***Забележка:***

*Този документ (шаблон) е в съответствие с изискванията на* ***ISO 27001:2013****, Приложение А, А.14.2.1.*

**ПОЛИТИКА ЗА СИГУРНОСТ ПРИ РАЗРАБОТВАНЕТО НА СОФТУЕР**

**Съдържание на документа (препоръчително):**

**1. Цел на Политиката**

*Напр.:*

*Основната цел на тази Политика е да осигури предпоставки за въвеждане на изискванията за информационна сигурност във всички фази от разработването на софтуер в Организацията.*

**2. Прилагане на Политиката**

*Напр.:*

*Тази Политика се реализира, чрез прилагане на следните, основни практики при разработването на софтуер:*

* ***Определяне на изискванията за сигурност****. Определяне и документиране на изискванията за сигурност във възможно най-ранния период на цикъла за разработване. Ако това не е направено, сигурността на разработената система не може реално дабъде оценена;*

* ***Валидиране на входните данни, постъпващи от неблагонадеждни (непроверени) източници****. Чрез валидиране на тези входни данни могат да се елиминират в голяма степен основните уязвимости на софтуера. Особено внимание трябва да се отделя на, напр. аргументите в командните линии, мрежовите интерфейси, файловете контролирани / управлявани от потребителите и др.;*
* ***Разработване на архитектура на софтуера и проект на софтуера по начин, който въвежда изискванията на политиките за сигурност****. Например – ако софтуерната система изисква работа с различни привилегии, в различни периоди от време, би трябвало да се одигури разделяне на системата на отделни, взаимно свързани подсистеми, всяка от които работи със собствен набор от привилегии;*
* ***Избягване на ненужно усложняване и нарастване на големината на проектите за софтуер****.**Усложнените и големи проекти повишават вероятността от поява на грешки в процесите на тяхното внедряване, конфигуриране и използване. В същото време, за постигането на необходимата и достатъчна сигурнст за тези проекти, трябва да се използват сложни контролни / защитни механизми;*
* ***Въвеждане на принципа за „отказано, по подразбиране”.*** *Решенията за достъп да се базират на разрешение, а не на изключение. Това означава, че, по подразбиране достъпа е забранен и приложената схема за защита определя еднозначно условията, при които достъпа е разрешен;*
* ***Въвеждане на принципа за „най-малко привилегии”.*** *Всеки процес би трябвало да се изпълнява с най-малкия набор от привилегии. Всяко одобрено разрешение би трябвало да е валидно за най-малкото, необходимо време. Този подход намялява възможностите за атака, свързана с изпълнението на произволен код от атакуващия, чрез одобрена и разрешена за ползване привилегия;*
* ***Въвеждане на принципа за „почистване” на данните, изпращани към други ситеми.*** *Всички данни преминаващи през сложни подсистеми (напр. ребационни бази данни) трябва да бъдат „почиствани”. При такъв случай, даден атакуващ може да активира неизползвани функционалности на тези подсистеми, чрез използването на SQL, команди или други “injection” атаки.*
* ***Въвеждане на принципа за „ешелонирана отбрана”.*** *Този принцип налага управлениетона риска да се извършва чрез различни защитни стратегии, така, че ако дадено ниво на защита бъда преодоляно, то следващото ниво на защита да извърши превенция на проблем по сигурността, преди той да се превърне в уязвимост, която може да бъде злонамерено използвана. Прилагането на този принцип предполага използването на техники за сигурност на програмирането;*
* ***Използване на ефективни техники за осигуряване на качеството.*** *Добрите техники за осигуряване на качеството могат ефективно да разкриват и елиминират уязвимости.Като част от програмата за осигуряването на качеството могат да бъдат въведени тестове за прониквания, одити на първичния код и др.*
* ***Прилагане на стандарти за сигурност при програмирането.*** *Внедряване на съответните стандарти в съответствие с използваните в Организацията езици и платформи за разработване на софтуер.*

**3. Свързани с Политиката документи:**

*Напр.:*

* *Политика за прилагане на изискванията за информационна сигурност в управлението на проекти (документ на СУИС);*
* *Политика и цели за информационна сигурност (документ на СУИС);*
* *Стандарт за сигурност при програмиране с ....*
* *....*