РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА - REPUBLIKA E MAQEDONISË SË VERIUT
АГЕНЦИЈА ЗА СУПЕРВИЗИЈА НА КАПИТАЛНО ФИНАНСИРАНО ПЕНЗИСКО ОСИГУРУВАЊЕ
AGJENCIA PËR MBIKËQYRJE TË FINANCIMIT KAPITAL TË SIGURIMIT PENSIONAL
Бр.-Nr. 08-939/7
30.09 20 21 год.-viti
СКОПЈЕ - SHKUP

Република Северна Македонија

Агенција за супервизија на капитално финансирано пензиско осигурување

Правила за информациска сигурност на Агенцијата за супервизија на капитално финансирано пензиско осигурување

Системско време и синхронизација на часовникот

Сите внесови за лог записи треба да го содржат системското време. Системскиот часовник на ИТ системите треба да се синхронизира со договореното точно референтно време (официјално стандардно време) во редовни интервали.

Деловни процеси

Сопственикот на деловниот процес е одговорен за заштита на информациите и податоците во рамки на деловниот процес, како и за начинот и опсегот на откривање на информациите од деловниот процес.
Доколку информацијата која има потреба од заштита се размени низ деловните процеси, тогаш сопствениците на деловните процеси заеднички треба да утврдат како да се обезбеди постојана заштита на информацијата.

Ракување со медиуми за податоци

Доколку со медиумите за податоци на ИТ системите, особено преносните медиуми за податоци, се ракува невнимателно или несоодветно, ова би можело да резултира со ненамерно откривање на информации на неавторизирани лица или до загуба на податоци.
Треба да бидат воспоставени соодветни оперативни процедури за да им се обезбеди на сите вработени конкретни инструкции за постапување со медиуми за податоци, и особено за преносни медиуми за податоци.
Медиумите за податоци треба да се користат и чуваат во согласност со барањата за заштита на производителот.

VPN врски (далечински пристап)

Да се пристапува на секундарната локација по пат на VPN врска (Virtual Private Network – Виртуелна приватна мрежа) кон интерните мрежа, треба да се користи техника која што наложува тајно познавање и сопственост (потврда на автентичност со два фактори) како минимално барање.

Уништување на податоци

Кога ИТ системи, на пример уреди како што се рачни компјутери, лаптоп компјутери и мобилни телефони како и сервери, системи за складирање и библиотеки за бекап, се повлекуваат од

употреба, треба да се оневозможи чувствителни информации да дојдат во погрешни раце (согласно Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци). Следните генерални правила треба да бидат запазени:

- Безбедно бришење со целосно пишување врз претходните податоци на медиумот за податоци со безопасни податоци како што се секвенци на битови по случаен избор, или физичко уништување на медиумите за податоци со нивно сечење, распарчување или со употреба на уреди за демагнетизација. Последното особено ќе се применува за дефектни медиуми за податоци, каде што податоците нема да може да се уништат со употреба на „безбедно бришење".
- Уништувањето на податоци и бришењето на податоците треба да се имплементира исклучиво со употреба на техники и алатки кои што ќе осигурат дека оригиналните информации нема да може да се вратат.

<u>Обезбедување на услуги од трети страни</u>

Во случаи кога услуги се обезбедуваат од трети страни, барањата за заштита и безбедност на податоците кои што треба да се прецизираат за ИТ системите се дефинираат и контролираат преку Договори со давателот на услуги (изведувачот), за кого што ќе се применуваат следниве барања:

- Договорите за ИТ услуги со трети страни треба да содржат прецизни описи на сите аспекти на заштитата на податоци и релевантни за безбедноста како и барањата за обезбедување на услуги, особено техничката и организациската заштита на податоците и контролите на безбедноста коишто треба да ги имплементира изведувачот.
- Кога на давателите на услуги им е доделена задачата за обработка на лични податоци, релевантните барања за заштита и безбедност на податоците треба да бидат детално наведени во посебен договор за обработка на податоците за којашто е ангажиран подизведувачот.
- Договорите со давателите на услуги треба да ги содржат следниве одредби за аспектите на заштита и безбедност на податоците, особено за критичните ИТ системи:
  - Правото на корисникот да изврши инспекција на оперативната документација и тековите на работата;
  - Обезбедување на извештаи и евиденција од страна на изведувачот;
  - Овластувањето на корисникот да дава инструкции на изведувачот;
  - Интеграција на подизведувачите;
  - Правото на корисникот или било која трета страна ангажирана од корисникот да ги провери ИТ системите на локацијата на изведувачот, вклучувајќи го и правото на пристап до згради и објекти и на проверка на релевантните ИТ системи;
  - Начинот на проследување на информации за инциденти поврзани со заштитата и безбедноста на податоците, како и за соработката во случај на сериозни проблеми или инциденти;
  - Однапред ќе се ставаат на располагање дефинираните правила кои се однесуваат на заштитата и безбедноста на податоците.

Политика на чист екран и чиста маса

Строго доверливите и доверливите информации треба да бидат заклучени кога не се потребни и кога канцеларијата е празна.

Компјутерите и терминалите треба да бидат во состојба „ log off “ или заштитени со „ screen lock“ механизам (ctrl, alt, del и enter/ lock computer) кога не се работи на нив. Сите screen-saver-и мора да бидат заштитени со лозинка. Исклучок кон ова правило може да се направи само со одобрување од страна на Претседателот на Советот на експерти на Агенцијата.

Изработил: Емилија Рамова
16.8.2021 Е. Рамова

Претседател на Советот на експерти
Максуд Али