Pravidlá bezpečného používania Centrálneho informačného systému (CST2021)

Verzia 1.0

Hlava 1. Slovník pojmov

Význam pojmov použitých v pravidlách:

1) Systém - aplikácie Centrálneho informačného systému 2021 (CST2021), na ktoré sa vzťahujú tieto pravidlá:
    1. SL2021 Projekty, umožňuje riadenie zmlúv o poskytnutí príspevku a vyúčtovanie projektov,
    2. SR2021, umožňuje predkladanie správ,
    3. SZT2021, umožňuje spravovanie totožnosti používateľa a spoločné prihlasovanie do aplikácií Systému,
    4. Správa (vrátane eSZOP), umožňuje správu oprávnení, slovníkov a popisov programov,
    5. WOD2021, umožňuje prípravu a riadenie výberových konaní a žiadostí o príspevok,
    6. e-Kontroly, umožňuje vedenie a evidenciu výsledkov kontrol projektov.
2) Správca obsahu – zamestnanec určený Orgánom, ktorý plní úlohy v oblasti zavádzania CST2021,
3) Prijímateľ – subjekt, ktorý je uvedený v čl. 2 bod 9 všeobecného nariadenia,
4) Osobné údaje – informácie uvedené v čl. 4 bod 1 GDPR,
5) Incident – jedna udalosť alebo séria nežiaducich alebo neočakávaných udalostí súvisiacich s ochranou informácií alebo so znížením úrovne systémových služieb, ktorý predstavuje vysokú pravdepodobnosť narušenia práce Systému a ohrozuje bezpečnosť informácií vrátane v Systéme spracúvaných osobných údajov,
6) Orgán – Riadiaci orgán, ktorý je uvedený v čl. 71 všeobecného nariadenia alebo v čl. 46 nariadenie Interreg, Orgán auditu, ktorý je uvedený v čl. 71 všeobecného nariadenia alebo čl. 45 nariadenia Interreg,
7) Ministerstvo – úrad príslušného ministra pre regionálny rozvoj – Riadiaci orgán,
8) Zraniteľnosť – nedostatok (slabina) aktíva alebo skupiny aktív, ktorá môže byť zneužitá najmenej jednou hrozbou, chápaná ako potenciálna príčina nežiaduceho incidentu, ktorý môže spôsobiť poškodenie Systému,
9) Program – program v zmysle nariadenia Interreg,
10) Partner – subjekt využívajúci Systém v rámci realizácie projektu,
11) GDPR – nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe, ktorým sa zrušuje smernica 95/46/ES (Ú. v. ES L. 2016.119.1),
12) Nariadenie Interreg - nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1059 z 24. júna 2021 o osobitných ustanoveniach týkajúcich sa cieľa Európska územná spolupráca (Interreg) podporovaného z Európskeho fondu regionálneho rozvoja a vonkajších finančných nástrojov (Ú. v. EÚ L 231 z 30. júna 2021),
13) Všeobecné nariadenie - nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1060 z 24. júna 2021, ktorým sa stanovujú spoločné ustanovenia o Európskom fonde regionálneho rozvoja, Európskom sociálnom fonde plus, kohéznom fonde, Fonde na spravodlivú transformáciu a Európskom námornom, rybolovnom a akvakultúrnom fonde a rozpočtové pravidlá pre uvedené fondy, ako aj pre Fond pre azyl, migráciu a integráciu, Fond pre vnútornú bezpečnosť a Nástroj finančnej podpory na riadenie hraníc a vízovú politiku (Ú. v. EÚ L 231 z 30. júna 2021),
14) Užívateľ – osoba s prístupom do Systému, určená Orgánom, aby v jeho mene vykonávala činnosti súvisiace s realizáciou programu alebo v mene Žiadateľa, Prijímateľa alebo Partnera plnila činnosti súvisiace s realizáciou projektu,
15) Príslušný orgán – je zodpovedný za kontakt s Prijímateľom v súvislosti s projektom v danom štádiu realizácie projektu. Pred podpísaním zmluvy je to orgán, ktorý organizuje výberové konanie žiadostí o príspevok. Po podpísaní zmluvy je to orgán, s ktorým Prijímateľ uzavrel zmluvu alebo orgán, ktorý vykoná vyúčtovanie projektu (ak je iný, ako uzatvárajúci zmluvu),
16) Žiadateľ – subjekt, ktorý pripravuje alebo podal žiadosť o príspevok, ale zatiaľ nepodpísal zmluvu o poskytnutí príspevku,
17) Udalosť súvisiaca s bezpečnosťou informácií – stav Systému, služby alebo siete, ktorý indikuje možné porušenie týchto pravidiel, bezpečnostnú chybu alebo doteraz neznámu situáciu, ktorá môže súvisieť s bezpečnosťou.

Hlava 2. Všeobecné ustanovenia

1) CST2021 je centrálny systém založený na povinnosti vyplývajúcej z čl. 69 ods. 8 a čl. 72 ods. 1 pís. e) všeobecného nariadenia, ktorý umožňuje vykonávať:
    a. funkcie Riadiacich orgánov, uvedené vo všeobecnom nariadení, a to najmä v oblasti elektronickej evidencie a uchovávania dát každej operácie, potrebných na monitorovanie, vyhodnocovanie, finančné riadenie, overovanie a audity v súlade s prílohou č. XVII k všeobecnému nariadeniu,
    b. povinnosť členského štátu zabezpečiť primeranú kvalitu, presnosť a spoľahlivosť monitorovacieho systému a údajov o ukazovateľoch,
    c. povinnosť členského štátu zabezpečiť, aby celá výmena informácií medzi prijímateľmi a orgánmi programu prebiehala prostredníctvom systémov elektronickej výmeny dát v súlade s prílohou č. XIV všeobecného nariadenia.
2) Pravidlá stanovujú práva a povinnosti užívateľov v oblastiach:
    a) používania Systému,
    b) konfigurácie počítačového zariadenia Užívateľa,
    c) začatia, pozastavenia a ukončenia práce Užívateľa v Systéme,
    d) používania elektronickej pošty a internetu,
    e) oznamovania chýb, porúch, poškodenia, zraniteľnosti a incidentov v Systéme,
    f) spracovania osobných údajov v Systéme.
3) Užívateľ, ktorý vkladá údaje do Systému, je povinný zabezpečiť ich kvalitu, najmä pravdivosť a súlad so štruktúrou dát požadovanou Systémom.

Hlava 3. Podmienky používania Systému

1. Pre správne používanie Systému je potrebné:
    a) pripojiť sa na internet;
    b) nainštalovať jeden z uvedených webových prehliadačov v požadovanej verzii major alebo novšej: Mozilla Firefox (verzia 80), Google Chrome (verzia 85), Microsoft Edge (verzia 86) alebo Safari (verzia 12),
    c) zapnúť podporu technológie Java Script, akceptovať tzv. "cookies" a vypnúť blokovanie automaticky otváraných okien vo webovom prehliadači.
2. Ministerstvo nezodpovedá za nemožnosť prístupu do Systému z dôvodov, ktoré ministerstvo nemôže ovplyvniť.
3. Aplikácie Systému sú v nepretržitom 24 – hodinovom prevádzkovom režime denne – s výnimkou prestávky na údržbu, ktorá pripadá na hodiny od 0:30 do 5:00 (7:00 v prípade aplikácie SR2021) stredoeurópskeho času.
4. V súvislosti s realizáciou prác súvisiacich so správou alebo modifikáciou funkčnosti Systému, z bezpečnostných dôvodov alebo z iných dôvodov nezávislých od Ministerstva, má Ministerstvo právo dočasne pozastaviť prístup Užívateľov do Systému v iných hodinách ako uvedených v odseku 3 na dobu potrebnú na vykonanie plánovaných prác alebo odstránenie nežiadúcich udalostí. Ministerstvo vopred oznámi plánované prestávky súvisiace s údržbovými prácami v Systéme.
5. Užívateľ nesmie neoprávnene monitorovať Systém, vrátane jeho zabezpečenia, ani sa pokúsiť narušiť bezpečnosť údajov spracúvaných v Systéme, vrátane pokusov o nabúranie zabezpečenia Systému.
6. Systém používa súbory „cookies" na uľahčenie používania Systému a na technické a štatistické účely. Nezablokovanie týchto súborov Používateľom znamená, že súhlasí s ich používaním a ukladaním do pamäte svojho počítača alebo iného zariadenia. Používateľ môže samostatne zmeniť nastavenia prehliadača tak, aby zablokoval ukladanie „cookies", ale táto úprava mu zabráni Systém používať.
7. Ministerstvo zhromažďuje informácie o IP adrese, z ktorej sa používateľ prihlásil do Systému. Ministerstvo zhromažďuje IP adresy výhradne za účelom odhaľovania pokusov o narušenie bezpečnosti Systému a vykonávania auditu bezpečnosti Systému.
8. Ministerstvo nezodpovedá za škody spôsobené v súvislosti s používaním Systému, alebo v súvislosti s nesprávnou prevádzkou Systému spôsobenou chybami, nedostatkami, poruchami, defektami, oneskorením prenosu dát, počítačovými vírusmi, poruchami pripojenia k webovej sieti alebo nedodržaním ustanovení týchto pravidiel.
9. Užívateľ je povinný nahlásiť každé porušenie informačnej bezpečnosti alebo porušenie bezpečnosti osobných údajov spôsobom uvedeným v Hlave 9 týchto pravidiel.
10. Užívateľ môže pracovať v danej relácii iba s použitím jedného účtu alebo v jednom pracovnom kontexte. Nedovoľuje sa súčasne spúšťať niekoľko relácií prehliadača a zároveň pracovať v Systéme na viac ako jednom vlastnom účte alebo v jednom pracovnom kontexte.
11. Ministerstvo si vyhradzuje právo pozastaviť používanie účtu Užívateľovi, ktorý porušil zákon alebo ustanovenia týchto pravidiel.
12. Ministerstvo môže trvalo zablokovať účet Užívateľa, ak tento Užívateľ bude aj naďalej konať v rozpore so zákonom alebo ustanoveniami týchto pravidiel. Ministerstvo oznámi príslušnému subjektu pozastavenie alebo zablokovanie užívateľského účtu, ktorý daný subjekt zastupuje.

Hlava 4. Prístup do Systému

1. Prihlásenie sa do Systému je možné pod podmienkou, ak si samotný Užívateľ alebo osoba oprávnená riadiť Užívateľov v subjekte, v ktorého mene má Užívateľ pôsobiť v Systéme (správca), založí účet a nastaví heslo. Užívateľ by si mal neodkladne zmeniť heslo poskytnuté správcom.
2. Používanie funkcií Systému je možné iba pod podmienkou, že osoba oprávnená riadiť Užívateľov v subjekte, v mene ktorého má Užívateľ v systéme pôsobiť, splnomocní Užívateľa. Autentifikácia Užívateľa prebieha v aplikácii SZT pomocou prihlasovacieho mena a hesla. V závislosti od udelených oprávnení má potom autentifikovaný Užívateľ prístup k jednotlivým aplikáciám Systému a ich funkciám.
3. Akceptovaním týchto pravidiel Užívateľ súhlasí so zasielaním elektronických informácií o Systéme.
4. Ministerstvo poskytuje návod na používanie Systému na webových stránkach programu.
5. Užívateľ je zodpovedný za všetky svoje aktivity v Systéme, ktoré vykoná na svojom účte prostredníctvom svojho prihlasovacieho mena a hesla, ktoré používa.

Hlava 5. Bezpečnostné predpisy

1. Užívateľ je povinný oboznámiť sa a prijať tieto pravidlá, čo potvrdí (predložením vyhlásenia na elektronickom tlačive) pri prvom prihlásení sa do Systému a po úprave týchto pravidiel.
2. Podmienkou pre získanie prístupu do Systému je predloženie vyhlásenia, uvedeného v bode 1. Informácie o dátume a hodine poskytnutého vyhlásenia Užívateľa sú uložené v Systéme.
3. Užívateľ je povinný dodržiavať tieto pravidlá.
4. Systém je konfigurovaný podľa týchto pravidiel sily hesla:
    a) heslo pozostáva najmenej z 10 znakov (maximálna dĺžka hesla je 32 znakov),
    b) heslo obsahuje veľké a malé písmená ako aj číslice a špeciálne znaky,
    c) heslo nesmie obsahovať prihlasovacie meno užívateľa,
    d) nové heslo sa musí odlišovať od všetkých archívnych hesiel.
5. Doba trvania neaktívnej relácie (doba nečinnosti), po ktorej bude Užívateľ automaticky odhlásený, je 30 minút.
6. Heslo musí byť neodkladne nahradené novým heslom, v prípade jeho neúmyselného odhalenia neoprávnenej osobe alebo podozrenia z jeho prezradenia.
7. Ak si Užívateľ nemôže zmeniť heslo (príslušná funkcia Systému je nefunkčná), oznámte to správcovi užívateľov v subjekte, ktorý Užívateľa zastupuje v Systéme.
8. Užívateľ za účelom zabránenia neoprávnenému prístupu do Systému:
    1) nesmie uchovávať prihlasovacie údaje do Systému na miestach prístupných iným osobám;
    2) prihlasovacie údaje nesmie poskytnúť iným osobám.
9. Používanie Systému s využitím prístupových údajov iného Užívateľa je zakázané.
10. Užívateľ je povinný nastaviť obrazovku monitora tak, aby znemožnil neoprávneným osobám prezeranie alebo zapisovanie aktuálne zobrazených informácií na obrazovke monitora.
11. Počítač Užívateľa by mal byť situovaný tak, aby bol neoprávneným osobám zabránený prístup k vonkajším portom alebo aby mal Užívateľ prístup k vonkajším portom aspoň vizuálne pod kontrolou.
12. Užívateľ je povinný dodržiavať zásadu čistého pracovného stola. Užívateľ by mal najmä pred opustením svojho pracoviska ukryť všetky dokumenty týkajúce sa používaného Systému a dátových nosičov (diskety, CD, DVD, BD, pendrive atď.).

Hlava 6. Konfigurácia zariadenia Užívateľa

1) Počítač Užívateľa musí byť vybavený antivírusovým softvérom s najmenej raz týždenne aktualizovanou databázou vírusov. Antivírusový softvér musí byť nepretržite aktívny.
2) Užívateľ je povinný neustále sledovať oznámenia zasielané antivírusovým softvérom nainštalovaným v pracovnom zariadení, na ktoré je povinný reagovať.
3) Počítač Užívateľa musí byť chránený sieťovou bránou (firewall).
4) Pri práci so Systémom by v počítači Užívateľa nemal byť otvorený žiadny server, najmä by nemali byť aktívne WWW a FTP servery (TFTP).
5) Zariadenie a softvér musia byť pravidelne aktualizované podľa pokynov výrobcov. Týka sa to najmä operačného systému a webového prehliadača.
6) Webový prehliadač musí byť konfigurovaný tak, aby mal aktívnu podporu protokolu OCSP (Online Certificate Status Protocol), na overenie platnosti certifikátu Systému.
7) Odporúča sa, aby Užívateľ počas práce v Systéme nepoužíval neznáme alebo nezabezpečené WiFi siete.

Hlava 7. Začatie, prerušenie a ukončenie práce Užívateľov v Systéme

1) Počas prihlasovania je Užívateľ povinný skontrolovať:
    a. či sa adresa v adresnom riadku panela prehliadača začína od https,
    b. či je v okne prehliadača malý visací zámok, ktorý informuje o bezpečnosti,
    c. či sa po kliknutí na visací zámok zobrazí informácia, že certifikát bol vydaný pre: *.cst2021.gov.pl a je platný.
2) Pripojenie k Systému je šifrované.
3) Na dočasné prerušenie práce v Systéme, uzamknite obrazovku, a teda zablokujte pracovnú plochu alebo aktivujte šetrič obrazovky chránený heslom. Ak počítač Užívateľa neumožňuje zabezpečiť obrazovku heslom, odhláste sa zo Systému.
4) Po ukončení práce sa odhláste zo Systém pomocou funkcie "Odhlásiť sa" umiestnenej nad menu v pravom hornom rohu obrazovky. Práca nesmie byť ukončená len zatvorením okna prehliadača pomocou znaku „X”.

Hlava 8. Elektronická pošta, Internet

1) Systém využíva funkciu zasielania oznámení na e-mailovú adresu, ktorá je uložená v Systéme. Užívateľ je povinný zaistiť bezpečnosť svojho vyššie uvedeného e-mailového účtu najmä formou:
    a) používania silného prístupového hesla,
    b) neotvárania e-mailových príloh a odkazov neznámeho pôvodu,
    c) zvýšenej opatrnosti pri otváraní neočakávaných príloh v korešpondencii od známych odosielateľov.
2) Užívateľ by mal používať webovú sieť spôsobom, ktorý neohrozuje bezpečnosť Systému.

Hlava 9. Oznámenie o ohrození bezpečnosti

1) V prípade:
    a) spozorovania zraniteľnosti,
    b) udalosti súvisiacej s bezpečnosťou informácií,
    c) incidentu,
    d) zistenia, že stav počítačového zariadenia, obsah súboru osobných údajov v systéme, zverejnené pracovné postupy, spôsob fungovania programu alebo kvalita komunikácie v telekomunikačnej sieti môžu indikovať porušenie bezpečnosti osobných údajov spracúvaných v Systéme,

    je užívateľ, ktorý zastupuje Žiadateľa, Prijímateľa alebo Partnera, povinný bezodkladne o tom informovať príslušný Orgán.
2) V prípade:
    a) spozorovania zraniteľnosti,
    b) udalosti súvisiacej s bezpečnosťou informácií,
    c) incidentu,
    d) podozrenia výskytu zraniteľnosti alebo incidentu,
    e) zistenia, že stav počítačového zariadenia, obsah súboru osobných údajov v systéme, zverejnené pracovné postupy, spôsob fungovania programu alebo kvalita komunikácie v telekomunikačnej sieti môžu indikovať porušenie bezpečnosti osobných údajov spracúvaných v Systéme,

    je užívateľ, ktorý zastupuje Orgán, povinný bezodkladne informovať o tom Správcu obsahu v danom Orgáne.
3) Užívateľ, ktorý je Správcom obsahu postupuje podľa Postupu spracovania hlásení v Service Desk Centrálneho informačného systému.

Hlava 10. Informácie o spracovaní osobných údajov Užívateľov a iných osobných údajov zavedených do systému

1) Správcami osobných údajov v zmysle ustanovení GDPR sú príslušné subjekty zapojené do implementácie programu, najmä Minister, Riadiaci orgán, Orgán auditu, Spoločný sekretariát, príslušný kontrolór.
2) Správcovia spracúvajú osobné údaje na účely uvedené v čl. 4 všeobecného nariadenia.
3) Osobné údaje sú uchovávané po dobu nevyhnutnú na splnenie hore uvedených cieľov, a teda do času vyúčtovania programov za roky 2021-2027 a uplynutia obdobia udržateľnosti a ukončenia kontroly udržateľnosti pre všetky projekty.

4) Užívateľ je povinný zachovávať mlčanlivosť o spracúvaných osobných údajoch a informáciách o spôsoboch ich ochrany, a to počas používania Systému ako aj po jeho ukončení.
5) Užívateľ zodpovedá za zhodnosť osobných údajov poskytnutých Systému so zdrojovými dokumentmi.
6) Každý Užívateľ má právo na prístup k svojim osobných údajom, na ich doplnenie, vykonanie ich aktualizácie alebo opravy.
7) Osobné údaje Užívateľov sú viditeľne spracúvané v Systéme, a teda pri správe oprávnení, ukladaní auditných dát o vykonávaných činnostiach a podpisovaní dokumentov. Okrem týchto pravidiel, Užívateľovi nie je poskytnutá dodatočná informačná doložka o tejto téme.
8) Každý Užívateľ môže podať sťažnosť dozornému orgánu, ktorým je riaditeľ Úradu na ochranu osobných údajov v Poľsku.