

Додаток 3
до наказу ПрАТ «Укргідроенерго»
від «04» 03 2026 р. № 94-Н

ПОЛІТИКА
інформаційної безпеки ПрАТ «Укргідроенерго»

м. Вишгород
2026

1. ЗАГАЛЬНІ ВІДОМОСТІ

ПрАТ «Укргідроенерго» (далі – Товариство) – це найбільша гідроенергуюча компанія України, що включена до переліку 15 найбільших підприємств державного сектору економіки, сумарні активи яких становлять 70 відсотків від загального показника у держсекторі. До складу Товариства входять станції (філії) Дніпровського та Дністровського каскаду, а саме: «Каскад Київських ГЕС і ГАЕС», «Канівська ГЕС», «Кременчуцька ГЕС», «Середньодніпровська ГЕС», «Дніпровська ГЕС», «Дністровська ГЕС» та «Дирекція з будівництва Дністровської ГАЕС», «Каховська ГЕС ім. П. С. Непорожнього».

Слова «керівник», «працівник», «який» далі за текстом читати як «керівник / керівниця», «працівник / працівниця», «фахівець / фахівчиня», «який / яка».

Місія: Генерувати екологічно чисту електричну енергію в сучасний та надійний спосіб, забезпечувати енергетичну стабільність і безпеку України, сприяти економічному розвитку й конкурентоспроможності держави.

Бачення: Стратегічною місією Товариства є забезпечення енергосистеми України електроенергією та резервом потужності завдяки гідроресурсам річок Дніпро та Дністер. Товариство, використовуючи гідроенергетичний потенціал великих гідроелектростанцій та гідроакумуючих електростанцій, усуває дефіцит Об'єднаної енергетичної системи України щодо маневрових потужностей, розвиває альтернативні та відновлювані джерела енергії, використовує енергоефективне обладнання, цифрові системи керування технологічними процесами, сучасні матеріали та будівельні технології тощо.

Шляхом впровадження визнаних стандартів, в тому числі з інформаційної безпеки, Товариство реалізує безперервне виконання покладених на нього завдань і досягнення місії. Крім того, забезпечується збереження наявних матеріальних активів, а також здоров'я власних працівників та громад, на території яких функціонують промислові системи Товариства.

2. МЕТА ПОЛІТИКИ

Ця Політика є частиною нормативної бази ПрАТ «Укргідроенерго» з питань забезпечення інформаційної безпеки та визначає основні напрями і принципи забезпечення інформаційної безпеки ПрАТ «Укргідроенерго» відповідно до вимог стандарту ДСТУ ISO/IEC 27001:2023 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2023)».

У межах цієї Політики також визначаються загальні принципи забезпечення захисту персональних даних, що обробляються Товариством, відповідно до вимог Закону України «Про захист персональних даних» та інших нормативно-правових актів України.

3. СФЕРА ЗАСТОСУВАННЯ ПОЛІТИКИ

Вимоги Політики поширюються на процеси та персонал апарату управління та філій ПрАТ «Укргідроенерго», які забезпечують:

- функціонування операційних процесів керування, контролю та планування діяльності ПрАТ «Укргідроенерго». Ключовим процесом з цього переліку є реалізація / продаж електроенергії на ринку електричної енергії України;
- функціонування технологічних систем (далі – ОТ систем), що залучені до виробництва електроенергії. Ключовими процесами є процеси налагодження

параметрів та моніторингу функціонування обладнання генерації електроенергії.

Вимоги цієї Політики також застосовуються до процесів та інформаційних систем, у межах яких Товариство здійснює обробку персональних даних, а також до працівників і третіх сторін, які мають доступ до таких персональних даних.

Крім того, вимоги Політики будуть поширюватись на інші організації, установи та фізичних осіб, які взаємодіють із Товариством, як-от постачальники або клієнти.

4. ОБ'ЄКТИ ЗАХИСТУ

ПрАТ «Укргідроенерго» шляхом впровадження технічних, адміністративних та організаційних заходів і засобів забезпечує захист необхідних для забезпечення внутрішньої операційної діяльності та взаємодії з партнерами:

- власної інформації та інформації партнерів, в тому числі – конфіденційної;
- власних інформаційних систем, що забезпечують обробку інформації;
- власних ОТ систем, що забезпечують налагодження параметрів та моніторинг функціонування обладнання генерації електроенергії;
- персональних даних, що обробляються Товариством у межах трудових відносин, договірної діяльності, взаємодії з контрагентами, державними органами та інших процесів.

5. МЕТА ЗАХИСТУ

Метою впровадження Системи управління інформаційною безпекою (далі – СУІБ) є потреба:

- забезпечити необхідний рівень доступності інформації та інформаційних систем, що необхідні для виконання завдань Товариства та реалізації її Місії;
- забезпечити кіберзахист від втручання та достатні показники безперервності функціонування ОТ систем, що забезпечують налагодження параметрів та моніторинг функціонування обладнання генерації електроенергії;
- попередити виток та несанкціоновану модифікацію інформації Товариства і партнерів / третіх сторін, обробка якої виконується засобами Товариства;
- забезпечити відповідність операційної діяльності Товариства вимогам законодавства країн, у яких надаються послуги з питань інформаційної безпеки;
- забезпечити відповідність операційної діяльності Товариства запитам / вимогам клієнтів, що пов'язані з інформаційною безпекою;
- забезпечити безпечну взаємодію Товариства з партнерами / третіми сторонами під час взаємодії;
- забезпечити законну обробку та належний захист персональних даних, що обробляються Товариством, відповідно до вимог законодавства України;
- забезпечити виявлення, фіксацію та реагування на порушення безпеки персональних даних (несанкціонований доступ, втрата, знищення, незаконне розповсюдження) у межах встановлених процедур.

6. ПРИНЦИПИ РЕАЛІЗАЦІЇ ПОЛІТИКИ

Для досягнення поставленої мети Товариство має намір керуватися такими принципами:

- законність: Товариство не використовує засоби та заходи, що порушують чинне законодавство та договірні зобов'язання;
- залучення вищого керівництва: діяльність ініційована і контролюється вищим керівництвом Товариства;
- економічна доцільність: Товариство прагне обирати заходи захисту з урахуванням витрат на їх реалізацію, ймовірності виникнення загроз інформаційній безпеці та обсягу можливих втрат від їх реалізації;
- комплектність та системність: інформаційна безпека реалізується на правовому, адміністративному, процедурному та програмно-технічному рівнях;
- персональна відповідальність: працівники та керівництво Товариства, а також представники третьої сторони, які взаємодіють з Товариством, несуть відповідальність за дотримання вимог інформаційної безпеки;
- мінімальна достатність: доступ до інформаційних ресурсів Товариства надається виключно за виробничою потребою та на рівні мінімально необхідних повноважень для виконання працівниками Товариства своїх посадових обов'язків;
- контроль доступу та конфіденційність персональних даних: доступ до персональних даних надається виключно уповноваженим особам, а передача персональних даних третім сторонам здійснюється лише за визначеними підставами та з урахуванням встановлених заходів безпеки.

7. ОBOB'ЯЗКИ КЕРІВНИЦТВА

Керівництво Товариства бере на себе повну відповідальність і приймає зобов'язання:

- забезпечити підтримку та постійне вдосконалення СУІБ;
- довести до відома всіх працівників Товариства, на яких поширюється дія сфери застосування СУІБ, вимоги цієї Політики;
- вдосконалювати СУІБ за рахунок впровадження процесного менеджменту, постановки цілей і проведення аналізу функціонування системи управління з боку керівництва;
- забезпечити СУІБ всіма необхідними ресурсами для досягнення поставлених цілей;
- забезпечити визначення відповідальних осіб / підрозділів за організацію заходів із захисту персональних даних та контроль виконання вимог законодавства України у сфері захисту персональних даних;
- забезпечити затвердження та підтримку в актуальному стані внутрішніх документів з питань обробки та захисту персональних даних (політики / положення, процедури, реєстри, порядки реагування на інциденти).

8. ПЕРЕГЛЯД ПОЛІТИКИ

Ведеться робота з постійної підтримки документа в актуальному стані. Документ повинен переглядатися за необхідністю, але не рідше одного разу на рік.

Відповідальність за внесення змін до Політики покладається на начальника центру інформаційної безпеки та кіберзахисту департаменту безпеки.