***Забележка:***

*Този документ (шаблон) е в съответствие с изискванията на* ***ISO 27001:2013****, Приложение А, А.14.2.5.*

**ПОЛИТИКА**

**ЗА**

**ИНЖЕНЕРИНГОВИТЕ ПРИНЦИПИ ЗА СИГУРНОСТ НА СИСТЕМИТЕ**

**Съдържание на документа (препоръчително):**

**1. Цел на Политиката**

*Напр.:*

*Тази Политика има за цел да осигури, че информационната сигурност е проектирана и внедрена в целия жизнен цикъл за разработване на информационни системи..*

**2. Прилагане на Политиката**

*Напр.:*

*Тази Политика определя рамката от принципи за инженеринг на сигурни / защитени системи в Организацията, отчитайки, че чрез този инженеринг се извършва:*

* *Оценка на възприемчивостта / податливостта към заплахите в проектираната или действителната среда на опериране;*
* *Разкриване и оценка на уязвимостите в системата и нейната среда за опериране;*
* *Определяне, специфициране, проектиране и разработване на мерки за защита, свързани със системните уязвимости;*
* *Определяне и оценка на мерките за защита, с цел установяване на тяхната жизненост, ефективност и очакваната степен на редукция на рисковете към мисията / бизнеса (свързани с разработваната система);*
* *Предоставяне на доказателства за надеждност на приетите мерки за защита;*
* *Определяне, остойностяване и оценка на цената и ползите от приетите мерки за защита;*

*Организацията приема изпълнението на* ***единадесет технически процеса*** *в инженеринга на сигурни / защитени системи, както следва:*

* *Изисквания на заинтересованите страни към системата;*
* *Анализ на изискванията към системата;*
* *Архитектурен проект на системата;*
* *Внедряване на системата;*
* *Интеграция на системата;*
* *Верификация на системата;*
* *Преход към системата;*
* *Валидиране на системата;*
* *Опериране / Работа на системата;*
* *Поддръжка на системана;*
* *Премахване на системата (сигурнаст при прекратяване функционирането на ИТ система)*

|  |  |
| --- | --- |
|  |  |

*Всеки процес от инженернига на сигурни / защитени системи подлежи на описване / документиране в следния базов формат:*

* ***Цел*** *– В тази секция се определят основните цели на процеса и се описват обобщено дейностите,свързани със сигурността, които се изпълняват по време напроцеса;*
* ***Резултати*** *– В тази секция се описва всичко, което е постигнато по сигурността и съответните доказателства, създадени по време наизпълнение на процеса;*
* ***Дейности и задачи*** *– В тази секция се прави подробно описание на действително извършената работа, по време на изпълнение на процеса, като се обръща специално внимание на съответните действия / задачи по сигурността.*

*Организацията приема да изпълнява, когато и както е приложимо,по-горе описаните процеси, съответните дейности и задачи към тях, съгласно документ на* ***Националния институт за стандартизация на САЩ*** *–* ***Systems Security Engineering / NIST Special Publication 800-160 (Initial Public Draft) / May 2014*** *(неразделно приложение към тази Политика)*

**3. Свързани с Политиката документи:**

*- Политика и цели за информационна сигурност (документ на СУИС);*

*- Политика за прилагане на изискванията за информационна сигурност в управлението на проекти (документ на СУИС);*

*- Политика за сигурност при разработването на софтуер(документ на СУИС);*

- *Systems Security Engineering / NIST Special Publication 800-160 (Initial Public Draft) / May 2014 (външен документ)*