

Посада

Підпис

Затверджено:

Директор ТОВ «МАКК Системс»

Кунда П.М.



MAKK
SYSTEMS

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Система управління інформаційною безпекою

Код документу:

ІБ.ПЛ-001

Версія документу

1.0

Дата затвердження

17.05.2021

Дата наступного
перегляду:

январь 2022

Посада

Підпис

Розроблено:

Керівник проектів Драч М.Д.

Київ 2021

1. Призначення документу

Політика інформаційної безпеки (далі - Політика) ТОВ «МАКК Систем» (далі Товариство) – це відкритий документ, який визначає та встановлює базові принципи забезпечення інформаційної безпеки та наміри керівництва Товариства їх дотримуватись відповідно до вимог ISO/IEC 27001:2013 Information security management systems. Requirements (пункти 5.2 и 5.3).

2. Область дії документу

Викладені в документі принципи забезпечення інформаційної безпеки поширюються на всі підрозділи Товариства та його партнерів / клієнтів / постачальників, які задіяні в забезпечення функціонування бізнес-процесів з області дії Системи управління інформаційною безпекою, або користуються їх результатами. До зазначених бізнес-процесів відносяться:

- ✓ бізнес-процес «Розробка програмного забезпечення»;
- ✓ бізнес-процес «Підтримка програмних та апаратних засобів»;
- ✓ бізнес-процес «Управління змінами в інформаційних системах».

3. Скорочення / визначення.

Конфіденційність – характеристика інформації, яка визначає доступ до інформації тільки уповноваженим особам або системам.

Цілісність – характеристика інформації, що визначає зміну інформації тільки уповноваженими особами або системами і тільки дозволеним способом.

Доступність – характеристика інформації, яка визначає доступність інформації тільки уповноваженим особам, коли їм це необхідно.

Інформаційна безпека – збереження конфіденційності, цілісності та доступності інформації.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління Компанії, яка займається плануванням, впровадженням, підтримкою, аналізом і поліпшенням інформаційної безпеки.

Вище керівництво Товариства – несе відповідальність за загальну конфіденційність і безпеку компанії.

Керівник служби інформаційної безпеки – співробітник/роль, відповідальний координацією зусиль та звітність щодо інформаційної безпеки, за внесення змін до Політики покладається на Керівника служби інформаційної безпеки.

Третя сторона – будь-яка організація (приватна чи державна), відомство чи регулюючий постачальники товарів орган, які взаємодіють з Товариством. До третьої сторони можуть відноситись:

- постачальники послуг
- виконавці робіт
- міжнародні та громадські організації

- державні підприємства та інші

Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (Закон України «Про захист персональних даних», Стаття 2. Визначення термінів).

4. Об'єкти захисту

Для забезпечення необхідного рівня функціонування Товариства повинний бути забезпечений захист:

- ✓ автоматизованої системи Товариства: комплексу апаратних та програмних засобів, призначених для автоматизації бізнес-процесів;
- ✓ приміщень, в яких розміщені елементи автоматизованої системи Товариства;
- ✓ інформації, яка обробляється і зберігається в автоматизованій системі Товариства;
- ✓ окремим об'єктом захисту Товариство вважає персональні дані співробітників Товариства та власних клієнтів;
- ✓ персонал Товариства та процеси взаємодії з третьою стороною.

5. Мета захисту

Метою Політики є визначення необхідності проведення заходів, направлених на захист Товариства від можливого нанесення йому 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 та впровадження циклічної моделі керування інформаційною безпекою: «планування - реалізація - перевірка - вдосконалення».

Товариство вважає, що впровадження заходів з інформаційної безпеки дозволить:

- ✓ забезпечити захист інформації та ресурсів Товариства від зовнішніх і внутрішніх загроз та загроз, пов'язаних з навмисними та ненавмисними діями працівників Товариства;
- ✓ підвищити конкурентоспроможності Товариства;
- ✓ забезпечити відповідність вимогам законодавства і договірних зобов'язань в частині інформаційної безпеки;
- ✓ підвищити ділову репутацію та корпоративну культуру Товариства;
- ✓ забезпечити адекватність заходів захисту загрозам інформаційної безпеки;
- ✓ запобігти та (або) мінімізувати наслідки від реалізації загроз інформаційної безпеки.

6. Сфера застосування документу

Політика поширюється на:

- ✓ працівників Товариства;
- ✓ клієнтів та партнерів Товариства;

- ✓ інформацію, яка циркулює та оброблюється в продуктах/інформаційних системах розроблених Товариством;
- ✓ обладнання та програмне забезпечення, які забезпечують функціонування Товариства.

7. Принципи реалізації Політики

Для досягнення поставленої мети Товариство має намір керуватися наступними принципами:

- ✓ *законність*: Товариство реалізує заходи забезпечення інформаційної безпеки у відповідності до чинного законодавства та договірних зобов'язань;
- ✓ *залучення вищого керівництва Товариства в процес забезпечення інформаційної безпеки*: діяльність ініційована і контролюється вищим керівництвом Товариства;
- ✓ *економічна доцільність*: Товариство 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 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 службовою необхідністю та на рівні мінімально необхідних повноважень;
- ✓ *врахування вимог інформаційної безпеки у проектній діяльності*: розробка та документування вимог до продуктів / послуг з інформаційної безпеки здійснюється на всіх етапах реалізації проектів.

8. Обов'язки керівництва

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

- ✓ забезпечити підтримку та постійне вдосконалення системи управління інформаційною безпекою Товариства, що відповідає вимогам міжнародного стандарту ISO / IEC 27001: 2013 «Information security management systems. Requirements» та Європейського регламенту з захисту персональних даних;
- ✓ за доведення вимог цієї Політики до всіх співробітників Товариства;
- ✓ покращення управління інформаційною безпекою Товариства за рахунок впровадження процесного менеджменту, постановки цілей і проведення аналізу функціонування системи управління інформаційною безпекою Товариства з боку керівництва;
- ✓ забезпечення системи управління інформаційною безпекою Товариства всіма необхідними ресурсами для досягнення поставлених цілей.

9. Оцінка результатів діяльності для забезпечення рівня інформаційної безпеки

В Товаристві визначені і застосовуються процедури з моніторингу, вимірювання, аналізу та оцінки, які необхідні для:

- ✓ забезпечення відповідності заходів захисту загрозам інформаційної безпеки;
- ✓ постійного підвищення результативності зусиль в сфері інформаційної безпеки;

Документована інформація за результатами проведених моніторингу, вимірювання і оцінки фіксується і зберігається.

Товариство аналізує і оцінює відповідні дані та інформацію, що отримуються в ході моніторингу і вимірювань.

Результати аналізу використовуються для:

- ✓ оцінки та підвищення рівня інформаційної безпеки;
- ✓ забезпечення відповідності та результативності заходів інформаційної безпеки;
- ✓ демонстрації успішної реалізації планів;
- ✓ оцінки показників функціонування процесів;
- ✓ виявлення потреби і можливостей для покращення рівня інформаційної безпеки;
- ✓ проведення аналізу з боку керівництва Товариства.

10. Перегляд Політики

Ведеться робота з постійної підтримки документа в актуальному стані. Документ повинен переглядається в міру необхідності, але не рідше одного разу на рік.

Перегляд Політики повинен бути направленний на задоволення вимог та постійного покращення результативності системи управління інформаційною безпекою.

Відповідальність за внесення змін до Політики покладається на Керівника служби інформаційної безпеки.