AZƏRBAYCAN RESPUBLİKASI DÖVLƏT NEFT FONDUNUN TƏHLÜKƏSİZLİK DEPARTAMENTİ HAQQINDA

Ə S A S N A M Ə

1. ÜMUMİ MÜDDƏALAR

1.1. Azərbaycan Respublikası Dövlət Neft Fondunun (bundan sonra – Fond) Təhlükəsizlik departamenti (bundan sonra – Departament) Fondun aparatının struktur bölməsidir.

1.2. Departament öz fəaliyyətində Azərbaycan Respublikasının Konstitusiyasını, Azərbaycan Respublikasının qanunlarını, Azərbaycan Respublikası Prezidentinin fərman və sərəncamlarını, "Azərbaycan Respublikasının Dövlət Neft Fondu haqqında Əsasnamə"ni, Fondun əmr və sərəncamlarını, habelə bu Əsasnaməni rəhbər tutur.

1.3. Departament bu Əsasnamə ilə müəyyən olunmuş funksiyaların yerinə yetirilməsi prosesində Fondun digər struktur bölmələri ilə qarşılıqlı şəkildə fəaliyyət göstərir.

2. DEPARTAMENTİN FƏALİYYƏTİNİN ƏSAS MƏQSƏDİ

Departamentin fəaliyyətinin əsas məqsədi Fondun fəaliyyətinin informasiya təhlükəsizliyinin, Fondun inzibati binasının, ərazisinin, inzibati binada olan əmlakının fiziki təhlükəsizliyinin sistemli idarə olunmasını təmin etməkdir.

3. DEPARTAMENTİN FUNKSIYALARI

Departamentin funksiyaları aşağıdakılardan ibarətdir:

3.1. Fondda fəaliyyət proseslərinin informasiya təminatının dayanıqlığının təmin edilməsi, bunun üçün informasiya təhlükəsizliyi üzrə risklərin və insidentlərin mövcud standartlara uyğun idarə edilməsi, informasiya texnologiyaları və sənəd dövriyyəsi infrastukturlarının təhlükəsizliyinə nəzarət edilməsi;

3.2. Fondun fəaliyyətinin təhlükəsizliyinin təmin edilməsi, onun maraqlarına edilə bilən təhdidlərin qarşısının alınması, Fondun inzibati binasının, ərazisinin, inzibati binada olan əmlakının və insanların hüquqazidd əməllərdən və fövqəladə hadisələrdən qorunma tədbirlərinin təşkil edilməsi.

4. DEPARTAMENTİN VƏZİFƏLƏRİ

Departament bu Əsasnamə ilə müəyyən olunmuş funksiyaları həyata keçirmək üçün aşağıdakı vəzifələri yerinə yetirir:

<u>İnformasiya təhlükəsizliyi üzrə analitika və layihələndirmə</u>:

4.1. fəaliyyət proseslərinə informasiya təhlükəsizliyi risklərini, onların ehtimal və fəsad dərəcələrini, risklərin emal növlərini (qəbuletmə, yönləndirmə, qarşısını alma, minimallaşdırma) və prioritetlərini, insidentlərin menecment sisteminin strukturunu və insidentlərə əks-cavab sxemlərini (monitorinq-aşkaretmə; xəbərvermə; bloklama; izləmə; ehtiyat varianta kecmə; qiymətləndirmə; sübut toplama; bərpaetmə; fövqəladə hal) müəyyən etmək, tətbiq modellərini dəqiqləşdirmək;

4.2. İnformasiya təhlükəsizliyini idarəetmə sisteminin (bundan sonra – İTİS) formalaşdırılmasını (davamlı təkmilləşdirilməsini) və tətbiqini tənzimləyən sənədlərin, o cümlədən informasiya mühafizə üsullarının (mümkün təhdidlərin reallaşmasına qarşı adekvat prosesləri təsvir edən prosedurların, reqlamentlərin) layihələrinin hazırlanmasını təşkil etmək, sənədləşdirmək;

4.3. informasiya mühafizə səlahiyyətlərini və rollarını təsnifatlaşdırmaq, “Səlahiyyətlər bölgüsü” cədvəli və koordinasiya layihələrini tərtib etmək;

4.4. baş verən insidentlərin təhdid sxemini (təhdidin mənbəyi - məqsədi - hədəfi - pozduğu tələb - istifadə etdiyi zəiflik - reallaşma texnologiyası - fəsadı) təhlil etmək, qalıq riskləri qiymətləndirmək;

4.5. informasiya təhlükəsizliyi fəsadlarının işgüzar fəaliyyətin fasiləsizliyinə zərərini qiymətləndirmək;

4.6. insidentlərə aid tendensiyaları müəyyən etmək, informasiya təhlükəsizliyinin menecmenti üzrə toplanan təcrübəni periodik ümumiləşdirmək, korrektiv təkliflər vermək;

<u>İnformasiya təhlükəsizliyi risklərinin menecmenti:</u>

4.7. informasiya təhlükəsizliyinə təhdidləri, təhdidlərin sxemlərini, o cümlədən mümkün xarici və daxili mənbələrini və digər faktorları müəyyən etmək, riskləri qiymətləndirmək;

4.8. risklər reyestrinin formalaşdırılmasına, mühafizəsinə və istifadəsinə aid işləri təşkil etmək;

4.9. mühafizə üsullarının müəyyən edilməsində iştirak, bu üsulların adekvat aləti olan mühafizə vasitələrinə (proqram və texniki təminat vasitələrinə, informasiya resurslarına, fiziki mühafizə vasitələrinə və mühəndis qurğularına) olan tələbatı müəyyən etmək, bu vasitələrin spesifikasiyalarına rəy vermək;

4.10. informasiya mühafizə hədəflərinə aid hazırlanmış layihələrin informasiya təhlükəsizliyi tələbləri üzrə ekspertizasını keçirmək;

4.11. informasiya mühafizə vasitələrinin, audit jurnallarının konfiqurasiya parametrlərini və bu vasitələrdən istifadə və qeydiyyat reqlamentlərini (altsiyasətlərini) müəyyən etmək, onların icrasının monitorinqini aparmaq;

4.12. mövcud və yenilənən infrastruktura və konfiqurasiyada zəifliklərin qiymətləndirilməsi üçün təhlükəsizlik tələbləri üzrə test sınaqlarını təşkil etmək;

4.13. mövcud və yenilənən infrastruktura və konfiqurasiyaya, mühafizə üsullarına və vasitələrinə aid korrektiv təkliflər vermək;

<u>İnformasiya təhlükəsizliyi insidentlərinin menecmenti:</u>

4.14. ehtimal olunan insidentlərin təsnifat kateqoriyalarını, əhəmiyyət dərəcələrini müəyyən etmək;

4.15. insidentlərin menecmentinə aid layihələr üçün təkliflər vermək, insidentlərin menecment sistemini üsul və vasitə komponentləri ilə komplektləşdirmək, insidentlərə cavabvermə sxemlərinin tətbiqi modellərini dəqiqləşdirmək;

4.16. informasiya təhlükəsizliyi insidentlərinə cavabvermə qruplarının formalaşmasını və fəaliyyətini praktiki təşkil etmək;

4.17. informasiya mühafizə hədəflərinin, o cümlədən mühafizə üsullarının və vasitələrinin təhlükəsizliyini monitorinq etmək, informasiya təhlükəsizliyi hadisələrini (insident olub-olmamasını) qiymətləndirmək, insidentlərə müvafiq cavabvermə sxemini seçmək, tətbiq etmək;
4.18. insidentlər üçün istifadə olunmuş təhdid sxemlərinin, onların komponentlərinin, mühafizə vasitələrindən istifadələrin statistikasını aparmaq;
4.19. insidentlə əlaqədar olan (informasiya təhlükəsizliyinin hədəfi olan) obyektlər və proseslər üçün informasiya təhlükəsizliyi risklərinin menecmentinə korrektiv təkliflər vermək;

İnformasiya təhlükəsizliyi üzrə maarifləndirmə:

4.20. informasiya təhlükəsizliyinə təhdid tendensiyalarını, mühafizə sahəsində qabaqcıl təcrübəni, bu sahədə normativ tələbləri müntəzəm izləmək, təsnifatlaşdırmaq;
4.21. mühafizə hədəflərini (informasiya proseslərində iştirak edən obyekt, proses və subyektləri) təsnifatlaşdırmaq;
4.22. informasiya təhlükəsizliyi insidentlərinə və cavab tədbirlərinə aid biliklər bazasının formalaşdırılmasını və istifadəsini təşkil etmək;
4.23. informasiya təhlükəsizliyi hadisələrində (o cümlədən insidentlərdə) insan faktorunun statistikasını aparmaq, tövsiyələr hazırlamaq;
4.24. informasiya təhlükəsizliyi üzrə aşkar edilən hadisələr barədə maraqlı tərəfləri məlumatlandırmaq;
4.25. İTİS proseslərində iştirak edən menecerlər, mütəxəssislər və personal üçün informasiya təhlükəsizliyinə aid kompetensiya tələblərini müəyyən etmək;
4.26. həmin menecerlər, mütəxəssislər və personal üçün müvafiq kateqoriyalar üzrə təlim proqramlarını hazırlamaq;

Fiziki təhlükəsizlik üzrə təşkilati-analitik fəaliyyət:

4.27. Fondun struktur bölmələrinin fəaliyyətində təhlükəsizlik tələblərinə riayət olunmasına nəzarət etmək;
4.28. Fondun fəaliyyətini tənzimləyən sənədlərin (qaydalar, təlimatlar və s.) hazırlanmasında iştirak edərək orada təhlükəsizlik məsələlərinə aid müddəaların əks olunmasını təmin etmək;
4.29. Fondda fiziki təhlükəsizlik sistemləri, qurğu və avadanlıqlarının layihələndirilməsinə təkliflər vermək, onların quraşdırılmasına nəzarət etmək;
4.30. Fondun fiziki təhlükəsizliyi üçün ayrılan maddi vəsaitlərin uçotunu aparmaq və onların istifadəsinə nəzarət etmək;
4.31. Fondun yerləşdiyi ərazidə ictimayi asayişin, həmçinin kriminogen vəziyyətin öyrənilməsi ilə əlaqədar yerli hüquq-mühafizə orqanlarının və qonşu müəssisələrin təhlükəsizlik xidmətlərinin nümayəndələri ilə rəsmi əlaqələr saxlamaq;
4.32. Fondun bütün fəaliyyət istiqamətləri üzrə təhlükəsizlik qaydalarının və digər hüquqi və texniki tələblərin pozulma halları, Fondun maraqlarına qarşı yönəlmiş əməllər barədə məlumatları toplamaq, təhlil etmək, Fondun fiziki təhlükəsizliyi üçün mümkün nəticələri proqnozlaşdırmaq;
4.33. Fondun fiziki təhlükəsizliyinin təmin edilməsi üçün görülən tədbirlərin səmərəliliyini və etibarlılığını vaxtaşırı qiymətləndirmək;
4.34. Fondun fiziki təhlükəsizliyinə qarşı risklər barədə Fondun İcraçı direktoruna, zəruri hallarda onun tapşırığı ilə müvafiq dövlət orqanlarına məlumat vermək;
4.35. Fondun fiziki təhlükəsizliyi ilə bağlı insidentlər üzrə ilkin araşdırmaları aparmaq;

4.36. təhlükəsizlik sahəsində çalışan əməkdaşların peşə hazırlığının təkmilləşdirilməsini, ixtisaslarının artırılması və mənəvi-psixoloji hazırlığının təmin edilməsi üçün tədbirlər görmək;

Fondun inzibati binası, ərazisi və inzibati binada olan əmlakının qorunması, işçilərin və Fondda olan digər şəxslərin fiziki təhlükəsizliyinin təmin edilməsi:

4.37. Fondun ərazisinin və inzibati binasının perimetr üzrə polis qüvvələri ilə mühafizəsini təşkil etmək, Fondda ehtimal edilən ekstremal hallar zamanı təhlükələrin zərərli təsirinin aradan qaldırılması üçün zəruri tədbir və prosedurları müəyyən etmək, işçilərin bu istiqamətdə hazırlığını, onların polis əməkdaşları ilə fəaliyyətlərinin koordinasiyasını təmin etmək;
4.38. Fondda təhlükəsizlik tələblərinin pozulma hallarının baş verməsinə səbəb ola biləcək şərtlərin aradan qaldırılması üçün tədbirlər görmək;
4.39. Fondda təhlükəsizlik tələblərinin pozulma halı baş verdikdə Fondun təhlükəsizliyinin təmin edilməsi məqsədi ilə tədbirlər görmək, müvafiq qaydada rəhbərliyi məlumatlandırmaq;
4.40. Fondun inzibati binası və ərazisinə cinayət qəsdi edildikdə mühafizə siqnalizasiyası və həyəcan düyməsi vasitəsi ilə əlavə polis qivvələrinin Fonda gəlməsini təmin etmək.

Fondun xüsusi rejimli zonalarının təhlükəsizliyinin təmin edilməsi:

4.41. Fondun xüsusi rejimli zonaların sərhədlərini, kateqoriyalarını və riskləri müəyyənləşdirmək, onların adekvat mühafizəsini təmin etmək;
4.42. Fondun xəzinəsində xəzinə əməliyyatlarının təhlükəsizliyini təmin etmək;

Fondda nəzarət-buraxılış rejiminin təşkil edilməsi:

4.43. Fondda nəzarət-buraxılış və Fonddaxili təhlükəsizlik rejimini müəyyən etmək;
4.44. şəxslərin və avtomaşınların Fonda icazəli daxil olması üçün xidməti və müvəqqəti kartların verilməsini təşkil etmək və qeydiyyatını aparmaq, bu qaydalara riayət olunmasına nəzarət etmək;
4.45. mal və materialların Fonda gətirilməsi və Fonddan icazəli çıxarılmasına nəzarət etmək və onların qeydiyyatını aparmaq;

Yanğına qarşı rejimin təmin olunması və fövqəladə hallarda təxliyənin təşkil edilməsi:

4.46. Fondun inzibati binasında və ərazisində yanğına qarşı rejimi müəyyən etmək;
4.47. yanğına qarşı rejimə Fondun işçiləri və Fondda olan digər şəxslər tərəfindən riayət olunmasına nəzarət etmək;
4.48. Fondda yanğın təhlükəsizliyi qaydalarının pozuntusu hallarının baş verməsinə səbəb ola biləcək şərtlərin aradan qaldırılması üçün tədbir görmək;
4.49. fövqəladə hallarda Fondun inzibati binasından və ərazisindən insanların təhlükəsiz və maneəsiz təxliyəsinin təmin edilməsi üçün tədbirlər görmək;
4.50. fövqəladə hallarda zərurət yarandıqda Fondun inzibati binasında olan əmlakının təxliyəsini təşkil etmək.

Mülki müdafiə:

4.51. Fondda mülki müdafiənin təmin edilməsi üçün təşkilati tədbirləri həyata keçirmək;
4.52. fövqəladə hallarda, o cümlədən texnogen qəzalarda, kütləvi qırğın silahlarının tətbiqi, təbii fəlakətlər və epidemiyalar zamanı görüləcək tədbirlər və vəzifələr barədə Fondun əməkdaşlarının təlimatlandırılmasını təmin etmək;
4.53. mülki müdafiə tələblərinin Fondda yerinə yetirilməsinə nəzarəti həyata keçirmək;

Fiziki təhlükəsizlik sistemlərinin istismarı:

4.54. Fondun təhlükəsizliyinin təmin edilməsində fiziki təhlükəsizlik sistemlərinin imkanlarından istifadə etmək;
4.55. fiziki təhlükəsizlik sistemlərinin məlumatlarını təhlil etmək, onlardan insidentlərin səbəb və nəticələrinin araşdırılmasında istifadə etmək;
4.56. təhlükəsizlik avadanlıqları və qurğularının, o cümlədən rabitə, mühafizə və müdafiə vasitələrinin düzgün istismarını, fasiləsiz işini təmin etmək, onlara vaxtında və zəruri texniki xidmət göstərilməsinə nəzarət etmək;
4.57. Fonddan informasiyanın müvafiq sənədlərlə təsdiq edilmiş prosedurlarda nəzərdə tutulmayan üsul və vasitələrlə çıxarılmasının qarşısının alınması üçün Fondda təhlükəsizliyin zəif yerlərinin aradan qaldırılması istiqamətində tədbirlər işləyib hazırlamaq.

5. DEPARTAMENTİN FƏALİYYƏTİNİN TƏŞKİLİ

5.1. Departamentin təşkilati strukturu və işçilərinin sayı Fondun İcraçı direktoru tərəfindən müəyyən və təsdiq edilir.
5.2. Departamentin fəaliyyətinə Departamentin direktoru rəhbərlik edir. Departamentin direktoru Fondun İcraçı direktoru tərəfindən vəzifəyə təyin edilir və vəzifədən azad edilir. Departamentin direktoru Departamentə həvalə olunmuş vəzifələrin yerinə yetirilməsinə görə şəxsən məsuliyyət daşıyır.
5.3. Departamentin direktoru:
5.3.1. tabeliyində olan işçilər arasında iş bölgüsü aparır, onların fəaliyyətini əlaqələndirir, əmək, icra və xidmət intizamına riayət edilməsinə nəzarət edir;
5.3.2. Departamentin fəaliyyətinə dair mühüm məsələlər barədə məlumatı Fondun rəhbərliyinə təqdim edir;
5.3.3. Departamentin işçiləri barəsində həvəsləndirmə və intizam tənbehi tədbirləri görülməsi üçün Fondun rəhbərliyinə təqdimatlar verir;
5.3.4. daxil olan məktub, ərizə, şikayət və təkliflərə qanunvericilikdə nəzərdə tutulmuş qaydada baxılmasını təşkil edir;
5.3.5. Departamentdə kargüzarlıq işlərinin aparılmasını təmin edir;
5.3.6. Departamenti təmsil edir.
5.4. Departamentin direktoru olmadığı halda onun vəzifələrinin yerinə yetirilməsi onun müavininə həvalə olunur.
5.5. Departamentin işçiləri İcraçı direktor tərəfindən vəzifəyə təyin və azad edilir.
5.6. Departamentin tərkibinə İnformasiya təhlükəsizliyi və Ümumi təhlükəsizlik şöbələri daxildir.
5.6.1. Şöbənin fəaliyyətinə şöbənin müdiri rəhbərlik edir. Şöbə müdiri Fondun İcraçı direktoru tərəfindən vəzifəyə təyin edilir və vəzifədən azad edilir. Şöbə müdiri şöbəyə həvalə olunmuş vəzifələrin yerinə yetirilməsinə görə şəxsən məsuliyyət daşıyır. İnformasiya təhlükəsizliyi şöbəsinin müdiri olmadığı halda onun vəzifələrinin yerinə yetirilməsi şöbənin işçilərindən birinə, Ümumi təhlükəsizlik şöbəsinin müdiri olmadığı halda onun vəzifələrinin yerinə yetirilməsi onun müavininə həvalə olunur.
5.6.2. İnformasiya təhlükəsizliyi şöbəsinin vəzifələri bu Əsasnamənin 4.1 – 4.29-cu bəndlərini, Ümumi təhlükəsizlik şöbəsinin vəzifələri bu Əsasnamənin 4.30 – 4.57-ci bəndlərini əhatə edir.

5.6.3. Şöbə müdiri:

5.6.3.1. tabeliyində olan işçilər arasında iş bölgüsü aparır, onların fəaliyyətini əlaqələndirir, əmək, icra və xidmət intizamına riayət edilməsinə nəzarət edir;

5.6.3.2. şöbənin fəaliyyətinə dair mühüm məsələlər barədə məlumatı Departamentin direktoruna təqdim edir;

5.6.3.3. şöbənin işçiləri barəsində həvəsləndirmə və intizam tənbehi tədbirləri görülməsi üçün Departamentin direktoruna təkliflər verir;

5.6.3.4. şöbədə kargüzarlıq işlərinin aparılmasını təmin edir;

5.6.3.5. şöbəni təmsil edir.

6. DEPARTAMENTİN FƏALİYYƏTİNİN ƏSAS METODLARI

Departament üçün bu Əsasnamə ilə müəyyən olunmuş funksiyaları həyata keçirmək üçün aşağıdakı metodlar tətbiq edilir:

6.1. preventivlik – təhdidlərin baş verə və zəifliklərin yarana bilmə hallarının qabaqlanması və ya azaldılması;

6.2. səlahiyyətlər bölgüsü – mühafizə hədəflərinin strukturlaşdırılması və cavabdehlərin konkretləşdirilməsi;

6.3. qeydiyyat – təhlükəsizlik hadisələrinin operativ qeydiyyatının təmin edilməsi;

6.4. aşkarlama – təhlükəsizlik insidentlərinə cəhdlərin, baş verən insidentlərin və onların subyektlərinin tez müəyyən edilməsi;

6.5. əks-cavab və lokallaşdırma – təhlükəsizlik insidentlərinə cavab reaksiyasının verilməsi, o cümlədən təsirinin daraldılması;

6.6. bərpa – təhlükəsizlik rejiminin bərpa edilməsi;

6.7. təhlil – təhlükəsizlik insidentlərinin təhlili və mühafizənin effektivliyinin dəyərləndirilməsi.