



РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА REPUBLIKA E MAQEDONISE SÉ VÉRUT
ВЛАДА НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
СЕКРЕТАРИЈАТ ЗА ЗАКОНОДАВСТВО
QEVERIA E REPUBLIKËS SÉ MAQEDONISE SÉ VÉRUT
SEKRETARIATI I LEGJISLACIONIT

Бр./Nr. 03-2431 /1

14 -06 - 2023 20 год./viti
СКОПЈЕ - SHKUP

Врз основа на член 55 став 2 од Законот за организација и работа на органите на државната управа („Службен весник на Република Македонија“ бр. 58/00, 44/02, 82/08, 167/10 и 51/11, и „Службен весник на Република Северна Македонија“ бр.96/19 и 110/19), а во врска со член 28 од Законот за заштита на личните податоци(*) („Службен весник на Република Северна Македонија“, бр. 42/20 и 294/21) и член 33 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), секретарот на Секретаријатот за законодавство на Владата на Република Северна Македонија донесе,

Политика на „чист еcran“ и „чисто биро“

Член 1

Со оваа политиката на „чист еcran“ и „чисто биро“ се утврдуваат безбедносни мерки, со цел да се намалат ризиците од неовластен пристап, губење и оштетување на документи, информации кои содржат лични податоци за време и надвор од работното време во Секретаријатот за законодавство на Владата на Република Северна Македонија (во понатамошниот текст: Секретаријатот).

Опсег

Член 2

Оваа политика се применува од страна на сите вработени во Секретаријатот, ангажирани лица од Секретаријатот и/или кое било друго лице кое користи каква било форма на информатичка технологија на Секретаријатот, или има одговорност за институционални информации зачувани во алтернативна форма, како што е хартија.

Политиката се однесува на сите документи, преносливи медиуми за складирање на податоци и информации и на сите електронски уреди, што содржат и прикажуваат информации, поврзани со работењето на Секретаријатот без оглед на локацијата.

Дефиниции

Член 3

1. „Електронски уред“ е било кој компјутерска работна станица или друг електронски уред кој што има преносна функционалност или можност за прикажување информации на екран (на пример лаптоп, паментен телефон, таблет, дигитален апарат за сликање).
2. „Екран“ е делот за приказ на било кој електронски уред.
3. „Обезбеден“ значи, во најмала рака заклучување или на друг начин спречување на пристап до информации, записи и/или физички простор.

Безбедносни мерки за „чисто биро“

Член 4

Согласно оваа политика треба да се спроведуваат следниве безбедносни мерки за „чисто биро“:

- Онаму каде што е практично можно, хартијата и електронските уреди треба да се чуваат во соодветни заклучени сефови, ормани или други форми на безбедносен мебел кога не се користат, особено вон работното време и/или за време на пауза;

- Кога не се достапни сефови за заклучување, ормани, фиоки, шкафови и слично, канцелариските врати мора да бидат заклучени доколку останат без надзор.

- Документи во тврда копија што содржат лични податоци или доверливи, ограничени или чувствителни информации треба да се чуваат само доколку е потребно и истите да се чуваат во обезбедени простории или заклучени фиоки согласно прописите од областа на заштита на личните податоци и касифицирани информации .

Вработените треба да осигураат дека сите лични податоци, доверливи, ограничени или чувствителни информации се обезбедени во нивната работна околина на крајот на работниот ден и кога се очекува вработените да бидат далеку од нивната работна околина за подолг период (на пример за време на пауза, одмор и слично).

Вработените не треба да ги направат достапни лични податоци, доверливи, ограничени или чувствителни информации на трети лица, и да ги објавуваат на социјални мрежи и неовластено да вршат пренос на истите на други медиуми (USB, External HDD, Mobildata, Online HDD драјвори „Google drive“ и други, и други сендери на огромни е-мејл фајлови).

Корисничка поддршка за „remote access“ може да врши само

одговорното лице, но можен е кориснички пристап до одреден „cloud service“ со сопствено корисничко име и лозинка.

Секој документ кој содржи личен податок или доверлива, ограничена или чувствителна информација мора да се отстрани од работните бироа и места и да се заклучи во фиоката кога на бирото нема вработено лице или на крајот на работниот ден.

Документите кои содржат лични податоци или доверливи, ограничени или чувствителни информации, кога се печатат, треба веднаш да се тргнат од печатачите.

Во простории во кои се врши прием на странки не треба да се овозможи директен пристап до лични податоци.

Приступот до безжични интернет услуги за посетители во просториите на Секретаријатот се обезбедува преку ограничен пристап до интернет услуги со корисничко име и лозинка.

Клучевите што се користат за пристап до документи кои содржат лични податоци, доверливи, ограничени или чувствителни информации не се оставаат на работната површина без соодветен надзор.

Документите кои содржат лични податоци, доверливи, ограничени или чувствителни информации веднаш после нивната обработка треба соодветно да се складираат, во папки или досиеја, а при нивното уништување не се оставаат на работните бироа. Истите се одложуваат на заштитена локација и не смеат да се ставаат во редовни канти за отпад. Уништувањето на документ што содржи лични податоци или доверливи, ограничени или чувствителни информации се врши со ситнење на шредер или на друг начин, при што информациите повторно да не можат да бидат употребливи.

Безбедносни мерки за „чист еcran“

Член 5

Согласно оваа политика треба да се спроведуваат следниве безбедносни мерки за „чист еcran“:

- Електронските уреди, компјутери, лаптопи и друго, не треба да се вклучуваат кога се без надзор и секогаш треба да бидат заштитени со лозинка.

- Компјутерските екрани и други електронски уреди треба да бидат под агол на страна од погледот на неовластените лица.

- Компјутерските работни станици треба да бидат исклучени на крајот од работниот ден, за да овозможат да се инсталираат безбедносни ажурирања.

- Заклучувањето за безбедност на еcranот треба да се активира кога нема активност за краток однапред определен временски период, најмалку 15 минути.

- Заштитното заклучување на еcranот треба да биде заштитено со лозинка за реактивирање.
- Лозинките не треба да се оставаат на лепливи белешки објавени на или под компјутер, ниту пак треба да се остават запишани и оставени на достапна локација.
- На еcranите не треба да се чуваат лични податоци подолго отколку што е потребно за нивна обработка.
- Лични податоци во било каква форма, не треба да бидат достапни во заеднички фолдери и/или локации.
- Преносни уреди, како што се некористени лаптопи, дигитални фотоапарати и таблети, се заклучуваат во фиока.
- Уреди за масовно складирање на податоци, треба да се третираат како уреди со чувствителни информации и податоци и да бидат заклучени во фиока.

Член 6

Секретаријатот преку офицерот за заштита на лични податоци ќе ја следи и потврди усогласеноста со оваа политика преку различни методи, вклучително, преку периодични контроли за почитување на безбедносните мерки од оваа политика.

Член 7

Вработените и ангажираните лица во Секретаријатот мора строго да се придржуваат до сите безбедносни мерки содржани во оваа политика. Прекршувањето на оваа политиката на „чист екран“ и „чисто биро“ може да доведе до дисциплински и други мерки.

Член 8

Оваа политика влегува во сила со денот на донесувањето, а ќе се објави на огласната табла во работните простории на Секретаријатот и на веб страната на Секретаријатот.

Секретар на Секретаријат за законодавство
д-р Оливера Нечовска

