

Uživatelé informační sítě krajského úřadu:

- 1) jsou povinni se seznámit s pravidly pro přístup a práci s informačními systémy a zařízením ICT v rámci organizace.
- 2) přidělené ICT prostředky organizace a informace (data), která získávají z počítačové sítě v závislosti na přidělené roli či přidělených přístupových oprávnění, smí používat pouze k výkonu svých pracovních povinností.
- 3) nesmí měnit administrátory ICT nastavené prostředí, včetně pomocných a bezpečnostních SW a služeb systému, zastavovat jejich běh, či je odinstalovat a nesmí se pokoušet vlastními silami řešit bezpečnostní problémy.
- 4) mohou používat pouze legálně přidělený a schválený SW. Svěřené ICT prostředky jsou povinni chránit před ztrátou, poškozením, zničením či odcizením, zejména uzamykat místnosti s ICT technologií při nepřítomnosti zaměstnanců v místnosti a přiměřeným způsobem chránit i přidělené mobilní ICT prostředky. Jsou povinni používat základní bezpečnostní prostředky, např. SW „uzamykání“ prostředku nebo jeho vypínání, pokud není ICT prostředek pod jejich přímou kontrolou (např. při opuštění kanceláře).
- 5) nejsou oprávněni přemísťovat svěřené počítačové vybavení (mimo přenosných zařízení) bez souhlasu OI. Jsou povinni dodržovat všechny bezpečnostní předpisy, opatření a pokyny plynoucí z používání svěřených ICT prostředků tak, aby nemohlo dojít k porušení bezpečnosti informací a chránit veškerá data a klasifikované informace, zvláště pak data s osobními údaji před neoprávněným přístupem jiných osob.
- 6) veškerá hlášení závad a podezřelého chování ICT jsou povinni oznamovat zaměstnancům OI prostřednictvím zadáním požadavku do Service Desku. Pokud tak nelze z technických důvodů učinit, lze v ojedinělých případech hlášení provést hlášení pomocí telefonu nebo e-mailu.
- 7) mají povinnost chránit své autentizační prostředky (prostředky pro ověření uživatele) před jejich prozračením komukoliv jinému. Je zakázán zápis hesel na různé pomůcky, či sdělování osobních hesel jiným osobám, včetně nadřízených. Jsou plně odpovědní za veškeré činnosti v ICT prostředí spojené s autorizovaným uživatelem, možným zneužitím jejich přístupové identity a uživatelských práv. V případě, že uživatel pojme podezření na možné zveřejnění, odcizení nebo prolomení svého hesla, je povinen tuto skutečnost nahlásit OI k zajištění okamžité změny hesla a současně tuto skutečnost nahlásí i MKB.
- 8) elektronickou poštu lze používat pouze k plnění pracovních povinností a nikoli pro soukromé účely. Při přijímání e-mailu musí být mimořádně opatrní při otevírání příloh elektronické pošty, protože mohou obsahovat viry nebo jiné škodlivé kódy.
- 9) internet mohou využívat pouze k pracovním činnostem a webové stránky organizace pouze k prezentování odborných nebo povinných informací. Nesmí prezentovat své osobní názory a činnosti neslučující se s činnostmi úřadu.
- 10) mají právo na poskytnutí nezbytných informací formou školení pro použití ICT pro výkon své práce a jsou povinni se takových školení účastnit.