasında məlumat mübadiləsinin şifrələnməsi.

7.28. Biznes proseslərdə, informasiyanın işlənməsi vasitələrində və proqram təminatlarında informasiya təhlükəsizliyinə təsir edən dəyişikliklərin idarə edilməsi üzrə azı aşağıdakıları nəzərdə tutan qaydalar hazırlanır və təsdiq edilir:

7.28.1. dəyişikliklərin müəyyən edilməsi və qeydiyyata alınması;

7.28.2. dəyişikliklərin planlaşdırılması və testləşdirilməsi;

7.28.3. informasiya təhlükəsizliyinə təsirlər də daxil olmaqla, dəyişikliklərin potensial təsirləri üzrə risklərin qiymətləndirilməsi;

7.28.4. informasiya təhlükəsizliyi tələblərinin yerinə yetirilməsinin yoxlanılması;

7.28.5. dəyişikliklərin təfərrüatlarının bütün aidiyyəti maraqlı tərəflərə çatdırılması;

7.28.6. dəyişikliklərin tətbiqi zamanı uğursuz dəyişikliklər və ya gözlənilməz halların ləğvi və ya geri qayıtma prosedurları və məsuliyyətlərinin müəyyən edilməsi;

7.28.7. insidentlərin həll edilməsi üçün zəruri olan təxirəsalınmaz dəyişikliklər üzrə proseslərin müəyyən edilməsi;

7.28.8. bu Tələblərin 7.28.1-7.28.7-ci yarımbəndlərində göstərilənləri ehtiva edən dəyişikliklər üzrə qeydlərin saxlanılması.

7.29. Nəzarət subyektləri tərəfindən mobil tətbiqlərdə informasiya təhlükəsizliyinin təmin edilməsi məqsədilə azı aşağıdakı tədbirlər həyata keçirilir:

7.29.1. istifadəçi interfeysi vasitəsilə daxil edilən həssas informasiyanın qanunsuz ələ keçirilməsinin qarşısının alınması üçün müvafiq nəzarət tədbirləri tətbiq edilir (anti-keylogging);

7.29.2. kənar şəxslər tərəfindən mobil tətbiqlərin xəta aşkarlama mühitində (debugger environment), emulyatorda və ya virtual maşında işlədilməsinin mümkün olmaması üçün müvafiq nəzarət tədbirləri tətbiq edilir (anti-debugging və anti-emulation);

7.29.3. mobil tətbiqlərin yalnız aktivləşdirildiyi mobil cihazda işləməsi təmin edilir (device-binding);

7.29.4. istehsalçı tərəfindən müəyyən edilməyən formada istifadə etmək məqsədilə mobil cihazın əməliyyat sisteminə müdaxilə edilməsi (jailbreak) yoxlanılır və belə mobil cihazda mobil tətbiqlərin işlənməsinə yol verilmir.

8. Hesabatlıq

8.1. Nəzarət subyekti bu Tələblərin 3.3-cü bəndinə əsasən təyin edilmiş informasiya təhlükəsizliyi üzrə məsul şəxsin soyadı, adı, atasının adı, ünvanı, əlaqə vasitələri barədə məlumatı, habelə təyin edilməsi barədə qərarın surətini təyin edilmə tarixindən, habelə bu məlumatlarda dəyişiklik olduqda, dəyişikliyin baş verdiyi tarixdən 5 (beş) iş günü ərzində bu barədə məlumatı Mərkəzi Banka yazılı şəkildə təqdim edir.

8.2. Nəzarət subyekti bu Tələblərin 3.7-ci və 3.8-ci bəndlərinə əsasən əldə etdiyi kənar auditor rəylərini, habelə bu Tələblərin 3.8-ci bəndinə əsasən əldə etdiyi tələblərə uyğunluq üzrə sənədin surətini 5 (beş) iş günü ərzində Mərkəzi Banka təqdim edir.

8.3. Nəzarət subyekti yüksək kateqoriyalı insident barədə bu Qaydaya 1 nömrəli Əlavədə göstərilən ilkin hesabatı insident baş verdiyi və ya aşkar olunduğu andan etibarən 4 (dörd) saat ərzində xüsusi təyinatlı informasiya mübadilə sistemi vasitəsilə Mərkəzi Banka təqdim edir. Bu müddət qeyri-iş saatlarına təsadüf etdikdə, məlumat növbəti iş gününün ilk iş saatı ərzində Mərkəzi Banka təqdim edilir.

8.4. Nəzarət subyekti insident tam aradan qaldırıldığı vaxtdan 5 (beş) iş günü ərzində bu Qaydaya 2 nömrəli Əlavədə göstərilən yekun hesabatı xüsusi təyinatlı informasiya mübadilə sistemi vasitəsilə Mərkəzi Banka təqdim edir.

8.5. Bu Tələblərin 4.12.1-ci yarımbəndinə əsasən müəyyən edilmiş kritik informasiya sistemi və əlaqəli aktivləri barədə aktual məlumatlar bu Tələblərə 3 nömrəli Əlavəyə uyğun olaraq hər təqvim ili üzrə növbəti ilin yanvar ayının ilk 10 (on) iş günü ərzində Mərkəzi Banka təqdim edilir.

8.6. Nəzarət subyekti bu Tələblərin 4.14-cü bəndinə müvafiq olaraq sınağı həyata keçirməmişdən 5 (beş) iş günü əvvəl Mərkəzi Bankı bu barədə məlumatlandırır, sınaq başa çatdıqdan sonra isə 7 (yeddi) iş günü müddətində nəticəsi barədə bu Tələblərə 4 nömrəli Əlavədə göstərilən hesabatı təqdim edir.

8.7. Bu Tələblərin 7.18.2-ci yarımbəndinə əsasən həyata keçirilmiş müdaxilə sınaqlarının nəticələri 5 (beş) iş günündən gec olmayaraq Mərkəzi Banka təqdim edilir.

"Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər"ə Əlavə 1

Yüksək kateqoriyalı insident üzrə

ilkin hesabat

Hesabat tarixi (gün/ay/il, saat/dəqiqə)	
İnsidentin nömrəsi	
İnsidentin baş vermə vaxtı (gün/ay/il, saat/dəqiqə) (məlumdursa)	
İnsidentin aşkarlanması vaxtı (gün/ay/il, saat/dəqiqə)	
Ümumi məlumatlar	
Nəzarət subyektinin adı	
İnsident üzrə məsul əməkdaş haqqında məlumat (soyadı, adı, atasının adı, vəzifəsi, o cümlədən əlaqə məlumatları (elektron poçt ünvanı, mobil telefon nömrəsi))	
İnsidentin qısa və ümumi açıqlaması	
İnsidentin təsir meyarı	□ Xidmət istifadəçilərinə təsir □ Xidmətin əlçatanlığına təsir □ İqtisadi təsir (maliyyə itkiləri) □ Reputasiya təsiri □ Aparılan əməliyyatlara təsir □ Digər nəzarət subyektləri və ya müvafiq maliyyə xidmətləri infrastrukturuna təsir
Aidiyyəti dövlət orqanlarına (qurumlarına) hesabat təqdim olunub (olunacaq)? (cavab "bəli" olduqda, müvafiq dövlət orqanının (qurumunun) adı)	

"Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər"ə Əlavə 2

Yüksək kateqoriyalı insident üzrə yekun hesabat

Hesabat tarixi və vaxtı (gün/ay/il, saat/dəqiqə)		
İnsidentin nömrəsi (ilkin hesabata istinad edilir)		
1. Ümumi məlumatlar		
Yenilənmiş məlumatlar (ilkin hesabata əlavə olaraq)		
İnsident haqqında məlumatlar		
İlkin hesabata edilmiş dəyişikliklər		
Digər əhəmiyyətli məlumatlar		
İnsident haqqında əlavə məlumatlar		
İnsidentin başlama tarixi və vaxtı (gün/ay/il, saat/dəqiqə)		
İnsident necə başladı?		
İnsident necə davam etdi?		
İnsident barədə xidmət istifadəçilərinə məlumat verilib? (cavab "bəli" olduqda, təfərrüatlar)		
Əvvəlki insidentlərlə əlaqəlidir? (cavab "bəli" olduqda, təfərrüatlar)		
Digər təşkilatlar/ üçüncü tərəflər bu insidentə məruz qalıb? (cavab "bəli" olduqda, təfərrüatlar)		
İnsidentin aradan qaldırıldığı gün və vaxt (gün/ay/il, saat/dəqiqə)		
2. İnsidentin təsnifləşdirilməsi		
Nəzarət subyektinin əməliyyatlarına təsir	Təsirə məruz qalmış əməliyyatların sayı	

	Təsirə məruz qalmış əməliyyatların faiz çəkisi (əvvəlki ayın orta günlük göstəricisinə nisbətdə)	
	Təsirə məruz qalmış əməliyyatların həcmi (min manatla)	
	İnsidentin müddəti	
	Qeydlər	
Nəzarət subyektinin istifadəçilərinə təsir	Təsirə məruz qalmış istifadəçilərin sayı (rəqəmlə)	
	Təsirə məruz qalmış istifadəçilərin sayı (faizlə)	
İqtisadi təsir (maliyyə itkiləri)	Zərərin həcmi (min manatla)	
Digər təşkilatlara və ya müvafiq nəzarət subyektinin strukturuna təsir (Bəli/Xeyr) (cavab "bəli" olduqda, təfərrüatlar)		

Reputasiya təsiri (Bəli/Xeyr) (cavab "bəli" olduqda, təfərrüatlar)		
3. İnsidentin təsviri		
İnsidentin səbəbi (cavab "digər" olduqda, təfərrüatlar)		□ Zərərverici fəaliyyət □ Emal xətası □ Sistem xətası □ İnsan amili □ Kənar amil □ Digər
4. İnsidentin təsiri		
Ümumi təsir		□ Tamlıq □ Konfidensiallıq □ Əlçatanlıq
Təsirə məruz qalmış xidmət kanalları		□ Filiallar □ Elektron ticarət □ Mobil tətbiq □ İnternet səhifə □ Bankomatlar □ Agent şəbəkəsi □ Digər
Təsirə məruz qalmış xidmət		
5. İnsidentin baş vermə səbəbi və təhlili		
İnsidentin baş vermə səbəbi (bir neçə səbəb göstərilə bilər)	Zərərverici fəaliyyət	□ Zərərverici proqram □ İcazəsiz müdaxilə □ Sistemin yüklənməsi □ Kənar zərər □ Fırıldaqçılıq □ Digər
	Emal xətası	□ Monitorinq və nəzarət xətası □ Kommunikasiya xətası □ Bərpa problemləri

		□ Digər
	Sistem xətası	□ Texniki xəta □ Şəbəkə xətası □ Verilənlər bazası xətası □ Proqram təminatı xətası □ Fiziki zərər □ Digər
	İnsan amili	□ Gözlənilməz xəta □ Fəaliyyətsizlik □ Resurs çatışmazlığı □ Digər
	Kənar amil	□ Texniki xidmət təchizatçısı □ Fors-major halı □ Digər
	Digər (yuxarıdakıların heç biri olmadıqda)	
İnsidentin baş vermə səbəbi ilə əlaqəli əlavə məlumatlar		
İnsidentin yenidən təkrarlanmasının qarşısının alınması üçün görülmüş (görüləcək) tədbirlər		
6. Əlavə məlumatlar		
İnsident barəsində digər təşkilatlara məlumat verilib? (verilibsə, bu barədə məlumat)		
İnsidentlə bağlı təşkilata qarşı hüquqi tədbir görülüb? (görülübsə, bu barədə məlumat)		

"Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər"ə Əlavə 3

Kritik informasiya sistemi və əlaqəli aktivlər barədə

məlumat

Kritik informasiya sistemi		
Kritik informasiya sisteminin adı		
Kritik informasiya sisteminin təyinatı		
Sistemin kritik hesab edilməsi meyarı		
Biznesə təsir analizinin nəticələri		
Əlaqəli aktivlər		
Əlaqəli aktivlərin adı	Dəstəkləyici funksionalı	Əməliyyat sistemi
Təchizatçılar barədə məlumat		
Kritik informasiya sisteminə dəstək göstərən təchizatçı(lar)	1. 2.	
Əlaqəli aktivlərə dəstək göstərən təchizatçı(lar)	1. 2.	

"Maliyyə bazarlarında fəaliyyətinə nəzarət edilən subyektlərdə informasiya təhlükəsizliyinin təmin edilməsinə dair Tələblər"ə Əlavə 4

Ehtiyat mərkəzə keçid üzrə

hesabat

Ümumi məlumat			
Nəzarət subyektinin adı			
Ehtiyat mərkəzə keçidin ssenarisi			
Keçidin icra tarixi və vaxtı			
Keçid müddəti			
Əhatə olunan sahələr (xidmətlər)			
Əhatə olunmayan sahələr (xidmətlər)			
Keçidin nəticəsi			
Ehtiyat mərkəzə keçidin təşkili üzrə məsul şəxslər			
Soyadı, adı, atasının adı	Struktur bölmə	Vəzifəsi	İmzası