

ПОЛИТИКАТА ПО ИНФОРМАЦИОННА СИГУРНОСТ

1. ВЪВЕДЕНИЕ

Информацията, в т.ч. предоставените лични данни от субектите на лични данни и тяхната защита, съгласно Регламент (ЕС) 2016/679, е в основата на осъществяваната от ИП АРХИТЕКТИ дейност. Обхватът на СУИС във фирмата е представен в Наръчника на системата за управление.

За опазването от неразрешена промяна, загуба или неправилно разпространение на тази информация, организацията: спазва законовите изисквания; поела е договорни ангажименти; има утвърдена практика въз основа на своята система за управление на информационната сигурност.

Политиката по информационна сигурност на организацията представлява последващо стъпало в общата политика и организационното развитие на дружеството, като определя нови параметри и по-високи критерии за удовлетворяване изискванията на клиентите, защита на техните лични данни и интереси и увеличаване на организационната устойчивост и конкурентоспособност.

2. ЦЕЛИ

Настоящата политика определя рамката на система от мерки, която е насочена към следните общи цели:

- Гарантиране на поверителност на информацията – чрез прилагане на система от одобрени организационни и технологични мерки и ограничения върху достъпа, разкриването и защитата на информацията;
- Осигуряване на цялостност на информацията – чрез защита срещу неправомерни изменения или разрушаване на информацията;
- Осигуряване на достъпност на информацията – чрез осигуряване на надежден и навременен достъп до информацията, на принципа: „всичко, което не е забранено е позволено“;
- Постигане на отчетност на информацията – чрез въвеждане на контрол върху достъпа и правата върху информационните системи;
- Осигуряване на непрекъсваемост на дейността на ИП АРХИТЕКТИ – чрез поддържане на планове и процедури, с оглед гарантиране на клиентите, че услугите ще бъдат предоставени и техните лични данни защитени дори и при настъпването на форсмажорни или предизвикани интервенции в системата;
- Минимизиране на рисковете, свързани с обработването на лични данни и сигурността на информацията като цяло, които могат да доведат до физически, материални или нематериални вреди на организацията, на нейни клиенти и бизнес партньори;
- Минимизиране на степента на загуби или вреди, причинени от пробиви в сигурността;

- Осигуряване на необходимите ресурси за внедряване и поддържане на ефективна система за управление на информационната сигурност;
- Идентифициране на основните рамки за определяне на целите по контрола и механизмите за контрола на системата за управление на информационната сигурност;
- Информирание на служителите, институциите, клиентите, доставчиците и бизнес партньорите, които имат достъп до информацията на ИП АРХИТЕКТИ за техните отговорности и задължения по отношение на сигурността.

3. ОБХВАТ

Политиката се прилага по отношение на цялостната дейност на фирмата, респективно – по отношение на: защитата на личните данни, инфраструктурата, служителите, софтуерите, хардуерите, информационните масиви, документите и записите.

Политиката се прилага и по отношение на трети страни – доставчици на услуги, подизпълнители, клиенти и други организации, имащи достъп до лични данни, информация и информационни системи на организацията.

4. ПОДХОД

ИП АРХИТЕКТИ възприема проактивен подход към управлението на информационната сигурност, като използва рамките на следните стандарти:

- ISO/IEC 27001:2013 – Информационни технологии. Техники за сигурност. Системи за управление на сигурността на информацията. Изисквания;
- ISO/IEC 27002:2013 – Информационни технологии. Методи за сигурност. Кодекс за добра практика за управление на сигурността на информацията.

Всички процеси и свързаните с тях цели и мерки по контрола, възприетите други политики и процедури, документите и записите, чрез които те се поддържат и подобряват, са систематизирани в **Декларация за приложимост**. С оглед поддържането и подобряването на системата за информационна сигурност, организацията управлява следните процеси:

- Организиране на сигурността на информацията;
- Управление на активите;
- Сигурност на човешките ресурси;
- Физическа сигурност;
- Сигурност на комуникациите и дейностите;
- Контрол на достъпа;
- Сигурност на информационните системи;
- Управление на инциденти по сигурността;
- Управление на непрекъснатостта на дейността;
- Управление на съответствието със законовите, договорените и техническите изисквания и стандартите.

Възприетият подход за управление на информационната сигурност е цикъл, който включва следните стъпки:

- Изграждане, утвърждаване и разпространение на политики и цели по информационна сигурност, политика за защита на личните данни и декларации за поверителност;
- Осигуряване на ресурси за внедряване, поддържане и подобряване на система за управление на информационната сигурност;
- Оценка на стойността на притежаваните информационни активи. Оценката се извършва на основата на целите, описани по-горе и загубите, които ще претърпи ИП АРХИТЕКТИ при евентуален отказ или временно нефункциониране на актива;
- Извършване на анализ на рисковете по отношение на отделните информационни активи;
- Избор и прилагане на подходящи мерки за защита на информационните активи и гарантиране на сигурността на информацията. Мерките са съобразени със степента на риска и правните и институционални изисквания;
- Обмяна на опит по информационна сигурност, осъзнаване и обучение на служителите;
- Периодичен одит на прилаганите мерки с цел проверка на ефективността на действащата система и предприемане на стъпки (коригиращи и/или превантивни мерки) за нейното подобрене;
- Периодичен преглед на системата от ръководството с оглед осигуряване на нейната адекватност и последващо функциониране и подобряване.

5. ПРИНЦИПИ

Основните принципи, на които се основава системата за управление на информационната сигурност на ИП АРХИТЕКТИ, са насочени към постигане на следните изисквания:

- **Достоверност** - потребителите на информационните активи да бъдат идентифицирани по уникален признак при получаване на достъп до информация;
- **Цялостност** - наличие на адекватни защитни контроли и предпазни мерки, които да осигуряват точността на информацията по време на получаване, съхранение, обработка и предоставяне/представяне на информацията;
- **Конфиденциалност** - наличие на адекватни защитни контроли и предпазни мерки, които да осигуряват разкриване на информация само пред оторизирани потребители;
- **Отговорност** - наличие на адекватни защитни контроли и предпазни мерки, които да гарантират поемането/ носенето на отговорност от страна на доставчици и потребители на информация;
- **Управление** - информационните активи, независимо от това дали са собствени или наети, да бъдат използвани единствено за осъществяване на основната дейност на

организацията, като не се допуска използването им за лични нужди или за други цели, освен за основното им предназначение;

- **Квалификация и обучение. Осъзнаване** - осъзнаване важността на системата за управление на информационната сигурност, необходимостта от непрекъснато провеждане на обучения по информационна сигурност на служителите;
- **Съответствие** - съответствие на системата за управление на информационната сигурност с: всички приложими законови изисквания; поетите договорни задължения; стандартите за информационна сигурност;
- **Трети страни** - осигуряване съответствието на комуникацията с трети страни с изискванията на СУИС;
- **Принципи, свързани с обработването на лични данни**, съгласно чл.5 от Регламент (ЕС) 2016/679.

6. ОТГОВОРНОСТИ

Системата за управление на информационната сигурност функционира чрез ясно дефинирани, разпространени, осъзнати и управлявани чрез СУИС отговорности. В синтезиран вид тези отговорности са описани в Декларацията за ангажираност и Политика за защита на личните данни.

7. КОНТРОЛ И ПРЕРАЗГЛЕЖДАНЕ

Настоящата политика се утвърждава от висшето ръководство на организацията и преразглежда по отношение на адекватност, пълнота и ефективност най-малко веднъж годишно, в рамките на прегледа на СУИС, както е дефинирано в **Процедура Р 1-1 Отговорност на ръководството**.

8. САНКЦИИ

Преднамерено и умишлено неспазване и заобикаляне на принципите на тази политика, на Декларацията за приложимост или на указанията и процедурите за тяхното осъществяване и прилагане, води до предприемане на съответните дисциплинарни мерки.

Като управител на Иво Петров – Архитекти ООД декларирам личната си ангажираност за прилагането на тази Политика.

10.04.2018 г.

гр. София



Управител
Ivo Petrov
architects

Иво Петров Архитекти ООД