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, подсигурявайки конфиденциалност, интегритет и достъпност на интелектуалната собственост и медийни активи.
- рамки на способностите според Стандарта:
    1. Управление и култура на сигурност;
    2. Персонал и ресурси;
    3. Управление на активи;
    4. Физическа сигурност;
    5. ИТ сигурност;
    6. Обучение и осъзнатост;
    7. 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. Управлние 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 заплаха. Оценката на риска
определя приложимостта на CPS Стандарта според изпълнените услуги и
дейности;

 1.2.2. Изисквания:

     1.2.2.1. Мениджмънта определя ролите 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
ба инциденти, свързани  със сигурността.

     1.2.2.3. Методологията за оценка на риска се предоставят.

     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 уяастниците 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 региране при инциденти
със сигурността, отговорен за откриването, анализирането и отсраняването 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 подсигурява, 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 й. Ръководството трябва да прилага подходящи и
пропорционални нива на предварителна проверка, която трябва да бъде
извършена
 над всички служители и ресурси. Уяастниците 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
подсигурява, 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 документирани.

     2.1.2.2. Участниците документират 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 подсигурява 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 документирани 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.

3. Управление на активи:

3.1. Административен контрол:

3.1.1. Обобщение: Определя какво се изисква за установяване и съобщаване на ролите и отговорностите за управление на активи. Трябва да се обърне специално внимание на видовете

```
 на актива, който се обработва. Активът:
     - се дефинира като интелектуална собственост или съдържание, включващо
редакции, неусвоено и усвоено съдържание, частна или чувствителна
информация, незавършен или завършен продукт;
     - включва медията или устройството, на което е получен, прихванат или
съхранен под контрола на организацията;
     - може да приеме физическа, цифрова или електронна форма и може да
съществува във всяка точка от веригата на доставки;
```

Трябва да се определи как да се борави с активите на всеки етап. Всяка дейност трябва да бъде документирана и очертаваща всички специални изисквания, необходими за гарантиране на сигурността на даден актив. Всеки проект трябва да се разглежда на базата на риск и стойност, очертавайки специалните изисквания за гарантиране, че целостта се поддържа и са спазени всички законови, регулаторни и договорни изисквания. Трябва да се има предвид административния контрол на компютърни системи и места за съхранение, съдържащи цифров IP или други търговски активи.

```
 3.1.2. Изисквания:

     3.1.2.1. Участниците въвеждат системи за управление на активи, която
може да бъде електронна или на хартиен носител. Тази система осигурява
подлежаща на одит верига на попечителство, която идентифицира локацията,
датата на създаване, движението и унищожението.

     3.1.2.2. Мениджмънта дефинира защитен процес, в съответствие с оценката
на риска и изискванията на клиента за всеки етап от обработката на активите.

     3.1.2.3. Мениджмънта възлага категория на риска за всеки актив,
базиеана на вида на съдържанието. Всека категория на риска е заложила
специфично предаване на сигурността, сухранение и транспортиране.

     3.1.2.4. Имената на хранилищата на медиини и цифрови файлове трябва да
бъдат анонимизирани и да не съдържат препратки към файловото съдържание.

     3.1.2.5. При облачните среди се установяват процедури за етикиране,
възлагане и защита на контейнерите, които съдържат данни и други контейнери.
```

3.2. Прихващане и трансфериране на активи:

```
 3.2.1. Обобщение: Определя изискванията за процедурите и работните процеси,
осигуряващи това, че всички активи са прихванати и трнсферирани по сигурен,
консистентен и одитиран начин.

 3.2.2. Изисквания:

     3.2.2.1. Да се обедят, че всички джижения, физически и цифрови, могат
да се одитират и преглеждат във веригите на активите на попечителство.
```

```
     3.2.2.2. Да се обедят, че техниките за защита са налични за употреба и
се прилагат, когато се инструктират.

     3.2.2.3. Участниците трябава:
         - да контролират и ограничават достъпа до уеб порталите, които се
използват за трансфериране на съдържание, поточно съдържание и
разпространение на ключове до оторизирани потребители.
         - да възлагат уникални потрбителски имена и пароли на потребителите
на портала и да разпространяват тези идентификационни данни по сигурен
начин.
         - да подсигурят, че само потребителите имат достъп до техния
собствен цифров актив.

     3.2.2.4. Създаване, документиране и внедряване на сценарии за клиенти
на облачните среди, при които клиентско съдържание/данни могат да бъдат
преместени от едно физическо местоположение на друго.

     3.2.2.5. При облачните среди, участниците предоставят:
         - клиенти с информация относно местоположенията на техните активи и
данни със съдържание;
         - възможност за контролиране на физическото местоположение на
съхранение на активите и данните на клиентското съдържание, ако е поискано;
```

3.3. Съхранение на сигурни активи и контрол на съгласъването:

```
 3.3.1. Обобщение: Участниците трябва да гарантират, че активите се
съхраняват сигурно в определени и отделени зони, като се извършват редовни
надзорни проверки, за да се гарантира, че точността, целостта и сигурността
се поддържат.

 3.3.2. Изисквания:

     3.3.2.1. Участниците трябва да:
         - извършват тримесечни циклични преброявания за съхранени клиентски
физически активи, където е възможно да използват служители, независими от
процеса на управление на активите;
         - се уверят, че ръководството преглежда процедурите за циклично
преброяване и резултатите;
         - се уверят, че несъответствията се разследват в съответствие с
Администртивния контрол и се преглеждат от ръководството;
         - се уверят, че сайтът ще разпредели активи на сигурни физически
или цифрови места за съхранение;
```

Известете клиентите при несъответствия и резултатите от разследванията!

3.4. Процедури за изземване на активи:

```
 3.4.1. Обобщение: Определя изисквания за наблюдение на активи, след като
бъдат разпределени на физическо лице. В зависимост от дейността и вида на
актива може да съществуват различни процедури. Въпреки това, участникът
трябва да вземе предвид риска за елементи с висока степен на сигурност.
Процедурите трябва да обхващат сроковете преди по-нататъшното разследване.
Където бъдат установени несъответствия или престъпност, резултатът от всяко
разследване трябва да бъде прегледан и да се обмисли уведомяването на
собственика на актива.

 3.4.2. Изисквания:

     3.1.2.1. Участниците приемат процедури за изземване на активи, като
определя критерии за артикулите според оценката на риска.

     3.1.2.2. Резултатите от всяко разследване се документират и докладват
на Ръководство.

     3.1.2.3. Ако даден актив остане липсващ след първоначалното
разследване, следва да започне допълнително разследване с помощта на лице,
независимо от дейността.

     3.1.2.4. Трябва да има процедура за ескалация и уведомяване на клиента,
в съответствие с всички споразумения за ниво на обслужване или договорни
изисквания.
```

3.5. Контрол на празни медийни материали:

```
 3.5.1. Обобщение: Определя изисквания за контрол на празни медийни
материали като всеки такъв матееориал трябва да е уникално идентифицируем и
да се съхранява на сигурно място при ограничен достъп.

 3.5.2. Изисквания:

     3.5.2.1. Участниците трябва да се уверят, че всички празни медийни
файлове са маркирани и вписани при пристигането. Когато е възможно, те
трябва да бъде уникално идентифицирани.
```

3.6. Задържане на записи:

```
 3.6.1. Обобщение:

 3.6.2. Изисквания:

     3.6.2.1.
```

3.7. Транспортиране на активи:

```
3.7.1. Обобщение:

3.7.2. Изисквания:

    3.7.2.1.

    3.7.2.2.

    3.7.2.3.

    3.7.2.4.
        -
        -

    3.7.2.5.

    3.7.2.6.
```

3.8. Унищожаване и рециклиране:

```
3.8.1. Обобщение:

3.8.2. Изисквания:

    3.8.2.1.

    3.8.2.2.

    3.8.2.3.

    3.8.2.4.
```