

# Content Protection & Security Standard (CPS Standard)

---

## За Стандарта:

**Документ:** <https://www.mesaonline.org/wp-content/uploads/2016/04/Content-Protection-Security-Standard-February-2016.pdf>, страница 4

- Изискванията са дефинирани в рамките на Стандарта и придружаващия ги наръчник от основите на Content Security Management System (CSMS).
- Състои се от поредица от контроли, разработени за достъп, управление и минимизиране на рисковете до приемливо ниво, подsigурявайки конфиденциалност, интегритет и достъпност на интелектуалната собственост и медийни активи.
- рамки на способностите според Стандарта:
  - Управление и култура на сигурност;
  - Персонал и ресурси;
  - Управление на активи;
  - Физическа сигурност;
  - ИТ сигурност;
  - Обучение и осъзнатост;
  - Устойчивост на бизнеса;

## Отказ от отговорност:

**Документ:** <https://www.mesaonline.org/wp-content/uploads/2016/04/Content-Protection-Security-Standard-February-2016.pdf>, от страница 5 до страница 42

- CDSA цели изграждането на стандарт, който да намали всякаква вероятност от загуба на данни или тяхната кражба;
- Колкото и да е конкретен един стандарт, по своето съдържание и приложение, не може да гарантира напълно избягването на загубата на данни.
- CDSA не носи отговорност за загуба или иск на съдържание от собственика, участник или организация, или друга страна за сметка на Стандарта без значение дали CDSA е дала сертификат за съответствие или не;

## Общи положения при отказ от отговорност:

### 1. Управление и култура на сигурност:

#### 1.1. Управление на сигурността:

1.1.1. Обобщение: Определя изискванията за въвеждане на ефективна култура за управление и сигурност като Висшия мениджмънт е отговорен за контролите по сигурността. Изготвя се канал за комуникация и доставка на очакванията за сигурност, CSP стандартите и изискванията за сигурност на участниците;

#### 1.1.2. Изисквания:

- 1.1.2.1. да се убедят, че всички висши изпълнителни отдели добре разбират задълженията си и да демонстрират приложението на основни практики:
- сигурност в дневния ред на Борда;
  - ръководителите по сигурността са идентифицирани, носят отговорност за съответствието и се подкрепят от Борда;
  - ефективността на сигурността подлежи на преглед и одобрение;
  - създадена е група за управление на информационната сигурност;

## 1.2. Управление на риска:

1.2.1. Обобщение: Определя изискванията за оценка на риска и управленческите контроли. Участниците документират оценките на риска за всяка дейност, отнасяща се до медийните активи като се обръща внимание на доставчиците, третите страни и техните договорени задължения. Риска се идентифицира и класифицира по нивото му на заплахата. Оценката на риска определя приложимостта на CPS Стандарта според изпълнените услуги и дейности;

### 1.2.2. Изисквания:

1.2.2.1. Мениджмънта определя ролята и отговорностите по оценката на риска.

1.2.2.2. Оценката на риска се документира, описва се всеки риск, анализира се нивото му на въздействие и се оценява вероятността от появата на инциденти, свързани със сигурността.

1.2.2.3. Методологията за оценка на риска се предоставя.

1.2.2.4. Трябва да се създаде и поддържа регистър на риска, който да идентифицира всички рискове за сигурността на съдържанието.

1.2.2.5. Оценките на риска се преглеждат от Висшето ръководство ежегодно след инцидент със сигурността или преди значителни промени в бизнес дейността.

## 1.3. Съответствие:

1.3.1. Обобщение: От участниците се изисква да предоставят гаранция за способността за откриване и реагиране на инциденти, свързани със сигурността, както и на възстановяване след тях. Този процес определя изискванията за вътрешен одит.

### 1.3.2. Изисквания:

1.3.2.1. Участниците трябва да сформират екип за регистриране при инциденти със сигурността, отговорен за откриването, анализирането и отстраняването на

инциденти със сигурността.

1.3.2.2. Участниците трябва да установят, имплементират и поддържат процедура по наблюдение и реагиране при инциденти, свързани със сигурността.

1.3.2.3. Участниците трябва да установят, имплементират и поддържат процес по коригиране и превенция.

1.3.2.4. Трябва да се установи, имплементира и поддържа вътрешна процедура по одит, която да подsigурява, че:

- участниците съответстват на CPS Стандарта и на всички правни, регулаторни и договорени задължения;
- се насрочват и провеждат вътрешни одити поне веднъж годишно, не по-късно от 6 месеца след CDSA външния одит;
- където е приложимо, лицето, което извършва одита е независимо от това, което е отговорно за дейността;

**Резултатите след одита се записват и публикуват, за да позволят на тези, които са отговорни, да предприемат коригиращи или превантивни мерки.**

## 2. Персонал и ресурси:

### 2.1. Персонал и ресурси:

2.1.1. Обобщение: Определя изискванията за управлението на персоналната и ресурсната сигурност. Назначава се специален ръководител на програмата. Трябва да присъстват разпределени и разделени функции за сигурността, за да се постигат целите ѝ. Ръководството трябва да прилага подходящи и пропорционални нива на предварителна проверка, която трябва да бъде извършена

над всички служители и ресурси. Участниците трябва да осигуряват персонал и ресурси, както и да отоговарят на CPS Стандарта и на всички правни, регулаторни и договорени задължения.

#### 2.1.2. Изисквания:

2.1.2.1. Мениджмънта назначава мениджър на CPS програмата, който подsigурява, че мениджмънта на сигурността на системата, полиците и процедурите са установени, имплементирани и се поддържат. Отговорностите и правомощията на цялото ръководство, участващо в системата за управление на сигурността, трябва да бъдат определени и документираны.

2.1.2.2. Участниците документируют и имплементират личен процес по сигурността, който да съответства с текущите процедури по информационна сигурност на организацията.

2.1.2.3. Трудовите договори трябва да включват изискване за спазване на политиката, процедурите и процесите за сигурност.

2.1.2.4. Ръководството трябва да гарантира, че зоните на отговорност са разделени, когато е необходимо, за да се намалят възможностите за неразрешено модифициране и злоупотреба с информация или услуги.

2.1.2.5. Мениджмънта идентифицира и подsigурява наличностите на адекватен бюджет за задължителните изисквания на сигурността.

## 2.2. Ресурси на трети страни:

2.2.1. Обобщение: Определя изискванията за работа с ресурси на трети страни, изпълнители и компании като агенти, партньори за разтоварване и услуги за поддръжка. От мениджмънта се изисква да вземе предвид, като минимум, прилагането на политика процедури, споразумения за ниво на обслужване, споразумения за неразкриване и клаузи за поверителност в рамките на договорите. Участниците трябва да са в състояние да предоставят документиран политики и процедури, за да отговорят на изискванията на CPS Стандарта, правни, регулаторни и договорни задължения.

### 2.2.2. Изисквания:

2.2.2.1. Участниците трябва да имат защитени процеси за договаряне и ангажиране на всякакви ресурси на трети страни, отговарящи на съответните изисквания на CDSA. Мениджмънта гарантира, че подходящи споразумения за ниво на обслужване (SLA) и договорни задължения са договорени, изпълнени и преразглеждани редовно.

2.2.2.2. От участниците се изисква да уведомяват клиентите, ако компаниите подизпълнители се използват за обработка на съдържателни активи и следва да изискват от подизпълнителите да преминат през стандартни дейности.

2.2.2.3. Участниците трябва да гарантират, че подизпълнителите спазват договорните задължения за сигурност, както е посочено от собственика на съдържателния актив.

2.2.2.4. За облачни среди участниците установяват, документират и прилагат публикувана процедура за излизане от споразумението за услуга с клиент, включително

гаранция за отстраняване на клиентско съдържание/данни от всички изчислителни системи след прекратяване на клиентския договор.