Групата ЕНЕРГО-ПРО

ПОЛИТИКА ЗА СИГУРНОСТ

2026

ENERGO-PRO

ПОЛИТИКА ЗА СИГУРНОСТ („ПОЛИТИКАТА“)

1. Въведение

Основната дейност на ЕНЕРГО-ПРО а.с. („ЕНЕРГО-ПРО“) и неговите дъщерни дружества (заедно наричани „Групата“) е производството на енергия от възобновяеми източници. Допълнителните дейности на Групата включват разпределение, снабдяване и търговия с електроенергия.

ЕНЕРГО-ПРО се ангажира да защитава сигурността на служителите, участниците във веригата на създаване на стойност, посетителите и общностите, засегнати от неговата дейност. ЕНЕРГО-ПРО спазва принципите, заложени във Всеобщата декларация за правата на човека на Организацията на обединените нации, Ръководните принципи на ООН относно бизнеса и правата на човека, Доброволните принципи за сигурност и правата на човека (VPSHR) и Декларацията на Международната организация на труда относно основните принципи и права при работа.

Настоящата политика установява стандарт на ниво Група за управление на сигурността в рамките на дейностите и проектите на ЕНЕРГО-ПРО и определя изискванията за идентифициране, предотвратяване и управление на рисковете, свързани със сигурността, по начин, съответстващ на приложимото законодателство, добрата международна индустриална практика (ДМИП), Кодекса за поведение на Групата, Политиката на Групата относно правата на човека и други приложими политики на ЕНЕРГО-ПРО. Процедурите, плановете и контролните механизми на ниво държава могат да определят по-подробни изисквания, съобразени с местните правни, оперативни условия и разпоредби за сигурност, при условие че остават в съответствие с настоящата политика на Групата. Изискванията, съдържащи се в тази политика, са съобразени със съществените рискове за правата на човека, свързани със сигурността в ЕНЕРГО-ПРО, включително отношението към работниците и общностите, поведението на персонала по сигурността и управлението на конфликти и употребата на сила.

2. Цели

Целите на настоящата политика са:

• Да осигури сигурна работна среда за всички служители, участници във веригата на създаване на стойност (изпълнители, подизпълнители и други) и посетители.

• Да поддържа и защитава сигурността и целостта на дейностите, съоръженията и активите.

• Да създаде и поддържа взаимоотношения, основани на доверие, взаимно уважение и почтеност, с общностите, местните органи и други заинтересовани страни.

• Да осигури насоки и да изгради отговорност на ниво ръководство, мениджмънт и служители.

• Да зачита и демонстрира добра международна индустриална практика по отношение на правата на човека и сигурността.

3. Ръководство

Съветът на директорите на Групата и на дъщерните дружества на ЕНЕРГО-ПРО носят отговорност за осигуряване прилагането на настоящата политика. Висшето ръководство трябва да гарантира, че Политиката е интегрирана в съответните бизнес процеси и операции.

4. Обхват

Политиката се прилага за всички служители и за нашата верига на създаване на стойност.

Настоящата политика се прилага за ЕНЕРГО-ПРО, за дъщерните дружества на ЕНЕРГО-ПРО, функциониращи в България и Грузия, както и за дъщерното дружество „Мурат Нехри Електрик Юретим“ А.Ш., опериращо в Турция.

Тя се прилага също така за всички останали дъщерни дружества на ЕНЕРГО-ПРО, които обаче могат да поискат от Съвета на директорите на Групата одобрение за изключване от прилагането на конкретни разпоредби на настоящата политика. Съветът на директорите на Групата може да одобри такова искане, когато е убеден, че изключването се основава на обективни и търговски

обосновани причини и освен това е съобразено с местното законодателство, Кодекса за поведение на Групата и обвързващите ангажименти по финансиране. Одобрените изключения се документират и се споделят с ESG отдела на Групата.

Очакваме всички, които работят с нас и за нас, да спазват еквивалентни стандарти и можем да предприемаме действия за оценка на съответствието с тези принципи като част от нашите бизнес процеси.

5. Изисквания

ЕНЕРГО-ПРО потвърждава необходимостта от изграждане на култура на осведоменост и дисциплина по отношение на сигурността, особено при работа в отдалечени или сложни среди. Конкретните изисквания на настоящата политика имат за цел да установят минимален стандарт на ниво Група и се прилагат, доколкото е приложимо, спрямо правния, оперативния контекст и този на сигурността във всяка държава, офис, проект или дейност.

1. Управление на сигурността

Съветът на директорите на съответното бизнес звено носи отговорност за сигурността на всички офиси и дейности/проекти и за назначаването на надлежно квалифициран персонал за управление на сигурността. Всички строителни и експлоатационни обекти следва да разполагат с мерки и контрол за сигурност, включително, когато е приложимо, оценки на риска за сигурността при строителство/експлоатация, както и механизми за докладване и управление на инциденти, свързани със сигурността. В зависимост от нивото на заплаха, активите, разположени в среда с повишен риск за сигурността, следва също да разполагат с планове за управление на сигурността[1]. Съветът на директорите на съответното бизнес звено носи отговорност за оценка на съществеността на риска за сигурността чрез анализ на съответните заплахи и рискове и съответно определяне на необходимото ниво на мерките за сигурност.

[1] Насоки относно управлението на сигурността са налични в „Good Practice Handbook: Use of Security Forces: Assessing and Managing Risks and Impacts“, 2017 г., уебсайт на IFC.

Следните съображения се включват в управлението на сигурността:

I. Класификация на активите за бизнес звена с висок риск за сигурността: Преди извършването на каквато и да е оценка на риска всички активи по проекта трябва да бъдат идентифицирани и класифицирани в четири основни категории: човешки (персонал и изпълнители), физически (инфраструктура и оборудване), информационни (интелектуална собственост и данни) и репутационни (репутация и имидж на марката). На всяка категория се определя ниво на критичност с цел приоритизиране на мерките за защита и разпределението на ресурсите.

II. Оценка на риска за сигурността: Всички бизнес звена следва да извършват оценка на рисковете за сигурността, като степента на задълбоченост на оценката зависи от съществеността на риска за сигурността за съответното звено. Оценките се извършват с цел идентифициране на съществуващите и предвидимите рискове за сигурността, свързани с проекта/дейностите, и включват контролни и смекчаващи мерки за управление на тези рискове. Необходимо е да бъдат осигурени достатъчни финансови и човешки ресурси за прилагането на установените контролни мерки, както и за тяхното поддържане и наблюдение.

Оценката следва да отчита международните, правните и вътрешните изисквания на дружеството. Оценките на риска се преразглеждат в зависимост от нивото на заплаха или след съществен инцидент, свързан със сигурността, или промяна в дейността. Честотата на оценките на риска се определя въз основа на: (i) исторически фактори; (ii) политически фактори; (iii) социално-икономически фактори; (iv) етнически въпроси; (v) религиозни съображения; (vi) наличие или предполагаемо наличие на терористични групи или екстремисти; (vii) опортюнистична престъпна дейност; (viii) правни изисквания и изисквания за съответствие; (ix) местоположение; и (x) съществени конфликти в общността.

На високо ниво, ad hoc рисковете за сигурността на ниво държава могат да бъдат оценявани периодично от Съвета на директорите на Групата в сътрудничество със съответните бизнес звена.

Оценките на риска ще вземат предвид следните заплахи:

Физически заплахи за сигурността:

- ✓ Въоръжено нападение (терористично или престъпно)
- ✓ Отвличане, искане на откуп и изнудване
- ✓ Кражби и вандализъм
- ✓ Национални или местни граждански безредици
- ✓ Нестабилност или срив на правителството в приемащата държава
- ✓ Оперативни и екологични заплахи
- ✓ Заплахи, свързани с транспорта
- ✓ Рискове, свързани с настаняването
- ✓ Географски и климатични събития
- ✓ Отдалеченост и ограничен достъп до спешна помощ
- ✓ Социално-икономическо напрежение
- ✓ Етнически или религиозни конфликти
- ✓ Конфликти в общността или прекомерни оплаквания
- ✓ Наличие или предполагаемо наличие на терористични или екстремистки групи
- ✓ Социално-политически и свързани с общността заплахи

Нефизически заплахи:

- ✓ Сплашване или принуда
- ✓ Заплахи от страна на служители, включително синдикални членове
- ✓ Икономическа принуда, включително изнудване
- ✓ Увреждане на репутацията или имиджа на марката
- ✓ Информационни и технологични заплахи
- ✓ Прекъсване на ИТ системи и оперативни прекъсвания
- ✓ Рискове за киберсигурността, засягащи дейностите, инфраструктурата и личните данни
- ✓ Културни недоразумения и местни чувствителни въпроси

III. Планове за управление на сигурността: Бизнес звената, разположени в среди с висок риск за сигурността, следва да разполагат с планове за управление на сигурността. Тези планове се адаптират към изискванията на съответния проект/дейност и са съобразени с конкретната цел. Плановете определят как всеки проект/дейност ще осигурява сигурност и ще смекчава свързаните рискове. Те отчитат спецификите на обекта, включително културни, географски и политически фактори. В Плана за управление на сигурността изрично се посочва, че употребата на сила следва да бъде съразмерна, законосъобразна и строго ограничена до ситуации, при които е необходимо да се защити живот или да се предотврати сериозна вреда.

Ролите и отговорностите следва да бъдат ясно определени в съответствие с установените нива на риск, като се гарантира съответствие с мащаба и сложността на рисковете и приложимост към конкретната дейност.

Планът за управление на сигурността включва раздел относно управление и докладване на инциденти. Този раздел описва последователен подход за идентифициране, докладване, оценка, управление и реакция при инциденти, свързани със сигурността. В него се определят също ролите и отговорностите за управление и докладване на инциденти.

IV. План за непрекъсваемост на дейността (BCP): Бизнес звената с висок риск подготвят план за непрекъсваемост на дейността, съобразен със специфичната среда на заплахи. Тези планове определят ясни протоколи за незабавна реакция при реализирани заплахи (например въоръжени нападения, отвличания или пробиви в ИТ системите) и дефинират стъпките за възстановяване с цел осигуряване устойчивост на дейността при минимални прекъсвания.

V. Планове за извънредни ситуации и евакуация: Извънредните ситуации, свързани със сигурността, се включват в индивидуалните планове за готовност и реакция при извънредни ситуации за съответните активи. Освен това бизнес звената с висок риск поддържат план за реагиране при инциденти, свързани със сигурността (SIRP), както и процедури за

евакуация, включително маршрути за евакуация, предназначени да осигурят координирана и ефективна реакция при инциденти.

VI. Непрекъснат преглед и подобрение: Плановете и контролните механизми за сигурност се преглеждат редовно и се актуализират след всеки съществен инцидент. Процесът на анализ след събитие идентифицира пропуски с цел гарантиране, че мерките за смекчаване остават адаптивни, проактивни и подходящи за целта.

2. Надлежна проверка на изпълнители в областта на сигурността

Преди ангажирането на изпълнители в областта на сигурността, ЕНЕРГО-ПРО чрез своите офиси по държави извършва надлежна проверка на потенциалния изпълнител с цел установяване на неговия опит по отношение на правата на човека, съответните квалификации и спазването на приложимите законови изисквания. Примерен въпросник от Оценката за съответствие с правата на човека (HRCA) може да бъде предоставен при поискване от централата за целите на извършване на надлежната проверка. Изпълнителите в областта на сигурността са длъжни да осигурят обучение за осведоменост относно правата на човека за целия си персонал, включително обучение за подходящо поведение спрямо работници, общности и други заинтересовани страни, съобразно тяхната роля. При липса на такова обучение, офисите на ЕНЕРГО-ПРО по държави ще го осигурят.

3. Общности и местни органи

При разработването и прилагането на планове за сигурност на обектите следва да се отчита въздействието върху общностите. Персоналът по сигурността трябва да работи в тясно сътрудничество със съответните социални екипи с цел минимизиране на отрицателните въздействия върху местните общности и подпомагане на подходяща комуникация и ангажираност, когато е приложимо.

ЕНЕРГО-ПРО признава значението на изграждането на добри работни взаимоотношения с общностите и местните органи. Всички обекти с персонал по сигурността следва да създадат подходящи процеси за

управление на въпросите, свързани със сигурността на общностите, съобразно спецификата на обекта.

4. Права на човека

ЕНЕРГО-ПРО е разработило Политика за правата на човека, която определя принципите относно нашите очаквания в тази област. Политиката включва рисковете за правата на човека, свързани със сигурността и конфликтите.

ЕНЕРГО-ПРО гарантира, че служителите, изпълнителите и персоналът по сигурността получават подходящо обучение за осведоменост относно правата на човека.

5. Отговорност

- Висшето ръководство, включително ръководителите на обекти, носят крайната отговорност за сигурността.
- Висшето ръководство следва да демонстрира ангажираност чрез осигуряване на достатъчни финансови и човешки ресурси за създаване и поддържане на сигурна среда.
- Всички инциденти, свързани със сигурността, както и жалбите от общностите, свързани със сигурността, се съобщават незабавно на висшето ръководство, включително доклади от разследвания и съответните контролни мерки.

6. Комуникация

Настоящата политика се разпространява най-малко веднъж годишно до всички служители и участници във веригата на създаване на стойност чрез различни канали, включително програми за въвеждане в работата, обучения, корпоративния уебсайт, имейл и SMS съобщения, информационни табла в офисите, договори с изпълнители и други средства за комуникация.

В допълнение, всяко бизнес звено е длъжно да демонстрира как интегрира и спазва настоящата политика, включително чрез надлежна проверка на изпълнителите в областта на сигурността, обучение и комуникиране на тези изисквания в рамките на веригата на създаване на стойност.

7. Разпространение

Настоящият документ е достъпен на уебсайта на дружеството, включен е в избрани стандартни общи условия за осъществяване на дейността и може да бъде преразглеждан редовно въз основа на обратна връзка от заинтересованите страни и в отговор на регулаторни промени.

8. Влизане в сила

Настоящата версия на Политиката влиза в сила и се прилага, считано от май 2026 г.