



31.07.2019 г.

X 03-793\1/ 31.07.2019

документ,
регистриран от
Signed by: Valerina Georgieva Tsvetanova-Igrutova

ДО
ИЗПЪЛНИТЕЛНИЯ ДИРЕКТОР/УПРАВИТЕЛ
НА ЛЕЧЕБНО ЗАВЕДЕНИЕ ЗА БОЛНИЧНА ПОМОЩ

ДО
УПРАВИТЕЛИТЕ
НА ЛЕЧЕБНИТЕ ЗАВЕДЕНИЯ ЗА ИЗВЪНБОЛНИЧНА ПОМОЩ

ДО
ДИРЕКТОРИТЕ
НА ЗДРАВНИТЕ ЗАВЕДЕНИЯ
НА ТЕРИТОРИЯТА НА ГР. СОФИЯ

Относно: Мерки за подобряване на информационната сигурност

УВАЖАЕМИ КОЛЕГИ,

Във връзка с писмо № 09-00-123/29.07.2019 г. на Министерство на здравеопазването и във връзка с пробивите в сигурността и изтичане на информация от системите на НАП да се пристъпи незабавно към изпълнение на неотложни мерки за подобряване на информационната сигурност, както следва:

- 1. Да се провери каква организация е създадена за осигуряване на защита на информацията:**
 - Какви са прилаганите към момента политики, процедури, вътрешни правила и инструкции;
 - Определени ли са собствениците за всеки информационен актив;
 - Има ли ясно разписани роли и отговорности по отношение на сигурността:
 - Кой е отговорният ръководител;
 - Кой е системният администратор;
 - Кой осъществява контрола над действията;
 - Обучени ли са служителите от всички нива;
 - Как се реагира при нарушение на сигурността.
- 2. Да се извърши инвентаризация на всички материални активи, свързани с обработката на информацията:**
 - В инвентаризацията да се обхванат компютри, сървъри, принтери, външни памети и т. н.;
 - За всяко устройство да се създаде технически паспорт с подробно описание на всички компоненти, включително хард дискове (в този паспорт да се отбелязват всички промени, подменени или добавени части, ремонти и т. н.).
- 3. Да се извърши актуализация на системното програмно осигуряване:**
 - Операционни системи, офис пакети и т. н.;

- Да се инсталират всички актуализации (кръпки), препоръчани от производителя и най-вече тези, свързани със сигурността;
 - Да се създаде регистър на актуализациите.
4. **Да се извърши преглед на използваните други програмни системи:**
 - Системи за документооборот, заплати, други;
 - Каква информация се обработва, къде се съхранява, на кого се предава;
 - Кой има достъп до програмите и данните.
 5. **Да се извърши преглед на използваните системи за сигурност:**
 - Стандартните възможности на операционните системи;
 - Възможностите на защитените стени и конфигурацията им;
 - Антивирусни средства.
 6. **Особено внимание да се обърне върху антивирусната защита:**
 - Използват ли се антивирусни програми;
 - Да се създаде ред за актуализация на антивирусните програми;
 - Специално внимание да се обърне за работата с електронната поща (да не се отварят писма от непознати адресати, със съмнително и неясно съдържание и т. н.);
 - Да не се посещават електронни страници, които не са свързани с преките задължения;
 - Да се обучат служителите как да реагират при съобщение за вирусна атака.
 7. **Във връзка с достъпа до информационните ресурси (програми, данни, електронна поща и т. н.):**
 - Да се актуализират списъците за достъп (да се изтрият неработещите служители, напуснали такива, тези със сменени функции, външни изпълнители и т. н.);
 - Да се сменят всички пароли за достъп – до компютрите и приложенията (програмите);
 - Новите пароли да бъдат с минимална дължина 8 символа, големи и малки букви, цифри и символи.
 8. **Да се направи преглед на системите за физически достъп и да се въведе система за контрол:**
 - До районите и сградите;
 - До помещенията с компютри;
 - До помещенията с мрежово оборудване.
 9. **Да се забрани:**
 - Използване на собствени запамятаващи устройства;
 - Посещаване на електронни страници, несвързани с изпълнението на задълженията от служителите;
 - Слушане на музика;
 - Гледане на филми и видеа;
 - Инсталирането на неодобрен от ръководството софтуери;
 - Нерегламентирана промяна в конфигурациите на компютрите.
 10. **Да се актуализират (или да се създадат):**
 - Правила за създаване, използване и достъп до резервни копия на данни;
 - Правила за сигурно унищожаване на информация за различните видове носители;
 - Правила за ремонт или подмяна на оборудването.
 11. **Да се актуализират всички договори от гледна точка на сигурността на информацията:**

- За поддръжка на оборудването;
- За доставка на Интернет услуги;
- Други.

При необходимост да се предприемат и други необходими и възможни действия, съгласно предоставената Ви компетентност.

За изпълнението на мерките да се изготвят отчетни документи, като протоколи, декларации и др., от които да е видно отговорникът, изпълнителят и времето на изпълнението. Същите да се съхраняват по места.

С уважение,

31.07.2019 г.

X *д-р Данчо Пенчев*

Д-Р ДАНЧО ПЕНЧЕВ

Директор на СРЗИ

Signed by: Dantcho Ivanov Pentchev