Врз ~~основа на~~ член 15 од Законот за катастар на недвижности („Службен весник на Република Македонија“ бр.55/13, 41/14, 115/14, 116/15, 153/15, 192/15, 61/16, 172/16, 64/18 и „Службен весник на Република Северна Македонија“ бр.124/19), член 18 од Статутот на Агенцијата за катастар на недвижности (бр. 01-7492/10 од 30.04.2013, бр.01-548/8 од 30.01.2015 година, „Службен весник на Република Македонија“ бр. 173/2018 и „Службен весник на Република Северна Македонија“ бр.161/20), а согласно член 8 од Политика за создавање на систем за заштита на лични податоци во Агенцијата за катастар на недвижности бр.0204-12218/1 од 24.08.2021 година, директорот на Агенцијата за катастар на недвижности донесе

ПРОЦЕДУРА НА КОРИСТЕЊЕ НА ИТ СИСТЕМИТЕ И НИВНА БЕЗБЕДНОСТ

Агенцијата за катастар на недвижности (во понатамошниот текст: АКН) е посветена на заштита на своите вработени, професионалните корисници и организацијата од незаконски или штетни активности на поединци, без разлика дали тие се намерни или ненамерни.

Системите поврзани со Интернет/интранет/екстранет, вклучувајќи ги, но неограничувајќи се на, компјутерската опрема, софтверот, оперативните системи, медиумите за складирање, мрежните сметки за електронска пошта, пребарувањето на веб-страници и FTP (протокол за пренос на датотеки), се сопственост на АКН.

Се очекува секој да ги користи овие системи за работни цели и во интерес на организацијата и на нејзините клиенти во текот на секојдневното работење.

Ефективната безбедност е заеднички напор кој го вклучува учеството и поддршката од секој вработен во АКН и секој орган во состав кој работи со информации и/или информациски системи. Секој вработен или професионален корисник на АКН кој е корисник на компјутер во окружувањето е должен да ги знае овие упатства и да постапува соодветно на нив.

Во оваа Процедура е даден краток преглед на прифатливата употреба на компјутерската опрема и информациските системи во АКН. Со овие правила се заштитува АКН и вработените и професионалните корисници на АКН. Несоодветна употреба на компјутерската опрема ја изложува АКН на различни напади од ризици, компромитирање на мрежните системи и сервиси и правни прашања.

1. Област на примена

Оваа Процедура важи за сите вработени во АКН. Таа, исто така, важи и за сите изведувачи/добавувачи на АКН, како и за нејзините консултанти, привремено ангажирани лица, трети страни, подолу во овој документ наречени соработници.

Процедурата се применува и на целата опрема која АКН ја поседува, ја зема под закуп или со која работи.

2. Процедура

2.1. Општа употреба и сопственост

1. Вработените во и соработниците на АКН треба да бидат свесни дека податоците кои ги креираат на корпоративните системи остануваат да бидат во сопственост на АКН. За да се заштити мрежата, раководството ја гарантира доверливоста на информациите кои се складирани на кој било мрежен уред во сопственост на АКН.
2. За целите на одржување на безбедноста и на мрежата, овластени поединци во рамки на АКН може да ја надгледуваат опремата, системите и мрежниот сообраќај во кое било време во согласност со деловните, договорните и правните прописи и правила.
3. АКН го задржува правото на ревизија на мрежите и системите на периодична основа со цел да се обезбеди усогласеност со оваа Процедура.

2.2. Безбедносни и сопственички информации

1. Лозинките треба да се чуваат во тајност и сметките не треба да се споделуваат. Како овластен корисник, секој вработен во или соработник на АКН е одговорен за безбедноста на своите лозинки и сметки. Лозинките на ниво на систем треба да се менуваат периодично; лозинките на ниво на корисник треба да се менуваат на секои три месеци;
2. Сите персонални компјутери, преносни компјутери и работни станици треба да бидат заштитени со лозинка за автоматско заклучување на екранот кое треба да биде подесено автоматски да се активира на 15 минути или помалку, или со одјавување на корисникот во случај тој да не работи на компјутерот или на работната станица.
3. Доколку од електронската пошта на АКН се испраќаат електронски пораки кои содржат новости и известувања (newsgroupposting), истите треба да содржат и одрекување од одговорност (disclaimer) со кое се посочува дека изразените мислења се исклучиво на сопственикот на електронската пошта (вработен во или соработник на АКН) и не значи дека се воедно и мислења на АКН, освен доколку истите не се испраќаат во рамките на извршувањето на работните задачи.
4. Сите работни станици кои ги користат вработените во или соработниците на АКН кои се поврзани на Интернет/интранет/екстранет на АКН, без разлика дали се во сопственост на Агенцијата, мора континуирано да користат одобрен софтвер за скенирање вируси со ажурирана база на податоци на вируси (освен доколку не е поинаку пропишано со секторската или групната Процедура)

5. Прилозите во електронската пошта добиени од непознат испраќач не треба да се отворат или доколку се отворат, тоа треба да се стори со голема претпазливост. Тие прилози може да содржат различни вируси, пренатрупување на електронската пошта (emailbombs) или кодови за тројанци.

2.3. Користење на електронска пошта

Следниве активности се строго забранети, без исклучоци:

1. испраќање непобарани пораки преку електронска пошта, вклучувајќи и испраќање на „непотребна пошта“ (“junkmail”) или друг рекламен материјал на поединци кои конкретно не побарале такви материјали (спам пораки).
2. сите форми на вознемирување преку електронска пошта, телефон, без разлика на јазикот, зачестеноста или големината на пораките.
3. неовластено користење или фалсификување на информациите во заглавието на електронската пошта.
4. барана електронска пошта испратена до било која друга адреса на електронска пошта, освен онаа на сметката на испраќачот, со намера да се вознемирува или да се собираат одговори.
5. создавање или проследување „поврзани писма“ (“chainletters”) или други „пирамидални“ шеми од кој било вид.
6. користење непобарана електронска пошта од мрежи на Агенцијата или други даватели на услуги (сервис провајдери) на Интернет/интранет/екстернет во име на, или за рекламирање, која било услуга поставена на Агенцијата или поврзана преку мрежа на Агенцијата.
7. испраќање на исти или слични некомерцијални пораки на голем број групи на дискусии (спам во групи на дискусии).
8. користење приватна корисничка сметка за електронска пошта за службена комуникација или за каква било размена на информации поврзани со Агенцијата.

2.4. Неприфатлива употреба

Следниве активности се генерално забранети.

Во конкретни случаи, вработените во или соработниците на АКН може да бидат изземени од овие ограничувања во текот на извршувањето на нивните законски работни обврски (на пример, систем администраторите може да треба да го деактивира пристапот до мрежата на работна станица која ги попречува продукциските сервисни услуги).

Во ниту еден случај, вработен во АКН или соработник не е овластен да извршува каква било активност која е незаконска според локалните, националните или меѓународните закони при користење на ресурси во сопственост на АКН.Списокот подолу во ниту еден случај не е исцрпен, но дава рамка за активностите кои влегуваат во категоријата на неприфатлива употреба.

2.4.1. Активности поврзани со ситемите и мрежата

Следниве активности се строго забранети, без исклучоци:

1. повреда на правата на кое било лице или организација заштитени со авторски права, трговска тајна, патент или друга интелектуална сопственост, или слични закони или прописи, вклучувајќи, но неограничувајќисе на, инсталирање или дистрибуција на „пиратски“ или други софтверски производи кои не се соодветно лиценцирани за употреба од страна на АКН.
2. неовластено копирање на авторски заштитени материјали, вклучувајќи, но неограничувајќи се на, дигитализација и дистрибуција на фотографии од списанија, книги или други авторски заштитени извори, авторски заштитена музика, и инсталирање каков било авторски заштитен софтвер за кој Агенцијата, односно релевантното министерство/институција во кое/која се наоѓа Агенцијата/телото/проектот, или крајниот корисник нема активна лиценца.
3. експортирање на софтвер, технички информации, софтвер или технологија за шифрирање, спротивно на меѓународните или регионалните закони за контрола на експортирање.Секој вработен во или соработник на АКН треба да се консултира со соодветното раководство пред да експортира каков било материјал за кој станува збор.
4. поставување злонамерни програми во мрежата или серверот (на пример, вируси, црви, тројанци, пренатрупување на електронската пошта (emailbombs), итн.).
5. откривање на лозинка на корисничка сметка на други лица или дозволување други лица да ја користат сметката.Ова ги вклучува членовите на семејството и другите членови на домаќинството кога се работи од дома.
6. користење компјутерски средства на АКН за добивање или за пренос на материјали кои се спротивни на законите за спречување сексуално вознемирување или непријатно окружување на работното место во локалната јурисдикција на корисникот.
7. користење на компјутерската опрема или кое било друго средство на АКН за лични цели (освен за работа).
8. користење на Интернет за која било цел која не се смета за работна цел.
9. давање лажни понуди на производи, делови или услуги кои потекнуваат од која било сметка на АКН.
10. давање изјави за гаранција, лично или индиректно, освен доколку тоа не е дел од вообичаените работни задачи.
11. пробивање на безбедноста или нарушување на мрежната комуникација.Пробивање на безбедноста вклучува, но не е ограничено на, пристап до податоци за кои вработен во или соработник на АКН не е предвидено да го има или најавување на сервер или сметка до кој/а тој/таа

не е изрично овластен/а да има пристап, освен доколку тие работни задачи не се во опфатот на редовните работни задачи. „Нарушување“ вклучува, но не е ограничено на, прислушување на мрежниот сообраќај (networksniffing), преоптеретување со податоци (pingedfloods), лажирање на изворна ИП адреса (packetspoofing), ускратување пристап до услуга (denialofservice) и фалсификување на движењето на информациите за злонамерни цели.

12. скенирање на портови или скенирање на безбедноста, освен доколку вработен во или соработник на АКН претходно не ја известил АКН за истото.
11. каков било облик на следење на мрежата со кој ќе се пресретнат податоци кои не се наменети за опремата на вработен во или соработник на АКН, освен доколку оваа активност не е дел од неговите редовни работни задачи.
12. заобиколување на автентикација на корисникот или безбедноста на која било опрема, мрежа или сметка.
13. мешање со, или ускратување пристап до услуга на, кој било компјутер освен вашиот (на пример, напад со ускратување пристап до услуга).
14. користење која било скрипта, или испраќање пораки од каков било вид, со намера да се попречи, или оневозможи, корисничката сесија преку какви било средства, локално или преку Интернет/интранет/екстранет.
15. обезбедување информации за, или списоци на, вработени во АКН на страни надвор од АКН.

3. Мерки во случај на непочитување на Процедурата

Секој вработен кој ја прекршува оваа Процедура може да подлежи на дисциплинска постапка, во согласност со соодветното национално законодавство.

4. Објава

Оваа Процедура влегува во сила со денот на донесувањето и истата се објавува на ВЕБ страницата на АКН .

ДИРЕКТОР

м-р Борис Тунцев