Република Северна Македонија
Дирекција за безбедност
на класифицирани информации
Бр. 02-1039/11
Скопје, 30.11.2021 година

Врз основа на член 75 став 1 од Законот за класифицирани информации(*) („Службен весник на Република Северна Македонија“ бр. 275/19), 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, 51/11 и „Службен весник на Република Северна Македонија“ бр. 96/19, 110/19), а во врска со член 119 и 120 од Законот за заштита на личните податоци(*) („Службен весник на Република Северна Македонија“ бр. 42/20) и согласно член 33 од Правилникот за безбедност на обработката на личните податоци („Службен весник на Република Северна Македонија“ бр. 122/20), директорот на Дирекцијата за безбедност на класифицирани информации донесе

ПОЛИТИКА
ЗА ЧИСТ ЕКРАН И ЧИСТО БИРО

Цел
Член 1

Политиката за чист екран и чисто биро има за цел да ги намалува ризиците од неовластен пристап, губење и оштетување на документи што содржат лични податоци за време и вон работното време на Дирекцијата за безбедност на класифицираните информации (во натамошниот текст: Дирекцијата).

Опсег на примена
Член 2

(1) Оваа политика се применува на сите вработени во Дирекцијата, односно на секое вработено лице во Дирекцијата и/или кое било друго лице што користи каква било форма на информатичка технологија во сопственост на Дирекцијата, или има одговорност за институционални информации зачувани во алтернативен формат како што е хартија.

(2) Оваа политика ги опфаќа сите документи, преносливи медиуми за складирање на податоци и информации и сите електронски уреди што содржат или прикажуваат информации поврзани со работата на Дирекцијата.

Дефиниции
Член 3

За целите на оваа Политика:

- „електронски уред“ е која било компјутерска работна станица или друг електронски уред којшто има преносна функционалност или можност за прикажување информации на екран (на пр. лаптоп, паметен телефон, таблет, дигитален апарат за сликање);
- „екран“ е делот за приказ на кој било елетронски уред;
- „обезбеден“ значи, најмалку, заклучување на електронскиот уред или на друг начин спречување пристап до информации, записи и/или физички простор.

Безбедносни мерки

Член 4

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

(2) Кога не се достапни сефови за заклучување, ормари, фиоки, шкафови и слично, канцелариските врати мора да бидат заклучени доколку хартијата и електронските уреди останат без надзор.

(3) Документи во хартиена форма што содржат лични податоци или доверливи, ограничени или чувствителни информации треба да се чуваат само доколку е потребно за извршување службена работна задача.

(4) Од вработените се бара да се осигураат дека сите доверливи, ограничени или чувствителни информации складирани на медиуми (USB/CDROM/DVD) или во друга електронска форма 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 пр. за време на пауза).

(5) Секој документ што содржи личен податок или доверлива, ограничена или чувствителна информација мора да се отстрани од работното биро и место и да се заклучи во фиоката кога на бирото не е присутно вработеното лице или на крајот од работниот ден.

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

(7) Во областа за прием на странки/посетители не треба да се чуваат информации што содржат лични податоци и да има документи во хартиена форма, а доколку има електронски уреди, истите треба да бидат обезбедени.

(8) Клучевите/електронските карти што се користат за пристап до документи што содржат доверливи, ограничени или чувствителни информации не смеат да се оставаат на работното биро без соодветен надзор.

(9) Документите што содржат лични податоци или доверливи, ограничени или чувствителни информации при нивното уништување не смеат да се оставаат на работното биро или да се стават во редовните корпи за отпад. Уништувањето на документ што содржи лични податоци или доверливи, ограничени или чувствителни информации се врши на начин што оневозможува негово повторно користење.

(10) Електронските уреди не треба да се вклучуваат кога се без надзор и секогаш треба да бидат заштитени со лозинка.

(11) Компјутерските екрани и другите електронски уреди треба да бидат под агол настрана од погледот на неовластените лица.

(12) Компјутерските работни станици мора да бидат исклучени на крајот од работниот ден за да се остави можност за инсталирање безбедносни ажурирања во текот на вечерта.

(13) Заклучувањето за безбедност на Windows треба да се активира кога нема активност за краток однапред определен временски период, најмалку 15 минути.

(14) Заштитното заклучување на Windows треба да биде заштитено со лозинка за реактивирање.

(15) Лозинките не смеат да се оставаат на белешки што се видливи на достапна локација.

(16) Таблите што содржат лични податоци или доверливи, ограничени или чувствителни информации треба да се избришат по нивното користење.

(17) Преносните уреди што во моментот не се користат мора да се заклучени во фиока/ормар.

(18) Медиумите за складирање податоци (USB/CDROM/DVD) треба да се третираат како уреди што содржат лични податоци или доверливи, ограничени или чувствителни информации и мора да се заклучени во фиока/ормар.

Одржување и усогласеност

Член 5

Дирекцијата преку офицерот за заштита на лични податоци и внатрешниот ревизор ќе ја следи усогласеноста со оваа политика преку различни методи, вклучително, но не ограничувајќи се на, периодични контроли и внатрешни ревизии.

Дисциплински последици

Член 6

(1) Вработените во Дирекцијата и другите ангажирани лица што користат каква било форма на информатичка технологија во сопственост на Дирекцијата мора строго да се придржуваат кон безбедносните мерки од членот 4 на оваа политика.

(2) Прекршувањето на безбедносните мерки од членот 4 на оваа политика претставува основа за дисциплинска одговорност и може да доведе до дисциплински и други мерки.

Примена и ревизија на политиката

Член 7

(1) Оваа политика почнува да се применува од денот на нејзиното донесување и истата се објавува на веб-страната на Дирекцијата.

(2) Оваа политика ќе се ревидира во случај на промена на основот на којшто е донесена и по потреба за изменување и дополнување на системот за заштита на личните податоци што се обработуваат во Дирекцијата.

Директор,

Стојан Славески