ПРОУЧВАНЕ И ДОБИВ НА НЕФТ И ГАЗ АД
1000 София, ул. „Стефан Караджа" № 2
Тел. 02/ 980 16 11; факс: 02/ 981 73 89
www. ogep-bg.com
5870 Д. Дъбник, ул. „Д. Дебелянов" №12
тел. 064/ 880 445; факс: 064/ 880 449
e-mail: office@pdng-bg.com

Ниво 0 [TLP-WHITE]

Утвърдили:

Пламен Николов
Изпълнителен директор

Любомир Чакъров
Изпълнителен директор

ПОЛИТИКА
ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ НА „ПРОУЧВАНЕ И ДОБИВ НА НЕФТ И ГАЗ" АД

08.2022г.

Раздел I
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата политика има за цел осигуряването на мрежова и информационна сигурност в „Проучване и добив на нефт и газ“ АД.

Чл. 2. Мрежовата и информационна сигурност се осигурява чрез организационни, технологични и технически мерки, които са подходящи и пропорционални на рисковете за постигането на основните цели на мрежовата и информационната сигурност.

Чл. 3. Мерките, които „Проучване и добив на нефт и газ“ АД прилага във връзка с осигуряването на мрежова и информационна сигурност, са насочени към запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия й жизнен цикъл, включващ създаването, обработването, съхранението, пренасянето и унищожението й в и чрез информационните и комуникационните системи на Дружеството.

Чл. 4. В „Проучване и добив на нефт и газ“ АД за мрежовата и информационната сигурност са отговорни членовете на звеното за мрежовата и информационна сигурност в „Проучване и добив на нефт и газ“ АД, като:

- с оглед на спазването на всички изисквания, служителите са на пряко подчинение на изпълнителните директори и пряко ги информират за състоянието и проблемите в мрежовата и информационната сигурност;
- препоръчителни функции на служителите, отговарящи за мрежовата и информационната сигурност, са описани в приложение № 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност и в заповедта за определяне на звеното по мрежова и информационна сигурност.

Чл. 5. Настоящата политика се преразглежда редовно, но не по-рядко от веднъж годишно, и при необходимост се актуализира.

Чл. 6. Служителите имат право да обменят компютърна информация посредством вътрешна компютърна мрежа само във връзека с изпълнение на служебните си задължения и само със служителите, с които имат преки служебни взаимоотношения.

Чл. 7. На служителите на дружеството е строго забранено да използват мобилни компютърни средства на места, където може да възникне риск за средството и информацията в него. Потребителите на мобилни компютърни средства и мобилни телефони отговарят за защитата им от кражба и не ги оставят без наблюдение.

Чл. 8. При извършване на работа от разстояние служителите на дружеството спазват всички изисквания за осигуряване защитата на данните, в т.ч. лични данни на трети лица и/или по класификацията на информацията.

Чл. 9. Криптографските механизми, които се използват от „Проучване и добив на нефт и газ“ АД са съобразени с уязвимостта на информацията към заплахи за нейните конфиденциалност и интегритети с нормативните и регулаторните изисквания към нейното създаване, съхраняване и пренасяне.

Чл. 10. (1) Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.

(2) Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заеманата длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.

Чл. 11. При разработването на нови информационни и комуникационни системи в дружеството се спазват всички изисквания на Наредбата така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда.

Чл. 12. (1) С цел да се намалят загубите от инциденти чрез намаляване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки, „Проучване и добив на нефт и газ“ АД поддържа следната документация:

- опис на информационните активи;
- физическа схема на свързаност;
- логическа схема на информационните потоци;
- документация на структурната кабелна система;
- техническа, експлоатационна и потребителска документация на информационните и комуникационните системи и техните компоненти;
- инструкции/вътрешни правила за всяка дейност, свързана с администрирането, експлоатацията и поддръжката на хардуер и софтуер;
- вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на корпоративната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, системи за документооборот и други вътрешноведомствени системи, принтиране, факс, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.

(2) Документацията по ал. 1 е:

- еднозначно идентифицирана като заглавие, версия, дата, автор, номер и/или др.;
- поддържана в актуално състояние, като се преразглежда и при необходимост се обновява поне веднъж годишно;
- одобрена от изпълнителните директори на дружеството;
- класифицирана по смисъла на чл. 6 от Наредбата за минималните изисквания за мрежова и информационна сигурност;
- достъпна само до тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения.

(3) Дружеството поддържа информация, доказваща по неоспорим начин изпълнението на изискванията на Наредбата. Същата се поддържа в актуално състояние и е достъпна само за:

а) тези лица, които е необходимо да я ползват при изпълнение на служебните си задължения по силата на трудови или договорни отношения;

б) представители на съответните национални компетентни органи съгласно чл. 16, ал. 5 от Закона за киберсигурност;

в) други организации, оправомощени с нормативен акт или договорни отношения.

Чл. 13. (1) При установяване на взаимоотношения с доставчици на стоки и услуги, които са "трети страни", Дружеството договаря изисквания за мрежова и информационна сигурност, включително:

- за сигурност на информацията, свързани с достъпа на представители на трети страни до информация и активите на Дружеството;
- за доказване, че третата страна също прилага адекватни мерки за мрежова и информационна сигурност, включително клаузи за доказването на прилагането на тези мерки чрез документи и/или провеждане на одити;
- за прозрачност на веригата на доставките; третата страна трябва да е способна да докаже произхода на предлагания ресурс/услуга и неговата сигурност;
- последици при неспазване на изискванията за сигурност на информацията;
- отговорност при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност;
- за взаимодействие в случай на възникване на инцидент, който най-малко включва: контактни точки, начин за докладване, време за реакция, време за възстановяване на работата, условия за затваряне на инцидент.

(2) Изпълнителните директори на дружеството определят служител или служители, отговарящи за спазване на изискванията по ал. 1 и параметрите на нивото на обслужване.

Чл. 14. С цел повишаване на квалификацията на служителите и на осведомеността им по отношение на мрежовата и информационната сигурност, настоящата политика е сведена до знанието им.

Чл. 15. Потребителите на информационни системи в дружеството са задължени с отговорни действия да гарантират ефективното и ефикасно използване на системите.

Чл. 16. (1) „Проучване и добив на нефт и газ“ АД извършва анализ и оценка на риска за мрежовата и информационната сигурност регулярно, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите, влизащи в обхвата на Наредбата за минималните изисквания за мрежова и информационна сигурност.

(2) Анализът и оценката на риска са документиран процес по смисъла на чл. 5, ал. 1, т. 6 от Наредбата. В него са регламентирани нивата на неприемливия риск и отговорностите на лицата, участващи в отделните етапи на процеса. Анализът и оценката на риска се извършват по методика, гарантираща съизмерими, относително обективни и повтарящи се резултати. Методиката се одобрява от изпълнителните директори на дружеството и е достъпна за лицата,

на които е възложено да участват в процеса. Може да се прилага препоръчителна методика съгласно приложение № 3 от Наредбата.

(3) На основание на анализа и оценката на риска дружеството изготвя план за намаляване на неприемливите рискове, който включва минимум:

- подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
- необходими ресурси за изпълнение на тези мерки;
- срок за прилагане на мерките;
- отговорни лица.

Раздел II
АНАЛИЗ И ОЦЕНКА НА РИСКА ЗА СИГУРНОСТТА НА ИНФОРМАЦИОННИТЕ И КОМУНИКАЦИОННИТЕ СИСТЕМИ

Чл. 17. Управлението на риска за сигурността на информационните и комуникационните системи е част от политиката за управлението на мрежовата и информационната сигурност в „Проучване и добив на нефт и газ“ АД. По своята същност управлението на риска представлява съвкупност от процеси за идентифициране на потенциалните заплахи към носителите на информация и активите, участващи в предоставянето на електронни услуги, анализ и оценка на рисковете, породени от тези заплахи.

Чл. 18. Основните понятия, част от процеса по управление на риска са както следва:

- конфиденциалност – свойство на информацията да не е предоставена или разкрита на неоторизирани лица (т. 2.12 ISO/IEC 27000).
- интегритет – качество на информацията за точност и пълнота (т. 2.40 ISO/IEC 27000).
- наличност на информация – качество да бъде достъпна и използваема при поискване от оторизирано лице (т. 2.9 ISO/IEC 27000).

Чл. 19. Цел на процеса за управление на риска е да се минимизират загубите от потенциални нежелани събития, настъпили в резултат от реализиране на заплахи към сигурността на мрежите и информационните системи, които биха засегнали конфиденциалността, интегритета и достъпността на информацията, създавана, обработвана, предавана и унищожавана чрез тях Дружеството.

Чл. 20. Методиката за управление на риска има за цел да даде общ подход при анализа и оценката на риска за сигурността на информационните и комуникационните системи, предоставяни от дружеството, с цел получаване на съизмерими, относително обективни и повтарящи се резултати чрез:

- регламентиране на дейностите и тяхната последователност при анализа и оценката на риска за електронните услуги;
- определяне на критериите;
- определяне на приоритетите на риска.

Чл. 21. Анализът и оценката на риска са част от процеса за управлението му и се основават на познаване на всички компоненти, имащи отношение към целите.

Чл. 22. За целите на управлението на сигурността на мрежите и информационните системи е необходимо да се:

- познават всички обекти и субекти, които участват пряко или косвено в дейностите, попадащи в обхвата на Наредбата (информационни и комуникационни системи с прилежащия им хардуер, софтуер и документация; поддържащите ги системи (електрозахранващи, климатизиращи и др.); оперативни процеси/дейности; служители и външни организации), наричани за краткост "информационни активи";
- идентифицират и анализират всички потенциални нежелани събития с тях, наричани за краткост "заплахи", които биха довели до загуба на конфиденциалност, интегритет и достъпност на електронните услуги и/или информацията в тях;
- оцени вероятността от настъпване на тези събития, като се вземат предвид слабостите (уязвимостите) на информационните активи и мерките, които са предприети за справяне с тях;
- оцени въздействието (загуби на ресурси (време, хора и пари), неспазване на нормативни и регулаторни изисквания, накърняване на имидж, неизпълнение на стратегически и оперативни цели и др.) от евентуално настъпване на тези нежелани събития въпреки предприетите мерки;
- оцени рискът за сигурността;
- набележат мерки за смекчаване на рисковете с висок приоритет.

Чл. 23. При анализ и оценка на риска Дружеството използва регистър на рисковете (риск- регистър).

Чл. 24. В риск-регистъра се нанасят всички информационни активи, имащи отношение към обхвата на Наредбата:

- информационни системи;
- хардуерни устройства, с които са реализирани информационните системи;
- софтуери, с които са реализирани информационните системи;
- бази данни, включително лични данни по смисъла на GDPR;
- записи за събитията (логове, журнали) на информационните системи;
- документация на информационните системи (експлоатационна и потребителска);
- комуникационни системи;
- хардуерни устройства, с които са реализирани комуникационните системи;
- фърмуерът на тези устройства;
- софтуери на комуникационните системи;
- записи за събитията (логове, журнали);
- документация (експлоатационна и потребителска);

- поддържащи системи (електрозахранващи, климатични);
- системи за контрол на физическия достъп и на околната среда;
- процеси/дейности, свързани с управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
- документация на тези процеси и дейности;
- служители, имащи отговорности към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;
- външни организации, имащи отношение към управлението, експлоатацията и поддръжката на информационните и комуникационните системи;

Чл. 25. (1) За всеки от информационните активи в риск-регистъра на Дружеството се нанасят заплахите/нежеланите събития, които биха довели до нарушаване на конфиденциалността, интегритета и достъпността на информацията.

(2) Дружеството отчита всички потенциални заплахи, произтичащи вътре или извън администрацията, настъпили случайно или преднамерено, като се има предвид уязвимостта на информационния актив към съответната заплаха.

Чл. 26. В риск-регистъра на Дружеството за всяка заплаха се вписва какви мерки са предприети срещу нея.

Чл. 27. В риск-регистъра за всяка заплаха се вписва оценката за нейното въздействие – щетите (материални и нематериални), които дадена заплаха може да причини, ако се реализира. За оценка на въздействието се използва петстепенна скала от 1 до 5, като при 1 щетите са незначителни, а при 5 са най-големи.

Чл. 28 (1) Определя се вероятността за възникване на дадена заплаха, като се вземат предвид предприетите вече мерки. Колкото повече са предприетите защитни мерки, толкова по-ниска е вероятността от възникване на заплахата. При оценка на вероятността се вземат предвид следните фактори:

- за реализиране на преднамерени заплахи: ниво на необходимите умения, леснота на достъпа, стимул и необходим ресурс;
- за реализиране на случайни заплахи: година на производство на хардуера и софтуера, ниво на поддръжката им, квалификация на поддържащия персонал, ресорно обезпечаване на експлоатационните процеси, контрол върху тях и др.
- В риск-регистъра за всяка заплаха се нанася оценката за нейното въздействие.

Чл. 29. За оценка на въздействието се използва петстепенна скала от 1 до 5 и като се има предвид определен период, например една година:

вероятността от реализирането на заплахата е под 10 %;

вероятността от реализиране на заплахата е от 10 % до 30 %;

вероятността от реализиране на заплахата е от 30 % до 50 %;

вероятността от реализиране на заплахата е от 50 % до 70 %;

вероятността от реализиране на заплахата е над 70 %.

Чл. 30. За получаване на оценката на риска се използва следната формула:

(Оценка на въздействие х Оценка на вероятност) = Оценка на риска

Чл. 31. С цел прилагане на пропорционални на заплахите механизми за защита в Дружеството се прави приоритизация на рисковете на база на тяхната оценка и праговете, заложени в Наредбата.

Чл. 32. (1) Приема се, че за рискове с приоритет 3 по смисъла на Наредбата не се изисква предприемане на допълнителни мерки за смекчаване на заплахите, които ги пораждат.

(2) За рисковете с приоритет 2 по смисъла на Наредбата се прави анализ на възможните мерки, които биха могли да се предприемат за смекчаването им, и се преценява дали разходът на ресурси за прилагането им е пропорционален на щетите от реализиране на заплахата. В случай че щетите са повече от разходите, се определят отговорно лице и срок за прилагане на тези мерки.

(3) За всички рискове с приоритет 1 се определят отговорни лица, планират се мерки, които биха намалили риска от реализиране на конкретната заплаха, и се определят срокове за прилагането им.

Чл. 33. (1) Отговорните лица за съответните рискове организират прилагането на планираните мерки за защита и наблюдават инцидентите и щетите, свързани с тях. При необходимост инициират нов анализ и оценка на риска за тази заплаха.

(2) Ръководството на дружеството организира периодично, но не по-малко от веднъж в годината, анализ и оценка на риска, както и при всяко изменение в информационната и/или комуникационната инфраструктура промяна на административната структура и функциите.

Раздел III
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Ръководителите и служителите на дружеството са длъжни да познават и спазват разпоредбите на настоящата Политика.

§2. Контролът по спазване на приетата Политика се осъществява от звеното за мрежовата и информационната сигурност на използваните информационни системи в дружеството

§3. Настоящата Политика за мрежова и информационна сигурност се разглежда и оценява периодично с оглед ефективността й, като Дружеството може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тази Политика е разработена на основание чл. 4 от Наредба за минималните изисквания за мрежова и информационна сигурност и влиза в сила от деня на утвърждаването й със Заповед № 202/27.08.2021г. на изпълнителните директори на Дружеството.

§ 5. Настоящата политика е актуализирана в съответствие със Заповед № 174/01.08.2022г. на изпълнителните директори на дружеството.