



ПОЛИТИКА ПО СИГУРНОСТ ПРИ ПРЕДОСТАВЯНЕ НА УДОСТОВЕРИТЕЛНИ УСЛУГИ

**Ревизия: 2
В сила от: 08.12.2005 г.**

**“Спектър” АД
ул. “Карнеги” 11А
1000 София, България
тел.: + 359 2 9699 200
факс: + 359 2 9699 255
<http://www.spektar.org>**

СЪДЪРЖАНИЕ

1. Въведение	3
2. Цели.....	3
3. Обхват	4
4. Подход	5
5. Принципи	5
6. Отговорности	6
7. Контрол и преразглеждане.....	8
8. Санкции	8

1. Въведение

Информацията е в основата на осъществяваната от „Спектър“ АД дейност като доставчик на удостоверителни услуги. При този процес извършван в "Spektar Org®" се оперира с критична по значение информация, за която „Спектър“ АД поема ангажимент да пази от неразрешена промяна, загуба или неправилно разпространение.

Настоящата политика по информационната сигурност задава рамката на система от мерки, която е насочена към:

- гарантиране на ПОВЕРИТЕЛНОСТ на информацията – прилагане на система от одобрени ограничения върху достъпа и разкриването на информация;
- 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;
- постигане на ОТЧЕТНОСТ на информацията – чрез въвеждане на контрол върху достъпа и правата върху информационните системи.

2. Цели

Целите на настоящата политика са:

- осигуряване на непрекъснатостта на предоставените от "Spektar Org®" услуги на нейните клиенти и бизнес партньори;
- минимизиране на рисковете за сигурността на информацията, причиняващи загуби или вреди на "Spektar Org®", нейните клиенти и бизнес партньори;
- минимизиране на степента на загуби или вреди, причинени от пробиви в сигурността;
- осигуряване на необходимите ресурси за внедряване на ефективна програма за управление на информационната сигурност;
- идентифициране на основните параметри на програмата за управление на информационната сигурност;
- информиране на персонала на "Spektar Org®", институциите, клиентите и бизнес партньорите, които имат достъп до информацията на „Спектър“ АД за техните отговорности и задължения по отношение на сигурността.

3. Обхват

Политиката се прилага по отношение на:

Средства - обхващат оборудване и необходимата за неговото функциониране инфраструктура:

- компютърни информационни системи всички класове – работни станции, сървъри, включително преносими компютри;
- офис оборудване – принтери, копирна техника, факсове, телефони;
- структурни кабелни системи и активно мрежово оборудване;
- Интранет и Интернет оборудване;
- климатични инсталации;
- охранителни системи;
- необходимите за нормално обезпечаване на дейността сградни инсталации;
- сгради и помещения пригодени за персонал и оборудване.

Данни - обхващат необработени данни и обработена информация като:

- файлове, досиета с данни, независимо от формата на съхранение и обмен;
- информация произтичаща от обработка на данни, независимо от формата и на съхранение и представяне.

Софтуер – обхваща самостоятелно разработени програми и такива придобити от външни източници:

- операционни системи и системен софтуер;
- приложен софтуер.

Документи на хартиен носител – включително документация на системата за информационна сигурност, наръчници на потребителите, договори, указания и процедури.

Персонал – служители, доставчици, консултанти, клиенти и други организации имащи достъп до данни, информация и информационни системи на „Спектър“ АД.

4. Подход

„Спектър“ АД възприема проактивен подход към управлението на информационната сигурност, като използва рамките на следните стандарти:

- EN ISO 17799 - управление на информационната сигурност;
- EN ISO 15408 - критерии за оценка на информационната сигурност.

Възприетият от „Спектър“ АД подход за управление на информационната сигурност е цикъл, който включва следните стъпки:

- оценка на стойността на притежаваните информационни активи за "Spektar Org®". Оценката се извършва на база загубите, които ще претърпи „Спектър“ АД 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;
- периодичен одит на прилаганите мерки с цел проверка на ефективността на действащата система и предприемане на стъпки за подобрене.

Предприетите от „Спектър“ АД мерки обхващат следните процеси:

- физическа сигурност;
- сигурност на персонала;
- комуникационна сигурност;
- компютърна сигурност;
- техническа сигурност.

5. Принципи

Основният принцип при управление на информационната сигурност е прилагането на ефективен контрол, който е измерим със стандартите за сигурност и изискванията за съответствие, които са приложими за "Spektar Org®". Контролът е насочен към постигане на следните изисквания:

Достоверност

Потребителите на информационните активи да бъдат идентифицирани по

уникален начин 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 наети или собственост на "Спектър" АД, да бъдат използвани единствено и само за осъществяване на основната дейност на "Spektar Org®", като не се допуска използването им за лични нужди или за други цели освен за основното им предназначение.

Квалификация и обучение

Осъзнаване на важността на квалификацията, компетентността и необходимостта от непрекъснато провеждане на обучение на персонала, клиентите и бизнес партньорите на "Spektar Org" по отношение на информационната сигурност.

6. Отговорности

Съвет за информационна сигурност – контролен орган по отношение на информационната сигурност в "Spektar Org®". Участва в анализа на информационните рискове и се свиква за обсъждане на възникнали въпроси или инциденти, свързани с информационната сигурност.

Ръководител ЗУУ - координира разработването на указанията и процедурите за прилагане на настоящата политика и отговаря за прегледа на ефективност от тяхното прилагане. Ръководителят на ЗУУ трябва да осигури целия персонал да бъде напълно информиран по отношение на неговите задължения и отговорности, залегнали в гореспоменатите указания и процедури.

Координатори на подзвена - носят отговорност по отношение на данните и другите информационни ресурси използвани при дейностите, които се осъществяват под тяхното наблюдение и контрол, за да се гарантира, че ресурсите са адекватно защитени, а също така да се гарантира спазването на приложимите указания, процедури и механизми при изпълнението на съответните дейности. Притежават правомощия за инициатива за промени по отношение на действащата система за информационна сигурност.

Администратор по сигурността - отговаря за администрирането на правилата за сигурност на цялата система, включително одобряване, създаване и прекратяване на действието на удостоверенията.

Системен администратор – отговаря за инсталацията, конфигурацията и администрирането на инфраструктурата на публични ключове, както и за регистрацията и създаването на удостоверения.

Системен оператор – отговаря за ежедневната работа на системата за издаване на удостоверения, като извършва редовно процедури по архивиране, създаване на резервни копия на информация и възстановяване информационни системи.

Системен контролър – отговаря за управлението на архивите и файловете с данни за регистрираните действия, извършени в системата за издаване на удостоверения.

Целият персонал - служители, временно наети, консултанти или посетители са длъжни да спазват указанията, процедурите и механизмите за информационна сигурност и активно да участват в опазването на информационните активи/ресурси на "Spektar Org®", като те не трябва да имат

достъп и да боравят с информационните активи без да имат съответните пълномощия и са длъжни да докладват за нарушения по отношение на сигурността на Ръководител ЗУУ.

7. Контрол и преразглеждане

Изпълнението на политиката се контролира регулярно, като политиката и свързаните с нея указания и процедури се преразглеждат по отношение на пълнота, ефективност и пригодност най-малко веднъж годишно.

8. Санкции

Преднамерено и умишлено неспазване и заобикаляне на принципите на тази политика или на указанията и процедурите за нейното осъществяване и прилагане води до съответните дисциплинарни действия.