Český úřad zeměměřický a katastrální

Politika bezpečného chování externích uživatelů aplikací dálkového přístupu resortu ČÚZK

Verze 1.0 platná od 1.7.2018

Ochrana informací je ČÚZK vnímána jako významná součást poskytovaných služeb. Zabezpečení systémů a informací je zajišťováno organizačními a technickými pravidly. Aby tato pravidla byla účinná, je nutné, aby uživatelé využívající služeb resortu ČÚZK dodržovali minimálně následující bezpečnostní zásady.

1. Osobní odpovědnost uživatele

Uživatelé, jimž byl k službám resortu ČÚZK, na základě jejich písemné žádosti přidělen jedinečný identifikátor uživatele (přihlašovací účet) a heslo, odpovídá za způsob použití těchto přihlašovacích údajů a využívání služeb resortu ČÚZK jeho jménem. Uživatel je zcela a nevýlučně odpovědný za škody způsobené neoprávněným konáním a aktivitami ohrožujícími bezpečnost informací a dostupnost služeb resortu ČÚZK, které vznikly jeho pochybením v nedodržení níže uvedených bezpečnostních zásad.

Přidělený jedinečný identifikátor uživatele a přístupová práva ke službám resortu ČÚZK jsou evidována ČÚZK v souladu s platnou vyhláškou o kybernetické bezpečnosti, tj. od okamžiku jeho vydání žadateli, po celou dobu aktivního přístupu uživatele a následně po dobu 12 měsíců od ukončení přístupu uživatele za účelem dohledání původce bezpečnostních událostí a incidentů.

V případě, že žadatelem o přístup ke službám resortu ČÚZK není fyzická osoba, ale společnost nebo organizace, je tato společnost či organizace povinna zajistit vedení evidence všech uživatelů (fyzických osob), kterým pod svým účtem spravuje a vytváří další přístupy ke službám resortu ČÚZK a to včetně evidence jedinečného identifikátoru uživatele, fyzické osoby, které byl přidělen a časového období užívání uvedeném v předchozím odstavci. Toto si vyhrazuje ČÚZK případně zkontrolovat.

2. Řízení přístupu ke službám resortu ČÚZK

Využívat služeb resortu ČÚZK je povoleno pouze uživatelům, kteří si požádali o přístup k dané službě ČÚZK na k tomu určeném formuláři zveřejněném na webových stránkách ČÚZK a jejichž žádost byla schválena.

Uživatelé jsou povinni si po obdržení přístupových údajů při prvním přístupu ke službě změnit toto inicializační heslo za nové. Nové heslo musí mít minimální délku 12 znaků. Toto nové heslo jsou povinni držet v tajnosti. To znamená nikomu jej nesdělovat, neponechávat napsané v místech s přístupem dalších osob, neukládat do souboru volně přístupného dalším

uživatelům. Přičemž maximální doba používání hesla je stanovena na 6 měsíců. Poté si uživatel musí znovu heslo změnit na nové.

Pro heslo nesmí uživatel použít snadno identifikovatelná jména (vlastní, rodičů, sourozenců, dětí, domácích zvířat apod.), datumy narození, názvy měsíců, a jiné snadno predikovatelné kombinace. Stejně tak není povoleno zvolit si nejčastěji používaná hesla (např. 12345, heslo123, apod.), tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem.

Je zakázáno sdílet účet více fyzickými osobami.

3. Bezpečnost počítače uživatele

Uživatelé, společnosti a organizace využívající služby resortu ČÚZK jsou povinni zajistit bezpečnost počítačů notebooků, tabletů a chytrých telefonů, ze kterých k službám resortu ČUZK přistupují a to v následujícím minimálním rozsahu:

- Aplikovat opatření proti ovládnutí počítače cizí osobou:
    - Neponechávat přihlášený počítač volně bez dozoru, vždy jsou povinni uzamknout počítač
    - Nepoužívat při běžné práci na počítači účet s právy správce (administrátora) systému
    - Neodpovídat na podezřelé e-maily (zejména neposílat nikomu své přihlašovací údaje, apod.)
    - Používat pouze legitimní (legálně nabytý) software
    - Zajistit pravidelné bezpečnostní aktualizace softwaru na svém počítači
- Zajistit počítač před působením škodlivého kódu:
    - Mít nainstalovaný funkční antivirus
    - Zajistit pravidelnou a včasnou aktualizaci virové báze
    - Neotvírat podezřelé dokumenty a přílohy e-mailů zaslané či získané z neznámých či nedůvěryhodných zdrojů
    - Nenavštěvovat podezřelé webové stránky
    - Instalovat pouze ověřený software

Při jakémkoliv podivném či nestandardním chování počítače je jeho uživatel povinen okamžitě přestat využívat služeb resortu ČÚZK, odhlásit se a zajistit kontrolu počítače. V případě jeho napadení sjednat nápravu nebo tuto zajistit u svého správce počítače.

4. Bezpečnostní incidenty

Uživatel je povinen na Helpdesk ČÚZK prostřednictvím kontaktního formuláře https://helpdesk.cuzk.cz/ehd/vytvorPozadavek hlásit jako bezpečnostní incident minimálně tyto případy:

- podezření na kompromitaci hesla (jeho prozrazení, odposlechnutí, či uhodnutí jinou osobou); v takovém případě je uživatel povinen neodkladně provést změnu hesla;
- jakékoliv podivné nebo nestandartní chování služby resortu ČÚZK a jiných okolností souvisejících s využíváním těchto služeb indikujících bezpečnostní incident (neplatné certifikáty serveru, …).

V případě bezpečnostního incidentu je uživatel povinen reagovat na výzvu ČÚZK a poskytnout požadovanou součinnost včetně veškerých údajů potřebných k vyhodnocení a řešení bezpečnostního incidentu.