Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

Pokud jsou tato obecná pravidla v rozporu s ustanovením textu smlouvy/objednávky uzavírané mezi dodavatelem a Českou národní bankou (dále jen „ČNB“) nebo textu zadávací dokumentace na veřejnou zakázku nebo jejich jinou přílohou, má přednost ustanovení textu smlouvy/objednávky nebo zadávací dokumentace nebo jejich jiná příloha.

1. Dodavatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle smlouvy/objednávky podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u ČNB seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
2. Dodavatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy/objednávky s ČNB.
3. Dodavatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
4. Pracovníci dodavatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
5. Dodavatel a jeho pracovníci nejsou oprávněni:
    a. obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
    b. sdělovat své přístupové údaje k systémům ČNB;
    c. sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
    d. provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
6. Dodavatel a jeho pracovníci jsou povinni:
    a. okamžitě nahlásit sekci informatiky ČNB, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro dodavatele, jejichž předmět smlouvy/objednávky obsahuje tuto činnost;
    b. při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit a ověřit, že k odhlášení/uzamčení opravdu došlo;
    c. bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku ČNB;
    d. bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;

KONTAKT:
odbor obchodní
odbor architektury a bezpečnosti informačních technologií
Na Příkopě 28
115 03 Praha 1
T: +420 224 411 111
www.cnb.cz

e. v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk ČNB a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku ČNB.

7. Pracovníci dodavatele nesmí:
   a. zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);
   b. používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).
8. Pracovníci dodavatele nejsou oprávněni:
   a. používat soukromou e-mailovou schránku pro činnosti související s plněním dle smlouvy/objednávky, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;
   b. nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;
   c. ukládat jiné než veřejné informace mimo úložiště pod správou ČNB nebo dodavatele (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).
9. Dodavatel a jeho pracovníci nejsou oprávněni:
   a. nepovoleně používat, kopírovat a šířit software, jako např.:
      i. instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);
      ii. instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět smlouvy/objednávky obsahuje tuto činnost;
      iii. instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí
         1. pro situace výslovně schválené a popsané v jiném vnitřním předpisu ČNB (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a
         2. v případech, kdy předmět smlouvy/objednávky obsahuje tuto činnost;

b. používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;

c. bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

1. Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.
2. Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury státu, jsou přístupy uživatelů na Internet ze sítě ČNB automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).

Verze 1.0 ze dne 14. 4. 2023

KONTAKT:
odbor obchodní
odbor architektury a bezpečnosti informačních technologií
Na Příkopě 28
115 03 Praha 1
T: +420 224 411 111
www.cnb.cz