ЗАТВЕРДЖУЮ
Голова Громадської організації
«Світова асоціація з питань тварин України»
_____ О.В.Кошак
01.06.2022

ПОЛІТИКА БЕЗПЕКИ ДАНИХ

Положення про безпеку даних (інформаційну безпеку) Громадської організації «Світова асоціація з питань тварин України»

1. Загальні поняття та сфера застосування

1.1. Визначення термінів:

- Бізнес-процес - структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу діяльності, метою якої є отримання заданого результату, що має цінність для ГО.
- Загроза - потенційна причина небажаного інциденту, яка може призвести до шкоди для системи або організації.
- Інформаційна безпека - захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризику бізнес-процесів і отримання максимальної рентабельності інвестицій і бізнес-можливостей.
- Несанкціонована особа, об'єкт або процес - особа, об’єкт або процес, які не контролюються ГО та/або не задовольняють вимоги, які до них висуваються.
- Санкціонований об'єкт - об’єкт, який контролюється ГО та/або задовольняє вимоги, які до нього висуваються.
- ГО — Громадська організація «Світова асоціація з питань тварин України»

1.2. Дана Політика обов’язкова для застосування відповідальною особою, працівниками та членами ГО

2. Мета політики

Дані (інформація) є ресурсом, який, як і інші важливі бізнес-ресурси, має певну цінність для ГО а, отже, потребує відповідного захисту.

Метою Політики є реалізація заходів, направлених на захист ГО від можливого нанесення їй матеріальної, репутаційної чи іншої шкоди, яка може бути нанесена за допомогою випадкового або навмисного впливу на об’єкти захисту.

Зазначена мета досягається шляхом забезпечення властивостей об’єктів захисту, таких як доступність, цілісність та конфіденційність.

Необхідний рівень доступності, цілісності і конфіденційності забезпечується впровадженням організаційних та технічних заходів, розроблених на підставі оцінки властивих об’єктам захисту ризиків інформаційної безпеки.

3. Об’єкти захисту

3.1. Серед основних об'єктів на які розповсюджується дія інформаційної безпеки ГО розглядаються наступні види ресурсів:

• інформаційні ресурси - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання співробітників, партнерів ГО, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;

• програмне забезпечення - прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується ГО, співробітниками та системами для роботи та взаємодії з контрагентами та іншими внутрішніми та зовнішніми системами тощо;

• фізичні ресурси - співробітники, апаратні засоби IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми тощо), носії даних (стрічки, диски тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо.

• сервісні ресурси - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи (а також їх співробітники), послугами яких користується ГО для отримання, використання, передачі та знищення ресурсів.

3.2. Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто ГО використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків діяльності.

3.3. Для забезпечення необхідного рівня функціонування ГО повинний бути забезпечений захист:

- автоматизованої системи ГО: комплексу апаратних та програмних засобів, призначених для автоматизації бізнес-процесів ГО;
- приміщень, в яких розміщені елементи автоматизованої системи ГО;
- інформації, яка обробляється і зберігається в автоматизовані системі ГО.

3.4. Персонал є окремою категорією, на яку необхідно звернути увагу з метою забезпечення інформаційної безпеки ГО.

4. Принципи реалізації Політики

4.1. Для досягнення поставленої мети Підприємство має намір керуватися наступними принципами:

- законність: Підприємство реалізує заходи забезпечення інформаційної безпеки у відповідності до чинного законодавства та договірних зобов'язань;
- залучення вищого керівництва ГО в процес забезпечення інформаційної безпеки: діяльність ініційована і контролюється вищим керівництвом ГО;
- економічна доцільність: Підприємство прагне обирати заходи забезпечення інформаційної безпеки 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 ГО, а також представники третьої сторони, які взаємодіють з Підприємством, несуть відповідальність за дотримання вимог інформаційної безпеки;
- мінімальна достатність: доступ до інформаційних ресурсів ГО надається виключно за службовою необхідністю та на рівні мінімально необхідних повноважень;
- врахування вимог інформаційної безпеки у проектній діяльності: розробка та документування вимог до продуктів з інформаційної безпеки здійснюється на всіх етапах реалізації проектів.
- цілісність: властивість захищеності, безпомилковості та повноти ресурсів ГО.
- конфіденційність: властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.
- доступність: властивість доступності та можливості використання ресурсів ГО на вимогу санкціонованого об'єкта.
- спостережність: властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів. Це в першу чергу стосується інформації з обмеженим доступом, до якої відносяться відомості що становлять комерційну таємницю, персональні дані та іншу конфіденційну інформацію.

5. Область дії

5.1. Викладені в документі принципи забезпечення інформаційної безпеки поширюються на всі підрозділи ГО з області дії системи управління інформаційною безпекою, а також поширюються на інші організації, установи та фізичні особи, які взаємодіють з ГО в якості постачальників або споживачів інформаційних ресурсів ГО.

5.2. ГО забезпечує виконання усіх вимог інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів.

6. Додаткові умови

ГО залишає за собою право змінити умови даної Політики в будь-який час.