ПРИМЕР !

ПОЛИТИКА ЗА СИГУРНОСТ НА ИНФОРМАЦИЯТА

1. Цел на политиката

Да осигури насоки и подкрепа от Ръководството на организацията по отношение на информационната сигурност, в съответствие с изискванията:

- за устойчивост и непрекъснатост на бизнеса;
- за **непрекъснатост** и **наличност** на предлаганите ИТ услуги

Тази Политика определя подхода за минимизиране на рисковете към информационната сигурност, чрез защита от пробиви и инциденти по сигурността и намаляване (смекчаване) на последствията за бизнеса и предлаганите ИТ услуги, от тяхната реализация.

2. Информационна сигурност

Информацията е важен бизнес актив, който е от първостепенно значение за дейностите на организацията и в частност, за предлаганите от нея ИТ услуги.В този смисъл, информацията трябва да бъде подходящо защитена.

Информацията в организацията съществува под много форми - отпечатана или написана на хартия, съхранявана в електронен вид, обменяна по електронен път, предоставена или казана в разговор.

Независимо от формата или начина на създаване, обменяне или съхраняване, информацията трябва винаги да бъде съответно защитена.

Информационната сигурност осигурява защитата на информацията от различни по тип и природа заплахи (вкл. източници на заплахи), с цел гарантиране непрекъснатост на бизнеса, намаляване на бизнес риска и постигане на максимално възможната възвръщаемостта на инвестициите.

Информационната сигурност се постига чрез системно внедряване на подходящ набор от механизми на контрол (защитни механизми), включващи политики, процеси, процедури, инструкции, организационни структури и технологични решения (хардуер, софтуер, специализирани системи и др.). Тези контроли се създават, внедряват, наблюдават, преглеждат и подобряват в съответствие с останалите процеси за управление на бизнеса в организацията.

Информационната сигурност е свързана със запазването на конфиденциалността, целостта и наличността на информацията.

Информационната сигурност е свързана директно с постигането на непрекъснатост и наличност на предлаганите от Организацията ИТ услуги, в съответствие с документираните в СУУ изисквания към тях.

3. Цели и механизми за контрол

Отчитайки, че информационната сигурност е свързана със запазването на конфиденциалността, целостта и наличността на информацията, а от там и с осигуряването на изискванията за непрекъснатост и наличнаст на ИТ услугите, общата рамка на целите и механизмите за контрол по информационната сигурност се определят чрез тази **Политика;** възприетия и внедрен в Организацията **Метод за оценка на риска;** и **Приложение А** на **ISO 27001:2013** за Системи за управление на информационната сигурност (СУИС):

4. Отговорности за управление на информационната сигурност

Общата отговорност по управлението на информационната сигурност е в Ръководството на организацията.

Координирането на дейностите по разработване на планове, политики, вътрешни стандарти, ръководства, инструкции и процедури за прилагането, преглед и актуализация на Политиката за информационна сигурност е отговорност на Ръководството на организация.

Конкретни отговорности по оперативното управлението на информационната сигурност се възлагат на определен от Ръководството служител от Организацията.

Всички служители на организацията имат отговорности по изпълнението на установените ред и правила по информационната сигурност, вкл. и задължения за своевременно докладване по установен ред за пробиви / инциденти по сигурността.

5. Преглед на Политиката за сигурност на информацията

Политиката за сигурност на информацията се преглежда от Ръководството на организацията на планирани интервали (поне един път на година) и при настъпили значителни изменения, изискващи своевременни промени в прилаганите мерки за сигурност.

Резултатите от проведените прегледи от Ръководството на организацията са базата за вземане на решения и предприемане на действия свързани с:

- Подобряване на подхода за управление на информационната сигурност и на - процесите в организацията

- Подобряване на целите и механизмите за контрол

- Подобрения в разпределянето на ресурсите и/или отговорностите

6. Документи подкрепящи Политиката за сигурност на информацията

А. Документи разработени от организацията:

- Методика за оценка на риска;
- План за противодействие на рисковете към информационната сигурност;
- Процедура за управление на инциденти с информационната сигурност

Б. Международни стандарти:

- ISO 27001 - Информационни технологии – Техники за сигурност – Системи за управление на информационната сигурност – Изисквания
- ISO 27002 - Информационни Технологии – Техники за сигурност - Практики за управление на информационната сигурност