## *Забележка:*

## *Този документ (шаблон) е в съответствие с изискванията на ISO 27001:2013, Приложение А, А.9.1.1.*

## ПОЛИТИКА ЗА КОНТРОЛ НА ДОСТЪПА

## Съдържание (препоръчително) на Политиката:

## 1. Цел на Политиката:

## Напр.-

## *Да осигури изискванията на бизнеса за управление на достъп до информацията, определена, като актив на Организацията, и до съответните средства които я създават, обработват, съхраняват, обменят и изобразяват.*

## 2. Прилагане на Политиката

## Напр. –

## *Тази Политика е разработена, документирана и преглеждана / актуализирана на база изискванията за информационна сигурност на бизнеса. Всяка промяна в средствата на Организацията, които* *създават, обработват, съхраняват, обменят и изобразяват информация, определена, като актив налага преглед и актуализация (при необходимост) на тази Политика.*

## *Прилагането на Политиката се осъществява на база:*

## *спазването на конкретните изисквания за сигурност на отделните бизнес приложения;*

## *въведените ред и правилат за класифициране на информацията;*

## *прилагането на принципа „необходимост да знае”;*

## *изпълнението на задълженията за сигурност на информацията, произтичащи от договори и/или нормативната уредба;*

## *извършването на управление на правата за достъп в мрежата (мрежите) на Организацията , отчитайки всички типове връзки (комуникации);*

## *прилагането на принципа за разделяне на функциите по искане на достъп, упълномощаване за достъп и упавление на правата за достъп;*

## *изпълнение на периодични прегледи на предоставените права за достъп, за установяване на необходимостта от промени (отнемане на достъп, нови праомощия за достъп и др.);*

## *архивиране на всички възникнали, съществени събития по сигурността, свързани с управлението и използването на потребителските идентификатори и персоналната информация за автентикация;*

## *изпълнение на контрол върху действиета на всички привилегировани потребители, вкл. на системните администратори.*

## *Тази Политика, освен описаното, се основава на следните основни принципи:*

## *„Всичко е забранено, освен, това, което е изрично разрешено” (за разлика от принципа „Всичко е разрешено, освен, това, което е изрично забранено”);*

## *Функционалните характеристики на персонала, определят обхвата на прилагането на принципа „Необходимост да знае”;*

## *Функционалните характеристики на персонала, определят обхвата на прилагането на принципа „Необходимост да използва”;*

## 3. Свързани документи с тази Политика

## *Описват се процедурите, инструкциите и др. документи от състава на СУИС, свързани с прилагането на конкретни ред и правила за управление на контрола на достъпа.*