Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Brno 23. července 2026

20092/2026-NÚKIB-E/210

NUKIX006COI6

Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážená paní [redacted]

Národní úřad pro kybernetickou a informační bezpečnost (dále jen jako „**Úřad**“ nebo „**NÚKIB**“) obdržel dne 9. července 2026 Vaši žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „**InfZ**), vedenou pod č. j. 20095/2026-NÚKIB-E/210. V žádosti požadujete poskytnutí informací týkajících se organizačního zajištění Úřadu.

Tímto Vám sděluji, ve struktuře otázek dle Vaší žádosti, následující informace:

1. **Dotaz:** „*Uveďte, zda je ve Vaší organizaci některému organizačnímu útvaru nebo pracovní pozici svěřena koordinace funkcí zajišťujících soulad činnosti organizace s právními a interními předpisy. Pokud ano, uveďte název útvaru nebo pracovní pozice.* „

   Odpověď: V rámci Úřadu není zřízen samostatný organizační útvar ani pracovní pozice, které by byla svěřena celková koordinace funkcí zajišťujících soulad činnosti organizace s právními a interními předpisy. Jednotlivé oblasti související se zajišťováním souladu jsou vykonávány příslušnými organizačními útvary v rozsahu jejich věcné působnosti stanovené organizačním řádem.

2. **Dotaz:** „*Má Vaše organizace zřízen samostatný útvar nebo pracovní pozici označenou jako „Compliance“, „Compliance Officer“ nebo obdobně? Pokud ano, uveďte název.*“

   Odpověď: Úřad žádný takový samostatný útvar ani pracovní pozici nemá.

3. **Dotaz: „***Prosím uveďte organizační útvar nebo pracovní pozici odpovědnou za následující oblasti:*

   • *Legislativní monitoring*

   • *Implementace nové legislativy*

   • *Metodická podpora útvarům při plnění regulatorních požadavků*

   • *Řízení compliance rizik (pokud je rozlišováno od obecného řízení rizik)*

   • *Řízení předpisové základny*

   • *Řízení rizik*

   • *Interní kontrolní systém*

   • *Interní audit*

• *Etický kodex*

• *Prevence střetu zájmů*

• *Evidence vydaných a přijatých dar*

• *Protikorupční agenda*

• *Ochrana oznamovatelů*

• *Ochrana osobních údajů (GDPR)*

• *Kybernetická bezpečnost*

• *Dohled nad využíváním systémů umělé inteligence (pokud je organizačně zajištěn)*

Odpověď:

• *Legislativní monitoring*

Za legislativní monitoring odpovídá oddělení vládní agendy a legislativy, odbor právní a odbor mezinárodní spolupráce a Evropské unie.

• *Implementace nové legislativy*

Za implementaci nové legislativy odpovídá věcně příslušný celek v součinnosti odborem právním.

• *Metodická podpora útvarům při plnění regulatorních požadavků*

V případě poskytování právní podpory odpovídá za výkon této agendy odbor právní. V ostatních případech je odpovědnost svěřena věcně příslušnému organizačnímu celku.

• *Řízení (compliance) rizik (pokud je rozlišováno od obecného řízení rizik)*

Za řízení rizik odpovídá odbor plánování, řízení a fondů. Konzultační činnost k řízení rizik provádí interní auditor.

• *Řízení předpisové základny*

Tato činnost spadá do působnosti sekce personalistiky, práva a provozu.

• *Interní kontrolní systém a interní audit*

Za interní kontrolní systém a interní audit zodpovídá interní auditor.

• *Etický kodex*

Není svěřeno žádnému konkrétnímu organizačnímu celku.

• *Prevence střetu zájmů*

Oddělení personálních věcí a vzdělávání ve spolupráci s odborem právním spolupracuje na zajišťování povinností vyplývajících ze zákona č. č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů.

• *Evidence vydaných a přijatých darů*

Dle etického kodexu za evidenci zodpovídá nadřízený pracovník konkrétního zaměstnance, který dar přijímá nebo vydává.

• *Protikorupční agenda*

Za protikorupční agendu zodpovídá odbor bezpečnosti.

• *Ochrana oznamovatelů*

Za ochranu oznamovatelů zodpovídá odbor právní.

• *Ochrana osobních údajů (GDPR)*

Agenda GDPR spadá pod pověřence pro ochranu osobních údajů.

• *Kybernetická bezpečnost*

Za kybernetickou bezpečnost zodpovídá manažer kybernetické bezpečnosti.

• *Dohled nad využíváním systémů umělé inteligence (pokud je organizačně zajištěn)*

V současné době probíhají práce na tvorbě mechanismu pro dohled nad využíváním systémů umělé inteligence pro naplnění požadavků z nařízení Evropského parlamentu a Rady (EU) 2024/1689, akt o umělé inteligenci. Tento úkol zajišťuje odbor právní.

4. **Dotaz: „***Existuje ve Vaší organizaci mechanismus koordinace/centralizace výše uvedených oblastí? Pokud ano, stručně uveďte, jak je tato koordinace organizačně zajištěna.“*

   Odpověď: Koordinace této oblasti není na Úřadě svěřena konkrétnímu útvaru ani pracovní pozici. Agenda je vykonávána decentralizovaně napříč organizačními celky v souladu s jejich věcnou působností.

5. **Dotaz: „***Jsou výstupy z agend uvedených ve článku II. (zde bod 3) pravidelně předkládány vedení organizace?***“**

   Odpověď: Výstupy z uvedených agend nejsou vedení organizace předkládány v pravidelných intervalech. Vedení je o relevantních skutečnostech a významných výstupech průběžně informováno podle jejich povahy, významu a aktuální potřeby. Pro zajištění informovanosti vedení má Úřad nastaveny odpovídající komunikační a řídicí mechanismy, které umožňují předkládání informací a eskalaci záležitostí vyžadujících pozornost nebo rozhodnutí vedení.

6. **Žádost o zaslání následujících dokumentů:**

   • *organizační řád nebo jeho relevantní část,*

   • *organizační struktura,*

   • *interní předpis upravující systém řízení souladu nebo compliance (je-li vydán),*

   • *interní předpis upravující ochranu oznamovatelů,*

   • *etický kodex*

   Výše požadované dokumenty jsou poskytnuty přílohou ve formátu pdf.

S pozdravem

Elektronický podpis: 23.7.2026
Certifikát autora podpisu:
Jméno: Mgr. Vít Hrazdíra
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 19.11.2026 19:15 +01:00

Mgr. Vít Hrazdíra
vedoucí oddělení právní a
přestupkové agendy
Národní úřad pro kybernetickou
a informační bezpečno

Obdrží:
[redacted]
Vypraveno dne:
viz časový údaj na obálce datové zprávy

Pořadové číslo:	Platí od:	Ruší:
S05/2026	**01.07.2026**	**S14/2025**
Č. j.: 18388/2026-NÚKIB-E/200		
Druh vnitřního aktu řízení:		
SMĚRNICE **ŘEDITELE NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST**		
Název:		
Organizační řád **Národního úřadu pro kybernetickou a informační bezpečnost**		

ČÁST PRVNÍ

Čl. 1
Účel Organizačního řádu

(1) Organizační řád Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“) vymezuje postavení a úkoly Úřadu, jeho organizační strukturu, vnitřní vztahy a působnost jednotlivých organizačních celků.

(2) Organizační řád Úřadu se považuje za vnitřní předpis podle zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

(3) Organizační řád je závazný pro všechny zaměstnance v pracovním poměru k Úřadu a přiměřeně též pro zaměstnance, jejichž pracovněprávní vztah k Úřadu je založen na základě dohod o pracích konaných mimo pracovní poměr.

POSTAVENÍ, PŮSOBNOST A HLAVNÍ ÚKOLY ÚŘADU

Čl. 2
Postavení a působnost

(1) Úřad vykonává jako ústřední orgán státní správu pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon o ochraně utajovaných informací“) a dále zajišťuje činnost Příslušného orgánu veřejně regulované služby programu Galileo (dále jen „PRS“) (Competent PRS Authority – CPA) a také Příslušného orgánu pro program GOVSATCOM a Secure Connectivity. Úřad je zřizovatelem specializovaného archivu a bezpečnostního archivu, které jsou součástí soustavy veřejných archivů.

(2) Úřad je organizační složkou státu a jeho působnost je vymezena v zákoně č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“) a v zákoně o ochraně utajovaných informací. Činnost archivů je vymezena zákonem č. 499/2005 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů.

(3) Sídlem Úřadu je Brno.

Čl. 3
Hlavní úkoly

(1) Úřad v rámci zásad činnosti ústředních správních úřadů stanovených jiným právním předpisem

a) vytváří koncepci rozvoje ochrany kybernetické, informační a kryptografické bezpečnosti i pro vybrané oblasti ochrany utajovaných informací v České republice s vazbami na jiné obory a služby s celostátní a mezinárodní působností a navrhuje vládě České republiky řešení stěžejních otázek v této oblasti,
b) připravuje vládní návrhy zákonů a prováděcích právních předpisů ve věcech spadajících do jeho působnosti,
c) zaujímá stanoviska k návrhům, které předkládají vládě České republiky ministerstva a jiné ústřední orgány státní správy,

d) dbá o zachování zákonnosti ve svěřené působnosti a činí podle zákonů potřebná nápravná opatření,
e) zabezpečuje ve své působnosti úkoly související se sjednáváním a plněním mezinárodních smluv a jiných dohod s mezinárodním prvkem, s rozvojem mezistátních styků a mezinárodní spolupráce,
f) zabezpečuje ve své působnosti úkoly, které vyplývají pro Českou republiku z mezinárodních smluv a jiných dohod s mezinárodním prvkem, jakož i z členství v mezinárodních organizacích, úkoly související s členstvím České republiky v Organizaci Severoatlantické smlouvy (dále jen „NATO“),
g) předkládá za svěřenou oblast státní správy podklady potřebné pro sestavení návrhu státního rozpočtu, jeho plnění a pro vyhodnocení státního závěrečného účtu,
h) vyměňuje si s ministerstvy a jinými ústředními správními úřady navzájem potřebné informace a podklady,
i) informuje o vydaných opatřeních přiměřeným způsobem veřejnost; to neplatí, jestliže by zpřístupnění takových informací mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost vydaného opatření,
j) zajišťuje vyřizování žádostí o poskytnutí informací fyzickým a právnickým osobám podle jiného právního předpisu,
k) zajišťuje činnost Národního centra kybernetické bezpečnosti,
l) zajišťuje vzdělávání, určování a koordinaci identifikace povinných subjektů dle zákona o kybernetické bezpečnosti a realizaci úkolů svěřených Úřadu v oblasti regulace cloud computingu ve veřejné správě,
m) plní úkoly vládního koordinačního místa pro okamžitou reakci na kybernetické bezpečnostní incidenty — Computer Emergency Response Team (dále jen „vládní CERT“),
n) působí jako koordinační orgán ve stavu kybernetického nebezpečí,
o) stanoví v oblasti kybernetické bezpečnosti bezpečnostní opatření a vydává opatření,
p) zajišťuje činnost Národního centra PRS (veřejně regulované služby – public regulated service — programu Galileo), (dále jen „Národní centrum PRS“),
q) působí jako Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti pro Českou republiku podle přímo použitelného předpisu EU,
r) zabezpečuje činnost Rady pro kybernetickou bezpečnost a Výboru pro kybernetickou bezpečnost,
s) plní úkoly Národního střediska pro bezpečnost informačních systémů,
t) plní úkoly Národního střediska pro měření kompromitujícího vyzařování,
u) plní úkoly Národního bezpečnostního komunikačního střediska (NCSA),
v) zajišťuje a plní úkoly Národního střediska pro distribuci kryptografického materiálu (NDA),
w) zajišťuje a plní úkoly Vnitrostátního orgánu certifikace kybernetické bezpečnosti (NCCA),
x) zajišťuje a plní úkoly Vnitrostátního orgánu certifikace kryptografických prostředků a pracovišť,
y) zajišťuje a plní úkoly Vnitrostátního orgánu vývoje kryptografických prostředků,
z) provádí ukládání a péči o archiválie vzniklé činností Úřadu, jako součást Národního archivního dědictví.

(2) Úřad dále

a) stanovuje pravidla zavádění a používání prostředků a systémů určených k ochraně utajovaných informací a k zajištění kybernetické bezpečnosti, a kontroluje jejich dodržování,
b) vydává metodické pokyny v jednotlivých oblastech činnosti Úřadu,
c) koordinuje problematiku kybernetické bezpečnosti s celostátní a mezinárodní působností,
d) poskytuje na vyžádání orgánů státu posudky a odborná vyjádření v rozsahu své působnosti,

e) zpracovává odborná vyjádření a stanoviska z oblasti kybernetické bezpečnosti a z vybraných oblastí ochrany utajovaných informací,
f) získává od orgánů státu, právnických osob a podnikajících fyzických osob potřebné informace v rozsahu nezbytném pro plnění úkolů ve své působnosti,
g) podílí se na procesu integrace České republiky do mezinárodních struktur z hlediska kybernetické bezpečnosti,
h) podílí se na provádění kontroly a provádí metodickou činnost ve vybraných oblastech ochrany utajovaných informací a vykonává kontrolu v oblasti kybernetické bezpečnosti,
i) vytváří celostátní koncepci státního dozoru a kontroly v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,
j) podílí se na mezinárodních a nadnárodních jednáních v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,
k) zajišťuje jako orgán krizového řízení připravenost Úřadu na řešení krizových situací ve své působnosti,
l) zpracovává návrhy prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu, které podle krizového zákona zasílá Ministerstvu vnitra,
m) určuje prvky kritické informační infrastruktury, které nespadají pod písmeno l), určuje provozovatele základní služby a informační systémy základní služby a stanoví významné informační systémy a jejich určující kritéria,
n) řeší v rozsahu stanoveném zákonem o kybernetické bezpečnosti a zákonem o ochraně utajovaných informací opravné prostředky proti rozhodnutím Úřadu a ředitele Úřadu,
o) rozhoduje o vydání nebo zrušení platnosti veřejné listiny a o vyhlášení, prodloužení nebo zrušení stavu kybernetického nebezpečí,
p) stanovuje zásady personální a fyzické bezpečnosti v oblasti kybernetické bezpečnosti a vybraných oblastech ochrany utajovaných informací,
q) zabezpečuje rozvoj kryptologie, řídí kryptografickou ochranu a ochranu před kybernetickými útoky,
r) zajišťuje a koordinuje výzkum a vývoj v oblasti kybernetické i informační bezpečnosti a ve vybraných oblastech ochrany utajovaných informací, v jejichž rámci zejména provádí základní a aplikovaný výzkum v oblasti kryptologie, vývoj národních kryptografických prostředků určených k zajištění kryptografické ochrany utajovaných informací, včetně vývoje prostředků pro výrobu klíčových materiálů,
s) zajišťuje výrobu a distribuci klíčových materiálů pro informační systémy a kryptografické prostředky používané pro ochranu utajovaných informací orgány státu, podnikateli a podnikajícími fyzickými osobami,
t) provádí certifikaci kryptografických prostředků určených k ochraně utajovaných informací, kryptografických pracovišť, stínicích komor, informačních systémů určených pro ochranu utajovaných informací a vede jejich seznam,
u) provádí ověřování způsobilosti elektrických a elektronických zařízení, stínící komory, jednací oblasti, zabezpečené oblasti nebo objektu před únikem utajované informace kompromitujícím vyzařováním,
v) schvaluje projekty bezpečnosti komunikačních systémů
w) nejpozději k 30. červnu zveřejňuje Výroční zprávu Úřadu za předcházející kalendářní rok,
x) vede zákonem o kybernetické bezpečnosti a zákonem o ochraně utajovaných informací stanovené evidence,
y) spravuje a provozuje Portál NÚKIB,

z) zpracovává a vládě České republiky vládě České republiky ke schválení předkládá národní strategii kybernetické a informační bezpečnosti a akční plán k jejímu naplňování a tuto strategii aktualizuje.

ČÁST DRUHÁ

ORGANIZACE A ŘÍZENÍ ÚŘADU

Čl. 4
Organizační členění

(1) Úřad se člení na organizační celky a samostatná pracovní místa.

(2) Organizační struktura Úřadu je uvedena v příloze č. 1 k této směrnici, která uvádí úplné členění organizačních celků a samostatných pracovních míst Úřadu, včetně jejich zkráceného označení uvedených v příloze č. 2.

Čl. 5
Stupně řízení

(1) Stupně řízení v Úřadu jsou

a) 4. stupeň řízení
- ředitel Úřadu,

b) 3. stupeň řízení
- náměstkové ředitele Úřadu,

c) 2. stupeň řízení
- ředitelé odborů,

d) 1. stupeň řízení,
- vedoucí oddělení,
- zástupce ředitele odboru Vládní CERT.

(2) Pro potřeby této směrnice se zavádí pojem „vedoucí zaměstnanec“ pro označení funkcí uvedených v odstavci 1.

(3) Vedoucí zaměstnanci, kteří jsou ředitelem Úřadu písemně pověřeni funkcí příkazce operace, se podílejí na zadávání veřejných zakázek.

Čl. 6
Ředitel Úřadu

(1) Ředitel Úřadu odpovídá za výkon působnosti stanovené Úřadu. Řídí Úřad a odpovídá za jeho činnost. Ředitel Úřadu je oprávněn svěřit určité pravomoci vedoucím zaměstnancům. Jedná a rozhoduje ve věcech spadajících do působnosti Úřadu. Ředitel Úřadu řídí činnost náměstků ředitele Úřadu (dále jen „náměstek ředitele“), hlavního poradce ředitele Úřadu, ředitele odboru Kabinet ředitele, ředitele odboru bezpečnosti, bezpečnostního ředitele, auditora kybernetické bezpečnosti a interního auditora.

(2) V případě nepřítomnosti ředitele Úřadu jej, v plném rozsahu jeho práv, povinností a odpovědnosti s výjimkou práv, povinností a odpovědnosti ve věcech svěřených zákonem výlučně do pravomocí ředitele Úřadu, a které si vyhradil, zastupuje statutární náměstek, označován též jako I. náměstek ředitele.

(3) Ředitel Úřadu zejména

a) rozhoduje o předkládání návrhů právních předpisů, mezinárodních smluv, návrhů rozpočtu kapitoly Úřadu a dalších návrhů zpracovávaných Úřadem a předkládaných příslušným orgánům státu,
b) předkládá jako správce kapitoly státního rozpočtu návrh rozpočtu Úřadu, návrh střednědobého rozpočtového výhledu Úřadu, návrh závěrečného účtu Úřadu,
c) rozhoduje o záležitostech, které jsou řediteli Úřadu vyhrazeny příslušnými právními předpisy,
d) rozhoduje o zásadních záležitostech patřících do působnosti Úřadu nebo o záležitostech, které si vyhradil k osobnímu rozhodování,
e) rozhoduje o hlavních úkolech Úřadu a ukládá zabezpečení úkolů stanovených vládou České republiky,
f) podílí se na tvorbě bezpečnostní politiky státu zejména prostřednictvím členství ve stálých pracovních orgánech Bezpečnostní rady státu,
g) zabezpečuje plnění úkolů Úřadu ve vztahu ke kontrolnímu orgánu Poslanecké sněmovny Parlamentu České republiky (dále jen „Poslanecká sněmovna“),
h) rozhoduje o dělbě působnosti v Úřadu a o organizační struktuře Úřadu,
i) stanovuje organizační strukturu a systemizaci pracovních míst v Úřadu,
j) schvaluje a vydává interní normativní akty Úřadu,
k) vystupuje za stát v pracovněprávních vztazích jako zaměstnavatel, rozhoduje o personálních záležitostech, jmenuje a odvolává vedoucí zaměstnance, bezpečnostního ředitele, manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, auditora kybernetické bezpečnosti a pověřuje určeného zaměstnance výkonem interního auditu,
l) jmenuje a odvolává členy svých poradních orgánů a zástupce Úřadu v mezinárodním styku,
m) stanoví složení delegací a udílí pokyny pro mezinárodní jednání, uděluje souhlas k zahraničním pracovním stykům podle zvláštních právních předpisů.

Čl. 7
Náměstek ředitele

(1) Náměstek ředitele je podřízen přímo řediteli Úřadu.

(2) Náměstek ředitele jedná jménem ředitele Úřadu ve věcech spadajících do působnosti sekce, kterou řídí, odpovídá řediteli Úřadu za její činnost a za plnění dalších úkolů s možností vyhradit si osobní rozhodnutí o věcech spadajících jinak do působnosti podřízeného organizačního celku.

(3) V případě nepřítomnosti náměstka ředitele Úřadu jej, v plném rozsahu jeho práv, povinností a odpovědnosti s výjimkou práv, povinností a odpovědnosti ve věcech svěřených zákonem výlučně do pravomocí náměstka ředitele, ve věcech personálních a ve věcech, které si vyhradil, se souhlasem ředitele Úřadu zastupuje určený ředitel odboru nebo jiný zaměstnanec přímo podřízený náměstkovi ředitele Úřadu.

(4) Náměstek ředitele zejména

a) podílí se na tvorbě koncepce bezpečnostní politiky státu,
b) řídí, organizuje a odpovídá za činnost řízené sekce,
c) zastupuje Úřad navenek při jednáních v rozsahu působnosti řízené sekce,
d) vydává v rámci jím řízené sekce pokyny a metodické návody nebo uzavírá prováděcí protokoly, pokud to vyplývá ze smluvního vztahu (jiného interního aktu řízení) a vede jejich evidenci,
e) rozhoduje ve věcech, které mu jsou jako vedoucímu zaměstnanci vyhrazeny příslušnými právními předpisy a interními normativními akty,

f) předkládá návrhy a stanoviska v personálních věcech týkajících se podřízených zaměstnanců, které řídí, a odpovídá za jejich řízení, kontrolu a hodnocení jejich pracovní výkonnosti a pracovních výsledků,
g) odpovídá za koordinaci práce uvnitř řízené sekce s činností ostatních organizačních celků Úřadu tak, aby byla zaručena jednotnost řízení a rozhodování v Úřadu,
h) navrhuje vnitřní organizaci a systemizaci pracovních míst řízené sekce,
i) řídí, organizuje, hodnotí a kontroluje činnost přímo podřízených zaměstnanců při plnění pracovních úkolů,
j) odpovídá za návrhy programů a koncepce rozvoje činnosti týkající se svěřené působnosti, které předkládá řediteli Úřadu,
k) zabezpečuje zpracování návrhů a stanovisek k návrhům právních předpisů, materiálům nelegislativní povahy a dalších pracovních podkladů, ke kterým se jím řízená sekce vyjadřuje, a odpovídá za věcné zpracovávání návrhů právních předpisů, materiálů nelegislativní povahy a dalších pracovních podkladů v působnosti řízené sekce,
l) plní další pracovní úkoly uložené ředitelem Úřadu.

Čl. 8
Ředitel odboru v přímé podřízenosti ředitele Úřadu

(1) Je podřízen přímo řediteli Úřadu.

(2) Ředitel odboru v přímé podřízenosti ředitele Úřadu jedná a rozhoduje ve věcech spadajících do předmětu činnosti jím řízeného odboru, odpovídá řediteli Úřadu za jeho činnost a za plnění dalších úkolů s možností vyhradit si osobní rozhodnutí o věcech spadajících jinak do působnosti podřízeného organizačního celku. Dále odpovídá za správnost plnění pracovních úkolů, tvorbu, zpracování, přípravu a předkládání materiálů, námětů, návrhů, koncepcí a stanovisek a dalších podkladů zpracovávaných odborem.

(3) V případě nepřítomnosti jej, v plném rozsahu jeho práv, povinností a odpovědnosti s výjimkou práv, povinností a odpovědnosti ve věcech svěřených zákonem výlučně do pravomocí ředitele odboru v přímé podřízenosti ředitele Úřadu, ve věcech personálních a ve věcech, které si vyhradil, se souhlasem ředitele Úřadu zastupuje určený vedoucí oddělení nebo určený zaměstnanec příslušného odboru.

(4) Ředitel odboru v přímé podřízenosti ředitele Úřadu

a) podílí se na tvorbě koncepce bezpečnostní politiky státu,
b) řídí, organizuje a odpovídá za činnost jím řízeného odboru,
c) zastupuje Úřad navenek při jednáních v rozsahu působnosti jím řízeného odboru,
d) vydává v rámci jím řízeného odboru pokyny a metodické návody nebo uzavírá prováděcí protokoly, pokud to vyplývá ze smluvního vztahu (jiného interního aktu řízení) a vede jejich evidenci,
e) rozhoduje ve věcech, které mu jsou jako vedoucímu zaměstnanci vyhrazeny příslušnými právními předpisy a interními normativními akty,
f) předkládá návrhy a stanoviska v personálních věcech týkajících se podřízených zaměstnanců, které řídí, a odpovídá za jejich řízení, kontrolu a hodnocení jejich pracovní výkonnosti a pracovních výsledků,
g) odpovídá za koordinaci práce uvnitř jím řízeného odboru s činností ostatních organizačních celků Úřadu tak, aby byla zaručena jednotnost řízení a rozhodování v Úřadu,
h) navrhuje vnitřní organizaci a systemizaci pracovních míst v jím řízeném odboru,
i) pečuje o zvyšování odborné úrovně zaměstnanců zařazených v jím řízeném odboru,

j) řídí, organizuje, hodnotí a kontroluje činnost podřízených zaměstnanců při plnění pracovních úkolů,
k) zpracovává návrhy programu a koncepce rozvoje činnosti a jiné materiály týkající se svěřené působnosti a předkládá je řediteli Úřadu,
l) projednává z rozhodnutí ředitele Úřadu s orgány veřejné moci nebo odbornou veřejností věcné otázky v rozsahu svěřené působnosti,
m) sleduje, soustřeďuje a vyhodnocuje poznatky týkající se činnosti jím řízeného odboru, zpracovává návrhy na rozvoj odboru a předkládá je řediteli Úřadu k rozhodnutí,
n) v rozsahu působnosti odboru se podílí na věcné přípravě právních předpisů a materiálů nelegislativní povahy a zajišťuje věcné zpracovávání návrhů interních aktů řízení,
o) plní další pracovní úkoly uložené ředitelem Úřadu.

Čl. 9
Ředitel odboru

(1) Ředitel odboru je přímo podřízen náměstkovi ředitele.

(2) Ředitel odboru jedná a rozhoduje ve věcech spadajících do předmětu činnosti jím řízeného odboru, pokud si rozhodování nevyhradil náměstek ředitele nebo ředitel Úřadu, odpovídá náměstkovi ředitele za správnost plnění pracovních úkolů, tvorbu, zpracování, přípravu a předkládání materiálů, námětů, návrhů, koncepcí a stanovisek a dalších podkladů zpracovávaných odborem.

(3) V případě nepřítomnosti ředitele odboru jej, v plném rozsahu jeho práv, povinností a odpovědnosti s výjimkou práv, povinností a odpovědnosti ve věcech svěřených zákonem výlučně do pravomocí ředitele odboru, ve věcech personálních a ve věcech, které si vyhradil, se souhlasem ředitele Úřadu zastupuje určený vedoucí oddělení nebo určený zaměstnanec příslušného odboru. V případě odboru Vládní CERT je ředitel odboru ve své nepřítomnosti zastoupen v kompletní oblasti věcné agendy zástupcem ředitele odboru Vládní CERT. V případě nepřítomnosti i zástupce ředitele odboru Vládní CERT je zastupujícím určen vedoucí oddělení nebo určený zaměstnanec příslušného odboru.

(4) Ředitel odboru zejména

a) řídí, organizuje a odpovídá za činnost řízeného odboru,
b) zastupuje v rozsahu svěřené pravomoci Úřad při jednáních s orgány veřejné moci nebo dalšími subjekty,
c) rozhoduje o záležitostech, které jsou mu jako vedoucímu zaměstnanci vyhrazeny příslušnými právními předpisy a interními akty řízení,
d) informuje podřízené zaměstnance o důležitých skutečnostech a podkladech potřebných pro jejich činnost,
e) koordinuje práci jím řízeného odboru s činností sekce, navrhuje náměstkovi ředitele formy a metody práce a vytváří potřebné podmínky pro plnění úkolů,
f) kontroluje kvalitu, včasnost a úplnost plnění úkolů, včetně dodržování právních předpisů a jiných opatření v jím řízeném odboru,
g) předkládá návrhy a stanoviska v personálních věcech týkajících se podřízených zaměstnanců, které řídí, a odpovídá za jejich řízení, kontrolu a hodnocení jejich pracovní výkonnosti a pracovních výsledků,
h) navrhuje vnitřní organizaci a systemizaci pracovních míst v jím řízeném odboru,
i) pečuje o zvyšování odborné úrovně zaměstnanců zařazených v jím řízeném odboru,

j) řídí, organizuje, hodnotí a kontroluje činnost podřízených zaměstnanců při plnění pracovních úkolů,
k) zpracovává návrhy programu a koncepce rozvoje činnosti a jiné materiály týkající se svěřené působnosti a předkládá je náměstkovi ředitele,
l) projednává z rozhodnutí náměstka ředitele s orgány veřejné moci nebo odbornou veřejností věcné otázky v rozsahu svěřené působnosti,
m) sleduje, soustřeďuje a vyhodnocuje poznatky týkající se činnosti jím řízeného odboru, zpracovává návrhy na rozvoj odboru a předkládá je náměstkovi ředitele k rozhodnutí,
n) v rozsahu působnosti odboru se podílí na věcné přípravě právních předpisů a materiálů nelegislativní povahy a zajišťuje věcné zpracovávání návrhů interních aktů řízení,
o) plní další pracovní úkoly uložené náměstkem ředitele nebo ředitelem Úřadu.

Čl. 10
Zástupce ředitele odboru Vládní CERT

(1) Zástupce ředitele odboru Vládní CERT je přímo podřízen řediteli odboru Vládní CERT.

(2) V přidělených oblastech věcné agendy přebírá odpovědnosti a pravomoci ředitele odboru a plně tak zodpovídá za dané činnosti. V případě nesouladu názorů mezi ředitelem odboru a zástupcem ředitele odboru rozhoduje ředitel odboru, i kdyby šlo o věcnou agendu přidělenou zástupci ředitele odboru.

Čl. 11
Vedoucí oddělení v přímé podřízenosti náměstka ředitele Úřadu

(1) Vedoucí oddělení v přímé podřízenosti příslušného náměstka ředitele jedná a rozhoduje ve věcech spadajících do předmětu činnosti jím řízeného oddělení, pokud si rozhodování nevyhradil náměstek ředitele nebo ředitel Úřadu, odpovídá náměstkovi řediteli za správnost plnění pracovních úkolů, tvorbu, zpracování, přípravu a předkládání materiálů, námětů, návrhů, koncepcí a stanovisek a dalších podkladů zpracovávaných oddělením, řídí a organizuje práci zaměstnanců jím řízeného oddělení.

(2) Vedoucí oddělení uvedení v odstavci 1 plní dále obdobné úkoly jako ředitel odboru podle čl. 8 odst. 4.

Čl. 12
Vedoucí oddělení

(1) Vedoucí oddělení jsou přímo podřízeni příslušnému řediteli odboru a jejich pravomoc a odpovědnost je odvozena z pravomoci a odpovědnosti ředitele odboru.

(2) Vedoucí oddělení zejména

a) stanovuje formy a způsoby realizace pracovních úkolů, jejichž plnění přísluší jím řízenému oddělení,
b) kontroluje činnost podřízených zaměstnanců při plnění úkolů oddělení,
c) vytváří potřebné podmínky pro účelné plnění úkolů podřízenými zaměstnanci, plní další pracovní úkoly uložené příslušným ředitelem odboru.

ČÁST TŘETÍ

ČLENĚNÍ A PŘEDMĚT ČINNOSTI ORGANIZAČNÍCH CELKŮ A SAMOSTATNÝCH PRACOVNÍCH MÍST ÚŘADU

HLAVA I.

ORGANIZAČNÍ CELKY A SAMOSTATNÁ PRACOVNÍ MÍSTA PODŘÍZENÁ ŘEDITELI ÚŘADU

Čl. 13
Interní auditor a kontrolor

(1) Interní auditor je organizačně a funkčně nezávislé samostatné pracovní místo s přímou podřízeností řediteli Úřadu.

Kontrolor je organizačně a funkčně nezávislé samostatné pracovní místo s přímou podřízeností řediteli Úřadu.

(2) Interní auditor zejména

a) objektivně a nezávisle přezkoumává a vyhodnocuje kvalitu vnitřního kontrolního systému a prováděných operací uvnitř Úřadu,
b) provádí zejména audity finanční, systémů a výkonu,
c) předkládá na základě svých zjištění řediteli Úřadu doporučení ke zdokonalování kvality vnitřního kontrolního systému, k předcházení nebo zmírnění rizik a k přijetí opatření k nápravě zjištěných nedostatků,
d) zajišťuje v Úřadu konzultační činnost pro oblast vnitřního kontrolního systému a řízení rizik,
e) zpracovává střednědobé a roční plány interního auditu,
f) zpracovává pro ředitele Úřadu roční zprávu o výsledcích interního auditu, která zejména hodnotí obecnou kvalitu vnitřního kontrolního systému, analyzuje závažné nedostatky, které nepříznivě ovlivnily činnost Úřadu, předkládá doporučení ke zkvalitnění vnitřního kontrolního systému a uvádí zjištění o skutečnostech, které by mohly způsobit neúplnost nebo neprůkaznost účetnictví,
g) zpracovává roční zprávu o výsledcích finančních kontrol, kterou předkládá Úřad jako správce rozpočtové kapitoly Ministerstvu financí,
h) informuje vedoucí zaměstnance o nové právní úpravě v oblasti finanční kontroly,
i) podílí se na tvorbě interních aktů řízení,
j) spolupracuje při provádění vnitřních kontrol uvnitř Úřadu,
k) plní další pracovní úkoly uložené ředitelem Úřadu.

(3) Kontrolor zejména

a) hodnotí a ověřuje skutečnosti rozhodné pro hospodaření s veřejnými prostředky, které jsou poskytovány Úřadem ve formě veřejné finanční podpory,
b) ověřuje, zda žadatel nebo příjemce veřejné finanční podpory dodržuje právní předpisy v přímé souvislosti s poskytovanou veřejnou finanční podporou a podmínky stanovené Úřadem jako poskytovatelem veřejné finanční podpory ve výzvě a v rozhodnutí / ve smlouvě o poskytnutí veřejné finanční podpory,
c) zpracovává roční plán veřejnosprávních kontrol,
d) vyhotovuje protokol o veřejnosprávní kontrole a zajišťuje, aby kontrolní zjištění byla objektivní, nestranná a podložená důkazy,

e) vyřizuje námitky kontrolované osoby proti kontrolním zjištěním uvedeným v protokole o veřejnosprávní kontrole,
f) zpracovává roční zprávu o výsledcích veřejnosprávních kontrol, kterou předkládá Úřad jako správce rozpočtové kapitoly Ministerstvu financí,
g) zajišťuje v Úřadu konzultační a metodickou činnost pro oblast veřejnosprávní kontroly,
h) podílí se na tvorbě interních aktů řízení,
i) provádí vnitřní kontroly uvnitř Úřadu v odborné koordinaci/spolupráci s interním auditorem,
j) zpracovává roční plán vnitřních kontrol uvnitř Úřadu,
k) zpracovává roční zprávu o výsledcích vnitřních kontrol uvnitř Úřadu,
l) plní další pracovní úkoly uložené ředitelem Úřadu.

Čl. 14
Bezpečnostní ředitel

(1) Bezpečnostní ředitel je organizačně a funkčně nezávislou rolí s přímou podřízeností řediteli Úřadu. Ředitel Úřadu jmenuje a odvolává bezpečnostního ředitele v souladu s příslušnými právními předpisy.

(2) Bezpečnostní ředitel zajišťuje plnění povinností vyplývajících z právních předpisů upravujících problematiku ochrany utajovaných informací.

(3) Bezpečnostní ředitel v oblasti bezpečnosti zajišťuje plnění povinností vyplývajících ze zákona a souvisejících vyhlášek.

(4) Role Bezpečnostního ředitele je v současném organizačním uspořádání Úřadu delegována na pozici ředitele odboru bezpečnosti.

Čl. 15
Manažer kritické infrastruktury

(1) Role manažera kritické infrastruktury je funkčně přímo podřízena řediteli Úřadu. Organizačně je začleněna do odboru bezpečnosti. Ředitel Úřadu jmenuje a odvolává manažera kritické infrastruktury v souladu s právními předpisy.
(2) Manažer kritické infrastruktury odpovídá za plnění povinností vyplývajících z právních předpisů upravujících problematiku odolnosti kritické infrastruktury.
(3) Manažer kritické infrastruktury zejména

a) Poskytuje součinnost Ministerstvu vnitra a ministerstvu nebo jinému ústřednímu správnímu úřadu při plnění povinností podle Zákona o odolnosti subjektů kritické infrastruktury a součinnost Evropské komisi při provádění poradní mise.
b) Podílí se na implementaci organizačních, technických a dalších opatření nezbytných pro ochranu kritické infrastruktury Úřadu a zajištění její odolnosti proti hrozbám
c) Odpovídá za plánování, efektivní vedení a rozhodování v oblasti krizového řízení Úřadu.

(4) Role Manažera kritické infrastruktury je v současném organizačním uspořádání Úřadu delegována na pracovní místo vedoucího oddělení personální bezpečnosti a krizového řízení Odboru bezpečnosti NÚKIB.

Čl. 16

Auditor kybernetické bezpečnosti

(1) Auditor kybernetické bezpečnosti je organizačně a funkčně nezávislým samostatným pracovním místem s přímou podřízeností řediteli Úřadu. Ředitel Úřadu jmenuje a odvolává auditora kybernetické bezpečnosti v souladu s právními předpisy.

(2) Auditor kybernetické bezpečnosti zajišťuje plnění povinností, které pro tuto bezpečnostní roli vyplývají z právních předpisů upravujících problematiku kybernetické bezpečnosti.

(3) Auditor kybernetické bezpečnosti zejména

a) objektivně a nezávisle přezkoumává a vyhodnocuje plnění požadavků plynoucích Úřadu z právních předpisů upravujících kybernetickou bezpečnost,
b) provádí zejména audity kybernetické bezpečnosti,
c) předkládá na základě svých zjištění řediteli Úřadu doporučení k předcházení nebo zmírnění rizik a k přijetí opatření k nápravě zjištěných nedostatků,
d) zajišťuje v Úřadu konzultační činnost pro oblast zajišťování kybernetické bezpečnosti,
e) zpracovává střednědobé a roční plány auditu kybernetické bezpečnosti,
f) pro ředitele Úřadu zpracovává roční zprávu o kvalitě zajištění kybernetické bezpečnosti Úřadu, výsledcích auditů kybernetické bezpečnosti a vyhodnocení rizik; součástí zprávy je analýza závažných nedostatků,
g) plní další pracovní úkoly uložené ředitelem Úřadu.

Čl. 17

Odbor Kabinet ředitele

(1) Odbor Kabinet ředitele (dále jen „kabinet“) se člení na

a) oddělení vládní agendy a legislativy,
b) oddělení komunikace a
c) pracovní skupinu sekretariátu ředitele.

(2) V čele kabinetu stojí ředitel kabinetu, který je vedoucím zaměstnancem 2. stupně řízení.

(3) Kabinet zejména

a) poskytuje řediteli Úřadu strategickou, právní, mediální a komunikační podporu,
b) zabezpečuje agendu ředitele Úřadu a asistuje při celkové koordinaci činností a řízení Úřadu v rozsahu jemu svěřeném ředitelem Úřadu,
c) komunikuje a jedná s orgány státní správy a dalšími partnery, včetně zahraničních, v rozsahu jemu svěřeném ředitelem Úřadu,
d) dohlíží na časový harmonogram ředitele Úřadu,
e) dohlíží na přípravu, plánování, organizaci a zabezpečení důležitých vnitrostátních a zahraničních cest ředitele Úřadu,
f) koordinuje spolupráci organizačních celků se subjekty soukromého sektoru a spravuje k tomu účelu informační databázi,
g) zajišťuje pro ředitele Úřadu podklady, přípravu a vede spisovou agendu týkající se účasti ředitele Úřadu na jednání Bezpečnostní rady státu a členství nebo účasti v jejích stálých výborech,

h) koordinuje činnost sekretariátu Výboru pro kybernetickou bezpečnost a zabezpečuje podklady k plnění role sekretariátu,
i) připravuje návrhy složitých systémů právních úprav s dopady na právní poměry České republiky a zabezpečuje přípravu a odpovídá za tvorbu návrhů koncepčně nových právních předpisů s celostátní působností nebo právních úprav věcí dosud zákony neupravených, zejména v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,
j) koordinuje a zabezpečuje ve spolupráci s věcnými gestory činnosti Úřadu v legislativní oblasti při přípravě, posuzování a projednání právních předpisů v rámci legislativního procesu,
k) koordinuje přípravu, posuzování a projednání nelegislativních materiálů předkládaných Úřadem vládě, Parlamentu České republiky, popřípadě dalším orgánům státu a při jejich přípravě poskytuje věcně příslušným organizačním celkům metodickou pomoc,
l) vede vládní agendu (zejména programy vlády, záznamy z jednání vlády, podklady pro Plán legislativních a nelegislativních prací vlády) a v součinnosti s ostatními organizačními celky Úřadu zajišťuje plnění úkolů vyplývajících z usnesení vlády,
m) zabezpečuje za Úřad vybrané právní výstupy a souhrnná stanoviska v legislativní oblasti,
n) zajišťuje komplexní posuzování systémů právních úprav nebo nových právních předpisů v připomínkovém řízení a po legislativní stránce odpovídá za toto posuzování jakožto i zpracování a koordinaci souhrnných stanovisek,
o) zajišťuje zpracování stanovisek Úřadu k návrhům nelegislativních materiálů předkládaných jinými ústředními správními úřady vládě nebo poradním orgánům vlády,
p) zajišťuje administraci vstupů a výstupů informačního systému pro aproximaci práva (ISAP),
q) zajišťuje administraci v systému e-Legislativa,
r) připravuje a implementuje komunikační strategii Úřadu,
s) podílí se na nastavování efektivní komunikace uvnitř Úřadu,
t) spolupracuje s partnerskými organizacemi v oblasti mediální komunikace,
u) spravuje hlavní účty Úřadu a ředitele Úřadu na sociálních sítích,
v) poskytuje podporu vedoucím zaměstnancům Úřadu v oblasti mediálních a jiných veřejných výstupů,
w) zabezpečuje spolupráci Úřadu ve vztahu k hromadným sdělovacím prostředkům a zajišťuje styk s veřejností, především prostřednictvím funkce tiskového mluvčího / tiskové mluvčí,
x) zajišťuje komunikaci s jinými komunikačními útvary státní správy a samosprávy,
y) podílí se na zajištění aktualizací internetových a intranetových stránek Úřadu, není-li pro konkrétní oblast stanoven jiný organizační celek, dle pokynu zveřejňuje důležitá sdělení a informace o činnosti Úřadu na internetových stránkách úřadu
z) publikuje oficiální stanoviska Úřadu ke všem záležitostem, týkajícím se působnosti Úřadu, ve vztahu k hromadným sdělovacím prostředkům, tiskovým agenturám a veřejnosti, pokud si tuto činnost nevyhradil ředitel Úřadu nebo tím nepověřil někoho jiného,
aa) poskytuje součinnost Oddělení personálních věcí a vzdělávání v navrhování a realizování vybraných komunikačních kampaní za účelem náboru a hledání nových talentů a spolupracuje při činnostech směřujících k rozvoji a stabilizování zaměstnanců,
bb) podílí se na tvorbě obsahu Portálu NÚKIB a komunikaci v Portálu NÚKIB,
cc) zajišťuje agendu překladů dokumentů trvalé hodnoty včetně právních předpisů z i do českého jazyka.

(4) Oddělení vládní agendy a legislativy plní úkoly uvedené v odstavci 3 písmeno g) až q).

(5) Oddělení komunikace plní úkoly uvedené v odstavci 3 písmeno r) až bb).

(6) Pracovní skupina sekretariát ředitele poskytuje podporu řediteli kabinetu při plnění úkolů uvedených v odstavci 3 písmeno b) až e).

Čl. 18
Odbor bezpečnosti

(1) Odbor bezpečnosti se člení na

a) oddělení spisové a archivní služby,
b) oddělení fyzické bezpečnosti,
c) oddělení informační bezpečnosti, v jehož rámci je ustavena pracovní skupina bezpečnostního dohledu,
d) oddělení personální bezpečnosti a krizového řízení,
e) samostatnou pozici Manažera kybernetické bezpečnosti a
f) samostatnou pozici Architekta kybernetické bezpečnosti.

(2) V čele odboru stojí ředitel odboru, který je vedoucím zaměstnancem 2. stupně řízení.

(3) Odbor bezpečnosti zejména

a) zajišťuje činnosti spisovny a podatelny Úřadu, registru utajovaných informací,
b) podílí se na přípravě dokumentů v oblasti ochrany utajovaných informací v Úřadu,
c) eviduje utajované informace poskytované Úřadu v rámci mezinárodní spolupráce,
d) zpracovává a vede aktuální seznam osob, které mají přístup k utajovaným informacím NATO a EU a ostatních subjektů cizí moci,
e) zpracovává návrh skartačního plánu Úřadu a dohlíží na jeho plnění,
f) provádí skartace národních utajovaných a neutajovaných dokumentů a dokumentů registru utajovaných informací,
g) dohlíží na ukládání dokumentů Úřadu,
h) zajišťuje v rozsahu stanoveném bezpečnostním ředitelem ochranu utajovaných informací v Úřadu,
i) provádí kontrolu a metodicky řídí spisovou službu Úřadu,
j) provádí v rámci Úřadu kontrolu dodržování ochrany utajovaných informací,
k) zpracovává a vede evidenci případů neoprávněného nakládání s utajovanými informacemi v Úřadu a další evidence stanovené zákonem,
l) zajišťuje činnost bezpečnostního archivu a specializovaného archivu,
m) podílí se na tvorbě projektů fyzické bezpečnosti a vyjadřuje se k bezpečnostní a projektové dokumentaci při rekonstrukčních a stavebních realizací objektů Úřadu,
n) spolupracuje v součinnosti s osobou pověřenou plněním úkolů na úseku požární ochrany,
o) řídí a zabezpečuje činnosti při mimořádných bezpečnostních událostech,
p) spolupracuje s ochrannou službou Policie České republiky při výkonu ochrany objektů Úřadu,
q) vede evidenci a správu generálních a koncových klíčů od všech místností a vchodů v objektech Úřadu,
r) dohlíží na funkčnost bezpečnostních systémů a přístupových prvků Úřadu,
s) provádí na vyžádání vedoucího zaměstnance detekční kontrolu, zda zaměstnanec není na pracovišti pod vlivem alkoholických nápojů,
t) zpracovává ve spolupráci s oddělením personálních věcí a vzdělávání přehled pracovních míst nebo funkcí v Úřadu, na kterých je nezbytné mít přístup k utajovaným informacím,
u) zpracování personálního projektu Úřadu (§ 72 zákona o ochraně utajovaných informací),
v) zajišťuje a v rozsahu stanoveném zákonem a interními akty provádí činnosti na úseku personální bezpečnosti,

w) zpracovává a vede evidenci poučených osob – zaměstnanců Úřadu,
x) sleduje, zda poučené osoby – zaměstnanci Úřadu – splňují podmínky stanovené zákonem,
y) zajišťuje odborné školení v oblasti ochrany utajovaných informací,
z) odpovídá za plnění úkolů Úřadu v oblasti boje proti korupci; zabezpečuje implementaci státní protikorupční strategie do Interního protikorupčního programu Úřadu,
aa) zřizuje pracoviště krizového řízení,
bb) zajišťuje aktualizaci Statutu a Jednacího řádu Krizového štábu Úřadu včetně z nich plynoucích úkolů k zajištění činnosti Krizového štábu Úřadu,
cc) vytváří koncepci přípravy ke krizovému řízení státu v působnosti Úřadu a zajišťuje připravenost Úřadu na řešení krizových situací ve spolupráci s ostatními organizačními celky Úřadu,
dd) reaguje na aktuální krizové stavy; zprostředkovává komunikaci s Ústředním krizovým štábem a s pracovišti krizového řízení jiných resortů; podílí se na tvorbě a připomínkování vznikající legislativy v oblasti krizového řízení na mezirezortní úrovni; účastní se pravidelných mezirezortních iniciativ a akcí v oblasti krizového řízení (Výbor pro civilní a nouzové plánování); podílí se na vypracování periodických reportů (pro Evropský systém reakce na krize – IPCR),
ee) provádí aktualizaci Krizového plánu Úřadu, Dílčího plánu obrany Úřadu a Plánu krizové připravenosti subjektu kritické infrastruktury Úřadu, a to pod metodickým dohledem Generálního ředitelství Hasičského záchranného sboru (GŘ HZS) a Krajských vojenských velitelství (KKV) se sídly v Praze a Brně,
ff) provádí administraci a obsluhu elektronického účtu Úřadu v Národním systému reakce na krize (dále jen „NSRK“); nastavuje uživatelská práva v NSRK dle prioritních požadavků NCKB a SSAS; přijímá hlášení o krizových stavech prostřednictví účtu NSRK od orgánů krizového řízení NATO a zajišťuje jejich distribuci krizovému štábu Úřadu,
gg) spolupracuje s organizačními celky Úřadu na zajištění připravenosti Úřadu k řešení krizových situací,
hh) vykonává bezpečnostní správu informačních a komunikačních systémů nakládajících s utajovanými informacemi Úřadu, vede jejich dokumentaci a evidenci dle příslušných právních předpisů,
ii) spolupracuje s odborem informačních technologií a poskytuje metodickou podporu lokálním provozním bezpečnostním správcům,
jj) zajišťuje plánování a rozvoj informačních a komunikačních systémů Úřadu nakládajících s utajovanými informacemi,
kk) ověřuje podmínky pro provoz a soulad s požadavky na certifikaci informačních systémů nakládajících s utajovanými informacemi,
ll) vykonává metodickou a kontrolní činnost a správu bezpečnosti informačních systémů třetích stran pro nakládání s utajovanými informacemi,
mm) provádí evidenci a označování nosičů informací používaných v provozu informačních a komunikačních systémů nakládajících s utajovanými informacemi,
nn) vykonává bezpečnostní dohled nad informačními systémy v rozsahu ISMS Úřadu a ve vnitřním informačním systému pro nakládání s utajovanými informacemi,
oo) spolupracuje s manažerem a architektem kybernetické bezpečnosti, kterým poskytuje součinnost v oblasti kybernetické bezpečnosti, zejména při evidenci aktiv, provádění rozsáhlejších analýz rizik a plnění dalších úkolů,
pp) plní další pracovní úkoly uložené ředitelem Úřadu.

(4) Oddělení spisové a archivní služby plní úkoly uvedené v odstavci 3 písmeno a) až l).

(5) Oddělení fyzické bezpečnosti plní úkoly uvedené v odstavci 3 písmeno m) až s).

(6) Oddělení personální bezpečnosti a krizového řízení plní úkoly uvedené v odstavci 3 písmeno t) až gg).

(7) Oddělení informační bezpečnosti plní úkoly uvedené v odstavci 3 písmeno hh) až oo).

(8) Pracovní skupina bezpečnostního dohledu plní úkoly uvedené v odstavci 3 písmeno nn) až oo) a další úkoly stanovené vedoucím oddělení informační bezpečnosti v odstavci 3 písmeno hh) až mm).

Čl. 19
Manažer kybernetické bezpečnosti

(1) Manažer kybernetické bezpečnosti je organizačně a funkčně nezávislou samostatnou rolí s přímou podřízeností řediteli odboru bezpečnosti. Ředitel Úřadu jmenuje a odvolává manažera kybernetické bezpečnosti v souladu s právními předpisy.

(2) Manažer kybernetické bezpečnosti odpovídá za plnění povinností, vyplývajících z právních předpisů upravujících problematiku kybernetické bezpečnosti.

(3) Role Manažera kybernetické bezpečnosti je v současné organizační struktuře Úřadu sloučena s pracovní pozicí Manažera kybernetické bezpečnosti v rámci odboru bezpečnosti.

(4) Manažer kybernetické bezpečnosti vykonává funkci tajemníka Výboru pro řízení kybernetické bezpečnosti Úřadu.

(5) Manažer kybernetické bezpečnosti zejména

a) odpovídá za plnění povinností, vyplývajících z právních předpisů upravujících problematiku kybernetické bezpečnosti podle zákona o kybernetické bezpečnosti,
b) odpovídá za správu systému řízení bezpečnosti informací (ISMS) Úřadu,
c) odpovídá za tvorbu a prosazování pravidel, standardů a norem pro zajištění kybernetické bezpečnosti komunikačních a informačních systémů ve vnitřní působnosti úřadu a kontrolu jejich dodržování,
d) ukládá k realizaci opatření v oblasti kybernetické bezpečnosti,
e) posuzuje, vyhodnocuje, eviduje a schvaluje výjimky z pravidel, standardů a norem pro zajištění informační a kybernetické bezpečnosti,
f) podílí se na zpracování koncepce a strategie rozvoje komunikačních a informačních systémů Úřadu v oblasti kybernetické bezpečnosti,
g) koordinuje řízení bezpečnostních událostí a incidentů u Úřadu, vede jejich evidenci a provádí hodnocení řešení,
h) spolupracuje s architektem kybernetické bezpečnosti na rozvoji ISMS Úřadu,
i) spolupracuje s odborem informatiky v rámci návrhu a implementace technických opatření k zajištění kybernetické bezpečnosti,
j) spolupracuje s ostatními organizačními celky Úřadu při implementaci opatření bezpečnostních politik, hodnocení informačních aktiv a řízení kybernetických rizik,
k) schvaluje provádění bezpečnostních testů a analýz v oblasti kybernetické bezpečnosti, posuzuje a schvaluje vyhodnocení nálezů a návrhů protiopatření a podílí se na kontrole jejich realizace,
l) odpovídá za kontroly opatření v oblasti kybernetické a informační bezpečnosti,
m) odpovídá za soulad informačních systémů KII a VIS Úřadu se zákonem o kybernetické bezpečnosti,
n) stanovuje plán bezpečnostního povědomí zaměstnanců Úřadu v oblasti kybernetické bezpečnosti, spolupracuje s oddělením personálních věcí a vzdělávání,

o) řídí rizika v oblasti informační a kybernetické bezpečnosti,
p) poskytuje odborné konzultace a spolupracuje v oblasti kybernetické bezpečnosti rovněž v rámci rozvoje a správy informačních a komunikačních systémů nakládajících s utajovanými informacemi.

Čl. 20
Architekt kybernetické bezpečnosti

(1) Architekt kybernetické bezpečnosti je organizačně a funkčně nezávislou samostatnou pracovní rolí s přímou podřízeností řediteli odboru bezpečnosti. Ředitel Úřadu jmenuje a odvolává architekta kybernetické bezpečnosti v souladu s právními předpisy.

(2) Architekt kybernetické bezpečnosti zajišťuje plnění povinností, které pro tuto bezpečnostní roli vyplývají z právních předpisů upravujících problematiku kybernetické bezpečnosti.

(3) Role Architekta kybernetické bezpečnosti je v současné organizační struktuře Úřadu sloučena s pracovní pozicí Architekta kybernetické bezpečnosti v rámci odboru bezpečnosti.

(4) Architekt kybernetické bezpečnosti je členem Výboru pro řízení kybernetické bezpečnosti Úřadu.

(5) Architekt kybernetické bezpečnosti zejména

a) odpovídá za vrstvu kybernetické bezpečnosti v rámci enterprise architektury,
b) odpovídá za tvorbu, udržování modelu podnikové architektury kybernetické bezpečnosti,
c) spolupracuje s odborem informačních technologií na způsobu a plánu implementace kybernetické bezpečnosti do podnikové architektury,
d) schvaluje již ve fázi plánování zavádění a změny bezpečnostních mechanismů a prvků, kontroluje a schvaluje implementaci nových informačních a komunikačních systémů do podnikové architektury,
e) odpovídá za tvorbu a prosazování procesů, pravidel a politik pro zajištění kybernetické bezpečnosti komunikačních a informačních systémů ve vnitřní působnosti Úřadu a kontrolu jejich dodržování,
f) spolupracuje s manažerem kybernetické bezpečnosti při správě ISMS, bezpečnostních testech, kontrole opatření a řízení kybernetických bezpečnostních incidentů a událostí,
g) spolupracuje s odbornými organizačními celky Úřadu při formulaci požadavků na architekturu implementovaných informačních systémů s ohledem na kybernetickou bezpečnost nebo v rámci změnového řízení u stávajících IS,
h) spolupracuje s ostatními organizačními celky Úřadu při implementaci opatření kybernetických bezpečnostních politik, hodnocení informačních aktiv a řízení kybernetických rizik,
i) podílí se na zajištění souladu informačních systémů KII a VIS NUKIB se zákonem o kybernetické bezpečnosti,
j) odpovídá za návrh užití vhodného metodického rámce pro řízení kybernetické bezpečnosti Úřadu, popřípadě jeho částí včetně akceptace,
k) podílí se na pravidelném plánování v souladu se strategickými cíli Úřadu a na aktualizaci strategie kybernetické bezpečnosti,
l) provádí vyhodnocení implementace modelu podnikové architektury kybernetické bezpečnosti dle stanovených metrik,
m) poskytuje odborné konzultace a spolupracuje v oblasti kybernetické bezpečnosti rovněž v rámci rozvoje a správy informačních a komunikačních systémů nakládajícími s utajovanými informacemi.

HLAVA II.

ORGANIZAČNÍ CELKY PODŘÍZENÉ NÁMĚSTKOVI ŘEDITELE ÚŘADU POVĚŘENÉMU ŘÍZENÍM SEKCE NÁRODNÍHO CENTRA KYBERNETICKÉ BEZPEČNOSTI

Čl. 21
Sekce Národního centra kybernetické bezpečnosti

(1) Sekce Národního centra kybernetické bezpečnosti se člení na
a) odbor vládní CERT (GovCERT.CZ),
b) odbor regulace,
c) odbor kontroly,
d) oddělení DevSecOps, jehož součástí je pracovní skupina pro rozvoj a správu Portálu NÚKIB a pracovní skupina aplikační bezpečnosti.

(2) V čele sekce Národního centra kybernetické bezpečnosti stojí náměstek ředitele pověřený řízením této sekce, který je vedoucím zaměstnancem 3. stupně řízení.

(3) Dalšími vedoucími zaměstnanci sekce Národního centra kybernetické bezpečnosti jsou

a) ředitel odboru vládní CERT,
b) ředitel odboru regulace,
c) ředitel odboru kontroly,

kteří jsou vedoucími zaměstnanci 2. stupně řízení,

d) zástupce ředitele odboru Vládní CERT,
e) vedoucí oddělení DevSecOps,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(4) Sekce Národního centra kybernetické bezpečnosti zejména

a) provozuje činnost Národního centra kybernetické bezpečnosti, zejména odboru vládního CERT,
b) zajišťuje prevenci před kybernetickými hrozbami proti poskytovatelům regulovaných služeb a vybraným informačním systémům veřejné správy,
c) podílí se na koordinaci a řešení kybernetických bezpečnostních incidentů u poskytovatelů regulovaných služeb, osvětové a vzdělávací činnosti v oblasti své působnosti,
d) spolupracuje s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru,
e) účastní se kybernetických cvičeních na národní a mezinárodní úrovni,
f) zajišťuje koordinaci identifikace a registrace orgánů a osob spadajících do působnosti zákona o kybernetické bezpečnosti, které nejsou určovány aktem Úřadu,
g) určuje orgány a osoby spadající do působnosti zákona o kybernetické bezpečnosti,
h) plní úkoly svěřené Úřadu v oblasti regulace cloud computingu ve veřejné správě,
i) vykonává činnost Vnitrostátního orgánu certifikace kybernetické bezpečnosti (NCCA),
j) vykonává kontrolu v oblasti kybernetické bezpečnosti,
k) zastupuje ve spolupráci s Odborem mezinárodní spolupráce a Evropské unie Českou republiku v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti,
l) podílí se v rozsahu své působnosti na bezpečnostní politice Úřadu, spolupráci na mezinárodní úrovni a plnění mezinárodních závazků vyplývajících z členství České republiky v NATO

a členství v EU a členství v jiných mezinárodních organizacích, a to za součinnosti a informování Odboru mezinárodní spolupráce a Evropské unie,
m) zajišťuje rozvoj a provoz Portálu NÚKIB,
n) připravuje vydání protiopatření podle zákona o kybernetické bezpečnosti,
o) zajišťuje výkon agendy v oblasti bezpečnosti dodavatelského řetězce,
p) připravuje věcný obsah legislativy v oblasti kybernetické bezpečnosti,
q) podílí se na krizovém plánování a řízení v oblasti kybernetické bezpečnosti na úrovni státu,
r) plní další úkoly a povinnosti stanovené ředitelem Úřadu v rozsahu právních předpisů v oblasti kybernetické bezpečnosti.

Čl. 22
Odbor vládní CERT

(1) Odbor vládní CERT, v jehož čele stojí ředitel odboru a zástupce ředitele odboru pro určené oblasti věcné agendy, se dále člení na

a) oddělení Incident Handling,
b) oddělení analýzy kybernetických incidentů, jehož součástí je pracovní skupina Threat Hunting,
c) oddělení penetračního testování, jehož součástí je pracovní skupina testování síťových služeb, zranitelností a operačních technologií,
d) pracovní skupinu Threat Intelligence and Information Sharing,

(2) Dalšími vedoucími zaměstnanci odboru vládní CERT jsou

a) vedoucí oddělení Incident Handling,
b) vedoucí oddělení analýzy kybernetických incidentů,
c) vedoucí oddělení penetračního testování,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor vládní CERT zejména
a) podílí se na vývoji, naplňování a vyhodnocování strategií a politik,
b) poskytuje metodickou pomoc, nástroje a rady pro zvyšování účinnosti bezpečnostních opatření zaváděných u správců a provozovatelů informačních a komunikačních systémů spadajících do působnosti zákona o kybernetické bezpečnosti,
c) informuje poskytovatele regulované služby dle zákona o kybernetické bezpečnosti, orgány státní správy a další partnery o nových hrozbách a aktuálních trendech v kybernetické bezpečnosti,
d) analyzuje a vyhodnocuje informace z otevřených i neveřejných zdrojů potřebných pro analýzu nových hrozeb a aktuálních trendů,
e) podílí se na zajišťování výzkumu a vývoje v oblasti kybernetické bezpečnosti,
f) účastní se cvičení kybernetické bezpečnosti na národní i mezinárodní úrovni, dle volných kapacit poskytuje odboru cvičení a vzdělávání konzultace ke cvičením kybernetické bezpečnosti,
g) vykonává publikační a přednáškovou činnost,
h) poskytuje součinnost odboru kontroly podle zákona o kybernetické bezpečnosti,
i) ve spolupráci s oddělením DevSecOps navrhují procesy pro agendy vládního CERT, které jsou realizované prostřednictvím Portálu NÚKIB,

j) přijímá hlášení o kybernetických bezpečnostních událostech a incidentech, vede jejich evidenci,
k) udržuje pohotovostní linku pro příjem hlášení kybernetických bezpečnostních událostí a incidentů,
l) identifikuje a analyzuje kybernetické bezpečnostní události a incidenty a navrhuje a koordinuje postupy k minimalizaci jejich dopadů,
m) v rámci vyšetřování KBI provádí forenzní analýzu dodaných dat (zejména stanic, serverů, obrazů disku i paměti nebo vzorků malware, a také forenzní analýzu v síťových lozích),
n) provozuje forenzní laboratoř pro potřeby analýzy kybernetických bezpečnostních událostí a incidentů, a to i pro prostředí klasifikovaných systémů,
o) provádí bezpečnostní testování zejména u poskytovatelů regulované služby dle zákona o kybernetické bezpečnosti což zahrnuje na základě smluvní dohody reálnou simulaci pokusu o kompromitaci IT a OT systémů, dále provádění sociálního inženýrství včetně kontroly fyzického zabezpečení a následné hodnocení úrovně zabezpečení, provádí konzultace k provedeným testům,
p) provádí testování webových aplikací,
q) provádí proaktivní neintruzivní skenování sítí a informačních systémů regulovaných subjektů s cílem odhalit zranitelnosti s potenciálním významným dopadem. U subjektů, které o to výslovně požádají, může být skenování doplněno o pokročilejší formu testování zahrnující i aktivní ověřování identifikovaných zranitelností,
r) poskytuje součinnost pro odbor kontroly, kdy skenování zranitelností slouží jako podklad pro provedení kontroly,
s) spolupracuje s partnery na národní i mezinárodní úrovni, kteří se podílejí na zajišťování bezpečnosti kybernetického prostoru,
t) sdílí s partnery na národní i mezinárodní úrovni informace dle zákona o kybernetické bezpečnosti a dle dalších relevantních právních předpisů,
u) administruje CERT tým v rámci kooperačních skupin a komunitních programů, do kterých je Vládní CERT zapojen,
v) průběžně monitoruje a vyhodnocuje kybernetické bezpečnostní hrozby a trendy v této oblasti,
w) podílí se na rozvoji a implementaci pokročilé analytické kapacity CTI (Cyber Threat Intelligence) (ve spolupráci s odborem centrální analytiky),
x) provádí proaktivní i reaktivní vyhledávání známek útočníka, a udržuje k tomu potřebné nástroje a infrastrukturu,
y) provádí testování operačních systémů, síťových služeb a infrastruktury,
z) vyhledává informace o nových zranitelnostech, přijímá a zpracovává hlášení o zranitelnostech v oblasti kybernetické bezpečnosti,
aa) zabezpečuje a řeší problematiku bezpečnosti operačních technologií, za tímto účelem pak provozuje SCADA laboratoř a OT polygon.

(4) Oddělení Incident Handling plní zejména úkoly uvedené v odstavci 3 písm. j) až l).
(5) Oddělení analýzy kybernetických incidentů plní zejména úkoly uvedené v odstavci 3 písm. m) až n).
(6) Oddělení penetračního testování plní zejména úkoly uvedené v odstavci 3 písm. o) až r).
(7) Pracovní skupina Threat Intelligence & Information Sharing plní zejména úkoly uvedené v odstavci 3 písm. s) až w).
(8) Pracovní skupina Threat Hunting plní zejména úkoly uvedené v odstavci 3 písm. x).
(9) Pracovní skupina testování síťových služeb, zranitelností a operačních technologií plní zejména úkoly uvedené v odstavci 3 písm. y) až aa).

(10) Všechna oddělení a pracovní skupiny odboru vládní CERT se podílejí na plnění úkolů uvedených v odstavci 3 písm. a) až i).

Čl. 23
Oddělení DevSecOps

(1) V čele oddělení DevSecOps stojí vedoucí oddělení.

(2) Oddělení DevSecOps zejména

(a) vyvíjí, spravuje a provozuje Portál NÚKIB,
(b) vyvíjí, spravuje a provozuje informační systémy pro evidenci regulovaných služeb, osob poskytovaní služeb registrace doménových jmen, kybernetických bezpečnostních incidentů, dodavatelů bezpečnostně významných dodávek a koordinovaného zveřejňování zranitelností,
(c) zajišťuje rozvoj, zabezpečení, monitoring a provoz virtuální infrastruktury pro spravované systémy
(d) zajišťuje správu obsahu a jednotnou strukturu Portálu NÚKIB,
(e) ve spolupráci s ostatními organizačními celky úřadu koordinuje a realizuje komunikační strategii k Portálu,
(f) v rozsahu oblasti DevSecOps poskytuje součinnost vládnímu CERT pro plnění jeho úkolů,
(g) za součinnosti Odboru Informačních technologií zajišťuje vývoj, běh a rozvoj podpůrných a agendových aplikací pro odbor Vládní CERT,
(h) podílí se na udržování pohotovostní linky pro příjem hlášení kybernetických bezpečnostních událostí a incidentů ve spolupráci s vládním CERT,
(i) podílí se na vývoji, naplňování a vyhodnocování strategií a politik,
(j) poskytuje odboru Vládní CERT součinnost s koordinací a řešením kybernetických bezpečnostních událostí a incidentů,
(k) spolupracuje s partnery na národní i mezinárodní úrovni, a to z veřejného i soukromého sektoru, kteří se podílejí na zajišťování bezpečnosti kybernetického prostoru,
(l) účastní se cvičení kybernetické bezpečnosti na národní i mezinárodní úrovni, dle volných kapacit poskytuje odboru cvičení a vzdělávání součinnost a konzultace ke cvičením kybernetické bezpečnosti,
(m) vykonává publikační a přednáškovou činnost,
(n) poskytuje součinnost odboru kontroly podle zákona o kybernetické bezpečnosti,
(o) zajišťuje poskytování konzultací k hodnocení služeb cloud computingu,
(p) podílí se na zajišťování výzkumu a vývoje v oblasti kybernetické bezpečnosti,

(3) Všechny pracovní skupiny oddělení DevSecOps se podílejí na plnění úkolů uvedených v odstavci 2 písm. h), i), j), k), l), m), n).
(4) Pracovní skupina pro rozvoj a správu Portálu NÚKIB plní zejména úkoly uvedené v odstavci 2 písm. a), b).
(5) Pracovní skupina aplikační bezpečnosti plní zejména úkoly uvedené v odstavci 2 písm. a spolupracuje s vládním CERT na úkolech uvedených ve čl. 22 odstavci 3 písm. b), l), z).

Čl. 24
Odbor regulace

(1) Odbor regulace, v jehož čele stojí ředitel odboru, se dále člení na

a) oddělení regulace veřejného sektoru,
b) oddělení regulace soukromého sektoru,
c) oddělení regulace dodavatelů informačních technologií,
d) pracovní skupinu evropských certifikací,
e) pracovní skupina bezpečnosti dodavatelského řetězce,
f) pracovní skupinu registrace, evidence a podpory.

(2) Dalšími vedoucími zaměstnanci odboru regulace jsou

a) vedoucí oddělení regulace veřejného sektoru,
b) vedoucí oddělení regulace soukromého sektoru a
c) vedoucí oddělení regulace dodavatelů informačních technologií,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor regulace zejména:

Oblast ZKB

Podoblast poskytovatel regulované služby

a) zajišťuje výklad a aplikaci zákona o kybernetické bezpečnosti, pokud není část této agendy svěřena jinému organizačnímu celku,
b) vede správní řízení o registraci, změně nebo zrušení registrace poskytovatelů regulované služby podle § 6 zákona o kybernetické bezpečnosti a za tímto účelem v případě potřeby analyzuje regulovaná odvětví a služby, prověřuje splnění podmínek pro registraci podle § 3 až § 5 zákona o kybernetické bezpečnosti a provádí další úkony s tím spojené,
c) zajišťuje přijímání a zpracování údajů hlášených poskytovatelem regulované služby podle § 11 zákona o kybernetické bezpečnosti,
d) vede správní řízení o uložení povinnosti podle § 19 odst. 1 zákona o kybernetické bezpečnosti,
e) vede správní řízení o vydání, změně nebo zrušení výstrahy podle § 21 zákona o kybernetické bezpečnosti,
f) vede správní řízení o vydání, změně nebo zrušení varování podle § 22 zákona o kybernetické bezpečnosti,
g) vede správní řízení o vydání, změně nebo zrušení reaktivního protiopatření podle § 23 zákona o kybernetické bezpečnosti a v návaznosti na to přijímá oznámení o provedení reaktivního protiopatření,
h) vede správní řízení o uložení, změně nebo zrušení povinnosti dodavatele předat poskytovateli regulované služby informace a data související s provozem aktiv sloužících k poskytování regulované služby podle § 24 zákona o kybernetické bezpečnosti,

Podoblast strategicky významná služba

i) vede správní řízení o registraci, změně nebo zrušení registrace strategicky významné služby podle § 25 a § 26 zákona o kybernetické bezpečnosti a za tímto účelem v případě potřeby analyzuje regulovaná odvětví a strategicky významné služby a provádí další úkony s tím spojené,

j) přijímá informace o dodavatelích bezpečnostně významných dodávek podle § 31 zákona o kybernetické bezpečnosti,
k) koordinuje interní procesy Úřadu nutné pro zajištění mechanismu prověřování bezpečnosti dodavatelského řetězce podle § 27 až § 32 zákona o kybernetické bezpečnosti,
l) koordinuje externí procesy nutné pro zajištění mechanismu prověřování bezpečnosti dodavatelského řetězce podle § 27 až § 32 zákona o kybernetické bezpečnosti, (doplnit prosím)
m) vede správní řízení o vydání, změně nebo zrušení opatření obecné povahy, kterým Úřad stanoví poskytovatelům strategicky významných služeb podmínky nebo zakáže využití plnění dodavatele podle § 29 zákona o kybernetické bezpečnosti,
n) zajišťuje interpretaci ustanovení zajištění dostupnosti strategicky významných služeb podle § 33 zákona o kybernetické bezpečnosti,

Podoblast ostatní procesy ze zákona

o) přijímá hlášení údajů osob poskytujících služby registrace doménových jmen podle § 34 zákona o kybernetické bezpečnosti a zajišťuje aplikaci ustanovení § 35 zákona o kybernetické bezpečnosti,
p) zajišťuje interpretaci ustanovení o výjimce z práva na informace podle § 36 zákona o kybernetické bezpečnosti,
q) poskytuje řediteli Úřadu podklady a informace související s vyhlášením stavu kybernetického nebezpečí podle § 38 zákona o kybernetickém nebezpečí, vydáním opatření za stavu kybernetického nebezpečí podle § 39 zákona o kybernetické bezpečnosti a účinkem těchto opatření, dále poskytuje podklady a informace související s přechodem stavu kybernetického nebezpečí do nouzového stavu,
r) vede některé evidence podle § 46 zákona o kybernetické bezpečnosti, konkrétně evidenci regulovaných služeb včetně jejich poskytovatelů a jimi hlášených údajů, evidenci osob poskytujících služby registrace doménových jmen a jimi hlášených údajů a evidenci dodavatelů bezpečnostně významných dodávek,
s) Vytváří exporty a přehledy z těchto evidencí a předává je na základě požadavku relevantním celkům Úřadu a externím partnerům na základě předávacího protokolu

Oblast cloud

t) plní úkoly svěřené Úřadu v oblasti regulace cloud computingu ve veřejné správě, především vydává stanoviska spojená s posuzováním poskytovatelů a nabídek cloud computingu, pokud není část této agendy svěřena jinému organizačnímu celku,

Oblast certifikace

u) plní povinnosti svěřené Úřadu vyplývající z jeho role jako vnitrostátního orgánu certifikace kybernetické bezpečnosti podle nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) podle § 42 odst. 4 písm. j) zákona o kybernetické bezpečnosti, a to zejména prostřednictvím
    i. plnění povinností podle článku 58 aktu o kybernetické bezpečnosti,
    ii. aktivní účasti v procesu vzájemného hodnocení podle článku 59 aktu o kybernetické bezpečnosti,

iii. vedení řízení o autorizaci subjektů posuzování shody v případech stanovených v článku 60 aktu o kybernetické bezpečnosti,
iv. provádění oznámení akreditovaných, případně autorizovaných, subjektů posuzování shody podle článku 61 aktu o kybernetické bezpečnosti,
v. aktivní účasti na jednáních Evropské skupiny pro certifikaci kybernetické bezpečnosti podle článku 62 aktu o kybernetické bezpečnosti a
vi. vyřizování stížností podaných podle článku 63 aktu o kybernetické bezpečnosti,

v) plní povinnosti vyplývající z dohod uzavřených s Českým institutem pro akreditaci, o.p.s.,
w) účastní se výměny informací s vnitrostátními orgány certifikace kybernetické bezpečnosti a vnitrostátními akreditačními orgány ostatních členských států Evropské unie,
x) vykonává roli oznamujícího orgánu podle nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (“akt o kybernetické odolnosti”), a to zejména prostřednictvím
i. zavádění postupů podle mj. kapitoly IV aktu o kybernetické odolnosti,
ii. spolupráce s dalšími organizačními celky NÚKIB a relevantními orgány veřejné správy, zejména Ministerstvem průmyslu a obchodu a Českou obchodní inspekcí,
iii. účasti na jednáních Odborné skupiny pro akt o kybernetické odolnosti, jí podřízených tematických podskupin, komitologie, skupiny oznamujících orgánů a dalších skupiny zaměřených na přijímání prováděcích předpisů k aktu o kybernetické odolnosti a koordinaci v procesu implementace a jednotné aplikace aktu o kybernetické odolnosti,
y) provádí osvětu v oblasti evropských certifikací kybernetické bezpečnosti a aktu o kybernetické odolnosti, zejména zodpovídá dotazy veřejnosti, pořádá zaměřené přednášky a webináře, rozesílá newslettery a zajišťuje aktuálnosti informací v rámci své webové prezentace,

Oblast KI + krizové řízení

z) dává stanovisko ve věci určování kritické infrastruktury v odvětví ostatní digitální infrastruktura a služby podle zákona o kritické infrastruktuře,
aa) v rámci nouzového stavu dodává podklady pro ředitele Úřadu za účelem vyhlášení opatření ze stavu kybernetického nebezpečí jako krizová opatření v rámci nouzového stavu,
bb) v rámci krizových stavů konzultuje znění krizových opatření,
cc) podílí se na krizovém plánování na úrovni státu v oblasti kybernetické bezpečnosti, zejména zpracovává typový plán v oblasti kybernetické bezpečnosti,

Oblast jiných předpisů (Network code apod.)

dd) zajišťuje výklad a aplikaci nařízení Komise v přenesené pravomoci (EU) 2024/1366 ze dne 11. března 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2019/943 zavedením kodexu sítě pro odvětvová pravidla pro aspekty kybernetické bezpečnosti přeshraničních toků elektřiny (dále jen „NCCS“), pokud není část této agendy svěřena jinému organizačnímu celku,
ee) vede správní řízení za účelem přijetí návrhů podle čl. 8 NCCS a tyto návrhy připomínkuje,

ff) spolupracuje s vnitrostátními orgány tam, kde to vyplývá z působnosti podle jiných předpisů,

Obecná agenda

gg) podílí se na zpracování stanovisek, návrhů právních úprav, interních aktů řízení a materiálů nelegislativní povahy v oblasti kybernetické bezpečnosti, především těch předkládaných vládě České republiky a jejím orgánům,
hh) podílí se na informování vlády České republiky, orgánů státní správy, zahraničních partnerů a povinných subjektů podle zákona o kybernetické bezpečnosti o hrozbách, rizicích a aktuálních trendech v kybernetické bezpečnosti,
ii) podílí se na zvyšování kybernetické bezpečnosti u povinných subjektů podle zákona o kybernetické bezpečnosti,
jj) poskytuje metodickou podporu povinným subjektům podle zákona o kybernetické bezpečnosti a zabezpečuje v součinnosti s dalšími příslušnými organizačními celky metodickou činnost v oblasti kybernetické bezpečnosti,
kk) zodpovídá dotazy, poskytuje konzultace a podporu při výkladu právních předpisů regulujících kybernetickou bezpečnost,
ll) poskytuje konzultace pro využití Portálu NÚKIB,
mm) spolupracuje s pracovišti na národní i mezinárodní úrovni, která se podílejí na zajišťování bezpečnosti kybernetického prostoru,
nn) spolupracuje s příslušnými orgány členských států Evropské unie při určování regulovaných subjektů ze zákona o kybernetické bezpečnosti, pokud je to nezbytné,
oo) zajišťuje v rozsahu své působnosti plnění informačních povinností a dalších závazků vůči Evropské komisi a jiným orgánům zřizovaným předpisy Evropské unie v oblasti kybernetické bezpečnosti,
pp) poskytuje odboru cvičení a vzdělávání konzultace ke cvičením kybernetické bezpečnosti a těchto cvičení se účastní na národní i mezinárodní úrovni,
qq) poskytuje odboru cvičení a vzdělávání konzultace k připravovaným online kurzům, které se týkají jeho odbornosti,
rr) spolupracuje se soukromým sektorem i veřejným sektorem,
ss) vyžaduje za účelem plnění úkolů součinnost jiných státních institucí a regulátorů,
tt) vykonává publikační a přednáškovou činnost,
uu) podílí se na vytváření a udržování obsahu příslušné části webu Úřadu, veřejné části Portálu NÚKIB, dalších webů provozovaných Úřadem a interní wiki,
vv) podílí se na administraci a zodpovídání dotazů týkajících se Portálu NÚKIB,
ww) provádí registraci a evidenci externích subjektů do neveřejné části Portálu NÚKIB,
xx) podílí se na zodpovídání žádostí podle zákona o svobodném přístupu k informacím, pokud se týkají jeho odbornosti a dat, se kterými pracuje,
yy) podílí se na poskytování podkladů pro mediální prezentaci Úřadu tam, kde se tato týká jeho odbornosti,
zz) plní další pracovní úkoly uložené náměstkem ředitele pověřeným řízením sekce NCKB a ředitelem Úřadu.

Ve spolupráci s odborem kontroly

aaa) podílí se na vykonávání kontroly podle zákona o kybernetické bezpečnosti a s ní souvisejících úkonů,

bbb) spolupracuje v oblasti kybernetické bezpečnosti s ostatními kontrolními orgány,
ccc) podává příslušnému pracovišti Úřadu podněty na zahájení správního řízení v případě podezření z porušení povinností podle zákona o kybernetické bezpečnosti naplňujících znaky přestupku,
ddd) předává příslušnému pracovišti Úřadu podklady o kontrolovaných subjektech z evidencí dle odstavce 3 písm. r,
eee) podílí se na přípravě podkladů pro rozhodnutí ředitele Úřadu ve správním řízení,
fff) podílí se na vykonávání kontroly podle zákona o informačních systémech veřejné správy a s ní souvisejících úkonů.

Ve spolupráci s oddělením Development and Security Operations

ggg) podílí se na rozvoji Portálu NÚKIB vzhledem k plnění povinností vyplývajících ze zákona o kybernetické bezpečnosti,
hhh) zajišťuje obsahovou stránku veřejné části Portálu NÚKIB,
iii) vyžaduje spolupráci s ostatními celky Úřadu pro plnění úkolů a agend.

(4) Oddělení regulace veřejného sektoru plní zejména úkoly uvedené v odstavci 3 písm. a), b), d), h), p), q), aa), bb), cc), ff), gg), hh), ii), jj), kk), mm), nn), oo), pp), qq), rr), ss), tt), uu), xx), yy), zz), aaa), bbb), ccc), ddd), eee), fff) a ggg) dle zaměření své odbornosti na veřejný sektor.

(5) Oddělení regulace soukromého sektoru plní zejména úkoly uvedené v odstavci 3 písm. a), b), d), h), p), q), aa), bb), cc), dd), ee), ff), gg), hh), ii), jj), kk), mm), nn), oo), pp), qq), rr), ss), tt), uu), xx), yy), zz), aaa), bbb), ccc), ddd), eee), fff) a ggg) dle zaměření své odbornosti na soukromý sektor.

(6) Oddělení regulace dodavatelů informačních technologií plní zejména úkoly uvedené v odstavci 3 písm. a), b), d), h), p), q), t), z), aa), bb), cc), ff), gg), hh), ii), jj), kk), mm), nn), oo), pp), qq), rr), ss), tt), uu), xx), yy), zz), aaa), bbb), ccc), eee) a fff) dle zaměření své odbornosti na oblast dodavatelů informačních technologií.

(7) Pracovní skupina Evropské certifikace plní zejména úkoly uvedené v odstavci 3 písm. u) - y).

(8) Pracovní skupina bezpečnosti dodavatelského řetězce plní zejména úkoly uvedené v odstavci 3 písm. a), b), d), e), f), g), h), i), j), k), l), m), n), p), q), aa), bb), cc), ff), gg), hh), ii), jj), kk), mm), nn), oo), pp), qq), rr), ss), tt), uu), xx), yy), zz), aaa), bbb), ccc), eee) a ggg) dle zaměření své odbornosti na oblast bezpečnosti dodavatelského řetězce, strategicky významných služeb, protiopatření a elektronických komunikací.

(9) Pracovní skupina registrace, evidence a podpory plní zejména úkoly uvedené v odstavci 3 písm. c), o), r), s), ll, uu, vv, ww, ddd, ggg, hhh a administrativně podporuje další činnosti odboru.

Čl. 25
Odbor kontroly

(1) Odbor kontroly, v jehož čele stojí ředitel odboru, se dále člení na

a) oddělení kontroly 1,
b) oddělení kontroly 2 a

c) oddělení kontroly 3.

(2) Dalšími vedoucími zaměstnanci odboru kontroly jsou

a) vedoucí oddělení kontroly 1,
b) vedoucí oddělení kontroly 2 a
c) vedoucí oddělení kontroly 3,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor kontroly zejména

a) zpracovává plán kontrol a metodických auditů v oblasti kybernetické bezpečnosti,
b) plní další úkoly uložené náměstkem ředitele pověřeným řízením sekce NCKB a ředitelem Úřadu,
c) vede evidenci podle § 46 zákona o kybernetické bezpečnosti o provedených kontrolách a protokolů o kontrole.

(4) Oddělení kontroly 1, oddělení kontroly 2 a oddělení kontroly 3 zejména

a) vykonává kontrolu podle zákona o kybernetické bezpečnosti a s ní související úkony,
b) provádí metodické audity,
c) spolupracuje v oblasti kybernetické bezpečnosti s ostatními kontrolními orgány,
d) účastní se cvičení kybernetické bezpečnosti na národní i mezinárodní úrovni,
e) spolupracuje se soukromým a veřejným sektorem,
f) vykonává publikační a přednáškovou činnost,
g) podává příslušnému pracovišti Úřadu podněty na zahájení správního řízení v případě podezření z porušení povinností podle zákona o kybernetické bezpečnosti naplňujících znaky přestupku,
h) podílí se na přípravě podkladů pro rozhodnutí ředitele Úřadu ve správním řízení,
i) poskytuje odboru cvičení a vzdělávání konzultace k připravovaným online kurzům, které se týkají jeho odbornosti,
j) podílí se na zodpovídání žádostí podle zákona o svobodném přístupu k informacím, pokud se týkají jeho odbornosti a dat, se kterými pracuje,
k) projednává přestupky proti kontrole a spolupracuje s odborem právním na ukládání nápravných opatření ve správním řízení navazujícím na výkon kontroly,
l) plní další úkoly uložené náměstkem ředitele pověřeným řízením sekce NCKB a ředitelem Úřadu.

(5) Ve spolupráci s odborem regulace odbor kontroly včetně jeho oddělení

a) podílí se na zpracování návrhů právních úprav, interních aktů řízení a materiálů nelegislativní povahy předkládaných vládě České republiky a jejím orgánům,
b) podílí se na vykonávání kontroly podle zákona o informačních systémech veřejné správy a s ní souvisejících úkonů,
c) podílí se na poskytování metodické podpory pro zvyšování účinnosti bezpečnostních opatření zaváděných u poskytovatelů regulovaných služeb podle zákona o kybernetické bezpečnosti,
d) podílí se na zvyšování kybernetické bezpečnosti u poskytovatelů regulovaných služeb podle zákona o kybernetické bezpečnosti,
e) poskytuje řediteli Úřadu podklady a informace související s vyhlášením stavu kybernetického nebezpečí podle § 38 zákona o kybernetickém nebezpečí, vydáním opatření za stavu kybernetického nebezpečí podle § 39 zákona o kybernetické bezpečnosti a účinkem těchto

opatření, dále poskytuje podklady a informace související s přechodem stavu kybernetického nebezpečí do nouzového stavu.

HLAVA III.

ORGANIZAČNÍ CELKY PODŘÍZENÉ NÁMĚSTKOVI ŘEDITELE ÚŘADU POVĚŘENÉMU ŘÍZENÍM SEKCE PERSONALISTIKY, PRÁVA A PROVOZU

Čl. 26
Sekce personalistiky, práva a provozu

(1) Sekce personalistiky, právu a provozu se člení na

a) odbor právní,
b) odbor provozně ekonomický,
c) odbor plánování, řízení a fondů,
d) oddělení personálních věcí a vzdělávání.

(2) V čele sekce personalistiky, práva a provozu stojí náměstek ředitele pověřený řízením této sekce, který je vedoucím zaměstnancem 3. stupně řízení.

(3) Dalšími vedoucími zaměstnanci sekce personalistiky, práva a provozu jsou

a) ředitel odboru právního,
b) ředitel odboru provozně ekonomického,
c) ředitel odboru plánování, řízení a fondů,

kteří jsou vedoucími zaměstnanci 2. stupně řízení,

d) vedoucí oddělení personálních věcí a vzdělávání,

který je vedoucím zaměstnancem 1. stupně řízení.

(4) Sekce personalistiky, práva a provozu zejména

a) zajišťuje právní výstupy za Úřad v oblasti pracovněprávní, soukromoprávní, trestněprávní a správního řízení,
b) zajišťuje organizaci zadávání podlimitních nebo nadlimitních veřejných zakázek a vybraných zakázek malého rozsahu,
c) zajišťuje vedení správních řízení za porušení povinností stanovených zákonem o kybernetické bezpečnosti, zákonem o ochraně utajovaných informací nebo zákonem č. 179/2006 Sb., o ověřování a uznávání výsledků dalšího vzdělávání a o změně některých zákonů (zákon o uznávání výsledků dalšího vzdělávání), ve znění pozdějších předpisů (dále jen „zákon o uznávání výsledků dalšího vzdělávání“),
d) zajišťuje proces schvalování a evidence interních dokumentů a odpovídá za jejich legislativně právní úpravu,
e) zajišťuje plnění povinností vyplývajících pro Úřad ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, a nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním

osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),

f) zajišťuje návrhy a správu rozpočtu, vede komplexní účetnictví a zajišťuje výkaznictví Úřadu vůči požadavkům MF (IISSP a CSÚIS),
g) zajišťuje materiálně technické zázemí Úřadu, provoz, služby, správu a evidenci majetku, BOZP, autoprovoz,
h) zajišťuje činnosti spojené s vynakládáním finančních prostředků na investice, spolupracuje při plánování lidských zdrojů a zařazování zaměstnanců do organizačních celků v rámci organizační struktury Úřadu,
i) zajišťuje systemizaci pracovních míst a spolupracuje při tvorbě aktualizace organizační struktury dle návrhů jednotlivých útvarů,
j) zabezpečuje veškerou agendu personálních věcí a odměňování zaměstnanců,
k) zajišťuje péči o zaměstnance a sociální programy včetně agendy vztahující se k Fondu kulturních a společenských potřeb,
l) navrhuje a koordinuje problematiku společenské odpovědnosti Úřadu („CSR“),
m) zajišťuje spolupráci s odborovou organizací Úřadu ve věcech kolektivního vyjednávání,
n) zajišťuje zákonnost obsahu úřední desky Úřadu,
o) zajišťuje efektivní řízení projektů,
p) koordinuje mechanismus čerpání finančních prostředků z EU fondů,
q) centralizuje a koordinuje střednědobé a krátkodobé plánování Úřadu,
r) optimalizuje průřezové procesy,
s) plní další úkoly stanovené ředitelem Úřadu, zvláštními právními předpisy a interními akty řízení v rámci jednotlivých organizačních celků.

Čl. 27
Odbor právní

(1) Odbor právní, v jehož čele stojí ředitel odboru, se člení na

a) oddělení právní a přestupkové agendy,
b) oddělení právní agendy a druhostupňového rozhodování a
c) oddělení veřejných zakázek.

(2) Dalšími vedoucími zaměstnanci odboru právního jsou

a) vedoucí oddělení právní a přestupkové agendy,
b) vedoucí oddělení právní agendy a druhostupňového rozhodování a
c) vedoucí oddělení veřejných zakázek,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor právní zejména

a) projednává přestupky a správní delikty za porušení povinností stanovených zákonem o kybernetické bezpečnosti, zákonem o ochraně utajovaných informací a zákonem o uznávání výsledků dalšího vzdělávání,
b) ukládá ve spolupráci s odborem kontroly nápravná opatření dle zákona o kybernetické bezpečnosti,
c) vede správní řízení o pozastavení platnosti certifikace dle § 57 zákona o kybernetické bezpečnosti, vydává osvědčení o splnění povinnosti odstranit zjištěné nedostatky dle § 57 odst. 3 zákona o kybernetické bezpečnosti,

d) vede správní řízení o zákazu výkonu funkce člena statutárního orgánu dle § 58 zákona o kybernetické bezpečnosti, vydává rozhodnutí o zrušení zákazu výkonu funkce dle § 58 odst. 3 zákona o kybernetické bezpečnosti,
e) připravuje podklady pro rozhodnutí ředitele Úřadu o rozkladech a dalších podáních, o kterých rozhoduje nadřízený orgán, a vypracovává návrhy rozhodnutí ředitele Úřadu v těchto věcech,
f) zajišťuje jednání rozkladové komise ředitele Úřadu a administrativně zabezpečuje její chod,
g) posuzuje návrhy opatření obecné povahy a veřejnoprávních smluv vydávaných či uzavíraných Úřadem v oblastech jeho působnosti, a to před jejich uložením nebo uzavřením,
h) poskytuje metodickou pomoc příslušným organizačním celkům při stanovování formy a náležitostí rozhodnutí a dalších písemných dokumentů zpracovávaných v oblasti správního řízení ve všech oblastech působnosti Úřadu,
i) spolupracuje s věcně příslušným organizačním celkem na přípravě a tvorbě návrhů nových právních předpisů s celostátní působností nebo právních úprav věcí dosud právními předpisy neupravených, které jsou v působnosti Úřadu,
j) spolupracuje s věcně příslušným organizačním celkem na posuzování nových právních předpisů v připomínkovém řízení,
k) spolupracuje s věcně příslušným organizačním celkem na zpracování stanovisek Úřadu k návrhům nelegislativních materiálů předkládaných jinými ústředními správními úřady vládě České republiky nebo jejím poradním orgánům,
l) odpovídá za soulad interních dokumentů s právními předpisy a za proces jejich tvorby a legislativně technickou úpravu a ve své působnosti návrhy těchto interních dokumentů zpracovává,
m) zastupuje Úřad v řízeních před soudy a jinými orgány v trestním, občanskoprávním nebo správním řízení a vyžaduje k tomu součinnost ostatních organizačních celků,
n) připravuje podklady pro rozhodnutí o stížnosti uplatněné u veřejného ochránce práv, zastupuje Úřad při jednání s veřejným ochráncem práv, pokud si toto jednání nevyhradí v konkrétním případě ředitel Úřadu, a vyžaduje k tomu součinnost ostatních organizačních celků,
o) vyřizuje žádosti dle zákona č. 141/1961, o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů a žádosti dalších orgánů veřejné moci, nepatří-li jejich vyřízení do působnosti jiného organizačního celku, a vyžaduje k tomu součinnost ostatních organizačních celků,
p) vyřizuje žádosti, podněty či jiná podání učiněné fyzickými či právnickými osobami, nepatří-li jejich vyřízení do působnosti jiného organizačního celku, a vyžaduje k tomu součinnost ostatních organizačních celků,
q) zabezpečuje v rámci Úřadu ochranu duševního vlastnictví a zastupuje Úřad před příslušnými orgány v oblasti ochrany duševního vlastnictví (např. před Úřadem průmyslového vlastnictví),
r) zajišťuje plnění povinností vyplývajících pro Úřad ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a vyžaduje k tomu součinnost ostatních organizačních celků,
s) zpracovává návrhy nebo se vyjadřuje k návrhům smluv uzavíraných Úřadem, s výjimkou smluv a dohod uzavíraných v pracovněprávních vztazích se zaměstnanci Úřadu, objednávek podle zvláštního interního aktu řízení, smluv týkajících se vzdělávání zaměstnanců, smluv o zadávání inzerce a smluv o nákupu knih a učebních pomůcek,
t) zastupuje Úřad při vymáhání pohledávek, zejména uplatňuje nároky Úřadu ze smluvních pokut, náhrady škody, bezdůvodného obohacení a dalších titulů,

u) spolupracuje s věcně příslušným organizačním celkem na poskytování metodické činnosti v oblasti kybernetické bezpečnosti a vybraných oblastech ochrany utajovaných informací vůči orgánům státu a dalším subjektům,
v) na vyžádání poskytuje právní poradenství a připravuje právní stanoviska ostatním organizačním celkům v celém rozsahu působnosti Úřadu,
w) poskytuje metodickou pomoc příslušným organizačním celkům při zveřejňování objednávek a smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů a zajišťuje zveřejňování objednávek a smluv dle tohoto zákona v situacích, kdy povinnost zveřejnit tyto objednávky nebo smlouvy není uložena jinému organizačnímu celku,
x) zajišťuje plnění povinností vyplývajících pro Úřad z nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů – dále jen „nařízení GDPR“) a ze zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů a vyžaduje k tomu součinnost ostatních organizačních celků,
y) zajišťuje plnění povinností vyplývajících pro Úřad ze zákona č. 171/2023 Sb., o ochraně oznamovatelů, ve znění pozdějších předpisů a příslušného interního aktu řízení a vyžaduje k tomu součinnost ostatních organizačních celků,
z) spolupracuje s věcně příslušným organizačním celkem při zajišťování povinností uložených Úřadu jako evidenčnímu orgánu při vedení registru oznámení podle zák. č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů,
aa) spolupracuje s věcně příslušným organizačním celkem při zajišťování povinností uložených Úřadu zákonem č. 250/2017 Sb., o elektronické identifikaci, ve znění pozdějších předpisů,
bb) zajišťuje plnění povinností vyplývajících pro Úřad dle zákona č. 12/2020 Sb., o právu na digitální službu a změně některých zákonů, ve znění pozdějších předpisů a v této souvislosti obsluhuje agendu základních registrů ve smyslu zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, zejména pak spravuje nastavení soustavy práv a povinností ve smyslu těchto zákonů,
cc) spolupracuje s ostatními organizačními celky na plnění úkolů dle článku č. 7 nařízení Evropského Parlamentu a Rady (EU) 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center,
dd) zajišťuje plnění povinností vyplývajících pro Úřad z nařízení Evropského parlamentu a Rady (EU) 2024/1689, akt o umělé inteligenci,
ee) administruje zadávání podlimitních a nadlimitních veřejných zakázek, a vybraných zakázek malého rozsahu vč. komplexní přípravy zadávací dokumentace a smluvní dokumentace související s řešenou veřejnou zakázkou,
ff) koordinuje, metodicky řídí a usměrňuje činnost ostatních organizačních celků při zadávání veřejných zakázek malého rozsahu,
gg) plní další pracovní úkoly uložené náměstkem ředitele pověřeným řízením sekce personalistiky, práva a provozu nebo ředitelem Úřadu.

(4) Odbor právní plní zejména úkoly uvedené v odstavci 3 písm. w) až y).

(5) Oddělení právní a přestupkové agendy plní zejména úkoly uvedené v odstavci 3 písm. a) až d), g), h), q), r), cc) a dd).

(6) Oddělení právní agendy a druhostupňového rozhodování plní zejména úkoly uvedené v odstavci 3 písm. e), f), aa) a bb).

(7) Oddělení veřejných zakázek plní zejména úkoly uvedené v odstavci 3 písm. ee) a ff).

(8) Na plnění úkolů neuvedených v odstavcích 4 až 7 se podílí všechna oddělení odboru právního.

Čl. 28
Pověřenec pro ochranu osobních údajů

(1) Pověřenec pro ochranu osobních údajů (dále jen „pověřenec“) je funkční role zřízená podle nařízení GDPR. Pověřenec je organizačně zařazen v odboru právním. Pověřence jmenuje a odvolává ředitel Úřadu v souladu s právními předpisy.

(2) Pověřenec zajišťuje plnění povinností, které pro tuto roli vyplývají z právních předpisů upravujících problematiku ochrany osobních údajů.

(3) Při výkonu své funkce pověřenec vystupuje nezávisle; Úřad mu neukládá pokyny týkající se obsahu plnění jeho úkolů v oblasti ochrany osobních údajů.

(4) Pověřenec přímo reportuje řediteli Úřadu a má k němu přímý přístup. Toto přímé reportování není dotčeno jeho organizačním zařazením v odboru právním.

(5) Pověřenec zejména

a) poskytuje řediteli Úřadu a ostatním zaměstnancům Úřadu informace a poradenství o jejich povinnostech podle právních předpisů v oblasti ochrany osobních údajů,
b) monitoruje soulad s právními předpisy a vnitřními předpisy a další dokumentací Úřadu v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy zaměstnanců Úřadu,
c) poskytuje poradenství ohledně posouzení vlivu na ochranu osobních údajů a sleduje jeho provádění,
d) spolupracuje s Úřadem pro ochranu osobních údajů,
e) působí jako kontaktní místo pro Úřad pro ochranu osobních údajů v záležitostech týkajících se zpracování, včetně předchozích konzultací,
f) působí jako kontaktní osoba Úřadu pro subjekty údajů ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv,
g) spolupracuje s pověřenou osobou při přijímání a posuzování důvodnosti oznámení podaných prostřednictvím vnitřního oznamovacího systému zákona č. 171/2023 Sb., o ochraně oznamovatelů, ve znění pozdějších předpisů a příslušného interního aktu řízení, a navrhuje Úřadu opatření k nápravě nebo předejití protiprávnímu stavu, pokud se tato oznámení týkají oblasti ochrany osobních údajů.

(6) Pověřenec vedle výkonu této funkce plní další pracovní úkoly, pokud tím nedochází ke střetu zájmů; pověřenec zejména nesmí v jiné roli rozhodovat o účelech a prostředcích zpracování osobních údajů.

Čl. 29
Odbor provozně ekonomický

(1) Odbor provozně ekonomický, v jehož čele stojí ředitel odboru, se člení na

a) oddělení provozu a služeb, v jehož rámci je ustavena pracovní skupina autoprovozu,
b) oddělení účetnictví,

c) oddělení rozpočtu,
d) oddělení investic.

(2) Dalšími vedoucími zaměstnanci odboru provozně ekonomického jsou

a) vedoucí oddělení provozu a služeb,
b) vedoucí oddělení účetnictví,
c) vedoucí oddělení rozpočtu,
d) vedoucí oddělení investic,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor provozně ekonomický zejména

a) zajišťuje pro věcně příslušné organizační celky účtování správních poplatků a pokut v působnosti Úřadu, není-li stanoveno jiným právním předpisem jinak,
b) organizuje a metodicky usměrňuje inventarizaci majetku,
c) vytváří metodické směrnice pro účetnictví, rozpočet, hospodaření s majetkem a podílí se na přípravě nebo zpracovává návrhy interních dokumentů,
d) shromažďuje, koordinuje a zabezpečuje materiálně technické zabezpečení Úřadu vyjma toho, co je v kompetenci odboru bezpečnosti a odboru bezpečnosti informačních a komunikačních technologií,
e) vede evidenci movitého a nemovitého majetku, včetně činností s agendou souvisejících,
f) zajišťuje povinnosti Úřadu v oblasti bezpečnosti a ochrany zdraví zaměstnanců,
g) zajišťuje povinnosti Úřadu v oblasti požární ochrany,
h) zajišťuje provoz a servis služebních automobilů,
i) zajišťuje kurýrní službu, převoz pošty a distribuci v jednotlivých lokalitách,
j) zajišťuje ve spolupráci s odborem právním smluvní vztahy na dodávky energií, vody, plynu, tepla atd.,
k) spolupracuje s odborem právním při zadávání veřejných zakázek v rámci své věcné působnosti,
l) zajišťuje revizní zprávy na technologická zařízení dle příslušných předpisů,
m) zajišťuje údržbu majetku ve své působnosti, případně dozoruje nad stavebními opravami a úpravami,
n) zabezpečuje provozní činnosti v objektech Úřadu,
o) sleduje čerpání přidělené části rozpočtu Úřadu, navrhuje rozpočtová opatření,
p) zajišťuje vybrané statistické údaje,
q) zajišťuje v případě potřeby znalecké posudky a odborná vyjádření při správě majetku,
r) shromažďuje, připravuje a vede kompletní agendu Škodní a likvidační komise,
s) zajišťuje nabídková řízení nebo likvidaci majetku v rámci Úřadu,
t) zabezpečuje správy a rezervace služebních bytů,
u) připravuje návrh rozpočtu kapitoly státního rozpočtu 378-NÚKIB, návrh střednědobého výhledu a návrh závěrečného účtu kapitoly 378-NÚKIB,
v) zpracovává podklady od věcně příslušných organizačních celků týkající se investic, zadává je do ekonomického systému SMVS a kontroluje propojenost a čerpání rozpočtových položek jednotlivých akcí v SMVS s IISSP,
w) zpracovává podklady od věcně příslušných organizačních celků týkající se financování třetích stran, zadává je do systému RIS-ZED a kontroluje propojenost a čerpání rozpočtových položek jednotlivých akcí v RIS-ZED s IISSP,
x) zadává návrh rozpočtu a střednědobého výhledu do informačního systému IISSP,

y) sleduje čerpání rozpočtu Úřadu, navrhuje, zpracovává a realizuje rozpočtová opatření v systémech GINIS, IISSP, SMVS, a RIS-ZED,
z) plní funkci finančního manažera při financování projektů Úřadu, v případě potřeby připravuje podklady finančního charakteru pro veřejnosprávní kontrolu,
aa) provádí rozpis rozpočtu Úřadu na daný rozpočtový rok,
bb) organizačně zajišťuje, koordinuje a kontroluje měsíční doklad čerpání finančních prostředků ředitele Úřadu (tzv. semafor),
cc) zastupuje Úřad před Ministerstvem financí,
dd) plní v souladu se zákonem č. 320/2001 Sb., o finanční kontrole, v platném znění, funkci správce rozpočtu a funkci hlavní účetní kapitoly 378-NÚKIB,
ee) zajišťuje a zodpovídá za ekonomické výstupy Úřadu předávané IISSP (v CSÚIS), a na Ministerstvo financí,
ff) provádí účetní uzávěrky za daná účetní období,
gg) zajišťuje a zodpovídá za účetní výstupy Úřadu předávané do Centrálního systému účetních informací státu,
hh) zajišťuje chod pokladny,
ii) zajišťuje agendu tuzemských i zahraničních pracovních cest („ZPC“) v rozsahu daném interními normativními akty,
jj) na základě podkladů organizačních celků spravuje jednotlivé plány ZPC a zajišťuje aktuální informace ohledně skutečně vynaložených finančních prostředků na ZPC, zajišťuje letenky, ubytování, jízdenky a jiné výdaje v souvislosti s konáním ZPC zaměstnanců Úřadu,
kk) zajišťuje refundaci cestovních nákladů spojených se ZPC delegátů ČR na jednáních v působnosti Rady EU a za tímto účelem komunikuje s Ministerstvem financí,
ll) zajišťuje hotovostní a bezhotovostní platby,
mm) zajišťuje agendu platebních karet ve spolupráci s ČNB,
nn) zodpovídá za přípravu a realizaci investičních akcí schválených v rozpočtu Úřadu počínaje dokumentací pro stavební řízení a konče předáním staveb do majetku,
oo) zajišťuje opravy a rekonstrukce budov financované Úřadem,
pp) zajišťuje v souladu se zákonem o zadávání veřejných zakázek smluvní vztahy s dodavateli projektové dokumentace a následné realizace staveb,
qq) zajišťuje úkoly spojené se sledováním kvality a kvantity prováděných stavebních prací a dodávek, kontroluje dodržování norem a zásad technologie,
rr) předkládá roční plán investic a zajišťuje jeho plnění,
ss) spolupracuje s dalšími odbory při sestavování střednědobého a ročního plánu investičních akcí,
tt) spolupracuje při vypisování architektonické soutěže pro řešení zvlášť významných úkolů v rámci stavebního rozvoje,
uu) provádí archivaci zpracované projektové dokumentace, investičních akcí a příslušných smluvních vztahů,
vv) provádí komplexní inženýrskou činnost ve fázi projektové přípravy investic Úřadu,
ww) provádí komplexní inženýrskou činnost ve fázi realizace stavebních investic Úřadu až po jejich odevzdání do provozu,
xx) provádí financování stavebních investic Úřadu ve spolupráci se správci příslušných rozpočtových kapitol, zajišťuje převedení dokončených stavebních investic do majetku Úřadu,
yy) objednává odborné opravářské práce a údržbu pro detašovaná pracoviště v Praze,
zz) pracuje v jednotném informačním systému v zadávání objednávek a smluv týkajících se své působnosti,
aaa) kontroluje a likviduje faktury za práce a dodávky v rámci své působnosti,

bbb) plní další úkoly uložené ředitelem odboru nebo jeho prostřednictvím náměstkem/náměstkyní ředitele.

(4) Oddělení provozu a služeb plní zejména úkoly uvedené v odstavci 3 písm. b), e) až u) a aaa) až bbb).

(5) Oddělení účetnictví plní zejména úkoly uvedené v odstavci 3 písm. a) a b) a c) až nn).

(6) Oddělení rozpočtu plní zejména úkoly uvedené v odstavci 3 písm. v) až ee).

(7) Oddělení investic plní zejména úkoly uvedené v odstavci 3 písm. oo) až bbb).

(8) Všechna oddělení se podílejí na plnění úkolů uvedených v odstavci 3 písm. c) a d) a ccc).

Čl. 30

Odbor plánování, řízení a fondů

(1) Odbor plánování, řízení a fondů, v jehož čele stojí ředitel odboru, se člení na

a) oddělení plánování a řízení,
b) oddělení projektová kancelář, jehož součástí je pracovní skupina EU fondů

(2) Dalšími vedoucími zaměstnanci odboru plánování, řízení a fondů jsou

a) vedoucí oddělení plánování a řízení,
b) vedoucí oddělení projektová kancelář,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor plánování, řízení a fondů zejména

a) zpracovává a reviduje střednědobé a krátkodobé plány Úřadu,
b) koordinuje plánovací činnost samostatných organizačních celků Úřadu,
c) provádí řízení strategických a operačních rizik,
d) zajišťuje správu systému řízení rizik,
e) provádí optimalizaci relevantních/identifikovaných procesů a jejich workflow,
f) zajišťuje správu procesního modelu Úřadu,
g) zajišťuje zavádění úřadové architektury a naplňování jejich principů a pravidla, podle kterých se řídí úřadová architektura (enterprise architektura),
h) zpracovává ve spolupráci s ostatními organizačními celky Úřadu Zprávu o činnosti NÚKIB a Zprávu o naplňování Koncepce rozvoje Národního úřadu pro kybernetickou a informační bezpečnost,
i) zajišťuje procesy integrace a koordinace projektů a programů,
j) řídí významné projekty a programy, poskytuje metodickou podporu při řízení,
k) rozvíjí projektové manažery Úřadu a další potřebné role,
l) centralizuje a zavádí metodické postupy projektového řízení Úřadu,
m) implementuje legislativu i dobrou praxi v oblasti projektového řízení Úřadu,
n) provádí kontrolu správné aplikace pravidel projektového řízení na základě podmínek dle interního normativního aktu,
o) metodicky i prakticky podporuje projekty kofinancované z fondů EU (řízené ze strany Úřadu),

p) dohlíží na dodržování podmínek dotace a korektní čerpání dotací – v rozsahu svěřených projektů a na základě upřesnění interními předpisy a řídícími dokumenty,
q) přímo řídí, administruje a podílí se na tvorbě a podání žádostí – v rozsahu svěřených projektů a na základě upřesnění interními předpisy a řídícími dokumenty,
r) spolupracuje s poskytovateli EU dotací, posuzuje národní politiky podpory z relevantních EU fondů (program IROP, oblast eGovernmentu a kybernetické bezpečnosti a jejich budoucí obdoby) a identifikuje a řídí příležitosti pro zacílení EU-prostředků do požadovaných oblastí v kybernetické bezpečnosti,
s) monitoruje a rozšiřuje rozsah sledovaných příležitostí Úřadu pro čerpání z EU fondů i za hranice oblasti kybernetické bezpečnosti,
t) identifikuje a řídí příležitosti pro zacílení EU-prostředků do požadovaných oblastí agend a schopností NÚKIB, nebo pro jejich podporu,
u) centralizuje a pomáhá řídit portfolio žádostí, projektů a programů Úřadu, koordinuje vstupy z relevantních nebo specializovaných oblastí projektů, typů financování a úrovní řízení nebo plánování NÚKIB,
v) organizuje a řídí přípravu a realizaci Prague Cyber Security Conference a CyberCon a podílí se přímo na jejich realizaci,
w) provádí vzdělávací a školící činnost pro zaměstnance Úřadu v oblasti projektového řízení a ve vybraných oblastech působnosti odboru.

(4) Oddělení plánování a řízení plní zejména úkoly uvedené v odstavci 3 písm. a) až h).

(5) Oddělení projektová kancelář plní zejména úkoly uvedené v odstavci 3 písm. i) až n).

(6) Pracovní skupina EU fondů plní zejména úkoly uvedené v odstavci 3 písm. o) až u).

(7) Všechna oddělení se podílejí na plnění úkolů uvedených v odstavci 3 písm. v) až w).

Čl. 31
Oddělení personálních věcí a vzdělávání

(1) V čele oddělení personálních věcí a vzdělávání stojí vedoucí oddělení.

(2) Oddělení personálních věcí a vzdělávání zejména

a) koordinuje dle rozhodnutí vedení Úřadu přípravu a tvorbu strategických a koncepčních materiálů v oblasti lidských zdrojů, navrhuje interní pracovně právní předpisy a další interní dokumenty řízení v zabezpečovaných či souvisejících oblastech,
b) spolupracuje s odborem právním při posuzování nových právních předpisů v připomínkovém řízení předkládaných jinými ústředními orgány státní správy a na zapracování stanovisek k těmto návrhům,
c) spolupracuje při plánování lidských zdrojů a zařazování zaměstnanců do organizačních celků v rámci organizační struktury Úřadu,
d) spolupracuje s vedoucími jednotlivých útvarů a vedením Úřadu při tvorbě systemizace pracovních míst a zabezpečování organizačních změn,
e) provádí veškeré úkony personální agendy spojené se vznikem, průběhem a skončením pracovního poměru zaměstnanců,
f) provádí ve spolupráci s vedoucími zaměstnanci organizačních celků Úřadu výběr nových zaměstnanců Úřadu a související činnosti,

g) vede přijímací řízení s uchazeči o zaměstnání v Úřadu,
h) zpracovává koncepci vzdělávacích a sociálních programů pro zaměstnance Úřadu a organizačně je zabezpečuje,
i) vede plány vzdělávání zaměstnanců, zajišťuje vzdělávání zaměstnanců a připravuje podklady pro ředitele Úřadu pro uzavírání kvalifikačních dohod se zaměstnanci při prohlubování či zvyšování jejich kvalifikace,
j) metodicky spolupracuje s vedoucími zaměstnanci organizačních celků Úřadu při hodnocení zaměstnanců Úřadu,
k) metodicky spolupracuje s vedoucími zaměstnanci organizačních celků při tvorbě či změně kompetenčních modelů,
l) komplexně zabezpečuje agendu dohod o pracích konaných mimo pracovní poměr,
m) vede osobní spisy zaměstnanců,
n) zabezpečuje oblast odměňování a péče o zaměstnance,
o) připravuje podklady pro rozpočet platových a souvisejících věcných výdajů, sleduje jejich čerpání,
p) zabezpečuje platovou agendu Úřadu, připravuje návrhy pro odměňování zaměstnanců,
q) připravuje návrhy úprav složek platu v souvislosti s vývojem čerpání rozpočtu,
r) zabezpečuje včasné a správné zpracování měsíčních platů zaměstnanců,
s) vede evidenci mzdových listů a odpovídá za jejich uložení,
t) zajišťuje agendu daní z příjmů ze závislé činnosti a pojistné na sociální a zdravotní pojištění,
u) zastupuje Úřad při jednáních se Správou sociálního zabezpečení a zdravotními pojišťovnami,
v) sleduje a vyřizuje finanční odměny dle kolektivní smlouvy při dovršení stanovené doby trvání pracovního poměru,
w) zabezpečuje činnosti spojené se správou Fondu kulturních a sociálních potřeb Úřadu,
x) ve spolupráci s oddělením komunikace připravuje náborové akce Úřadu a prezentace na sociálních sítích zaměřené na hledání nových zaměstnanců,
y) zajišťuje inzerci pracovních míst na webu Úřadu a na pracovních portálech a zajišťuje účast na veletrzích pracovních příležitostí a obdobných akcích,
z) spolupracuje na aktivitách Úřadu v rámci personálního marketingu, ve spolupráci s oddělením komunikace prezentuje volné pozice na sociálních sítích,
aa) zabezpečuje agendu ochrany osobních údajů zaměstnanců v oblasti pracovně právních vztahů,
bb) projednává v součinnosti s příslušnými vedoucími zaměstnanci stížnosti zaměstnanců na výkon práv a povinností vyplývajících z pracovněprávních vztahů a vede o tom záznamy v osobních spisech,
cc) spolupracuje s odborem právním při zajišťování povinností uložených Úřadu jako evidenčnímu orgánu při vedení registru oznámení podle zák. č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů,
dd) spolupracuje s Odborovou organizací Úřadu ve věcech kolektivního vyjednávání,
ee) plní další pracovní úkoly uložené náměstkem ředitele.

HLAVA IV.

ORGANIZAČNÍ CELKY PODŘÍZENÉ NÁMĚSTKOVI ŘEDITELE ÚŘADU POVĚŘENÉMU ŘÍZENÍM SEKCE INFORMAČNÍCH SYSTÉMŮ

Čl. 32
Sekce informačních systémů

(1) Sekce informačních systémů se člení na

a) odbor bezpečnosti informačních a komunikačních technologií,
b) odbor informačních technologií a
c) oddělení bezpečnosti satelitních služeb.

(2) V čele Sekce informačních systémů stojí náměstek ředitele pověřený řízením této sekce, který je vedoucím zaměstnancem 3. stupně řízení.

(3) Dalšími vedoucími zaměstnanci Sekce informačních systémů jsou

a) ředitel odboru bezpečnosti informačních a komunikačních technologií,
b) ředitel odboru informačních technologií,

kteří jsou vedoucími zaměstnanci 2. stupně řízení,

c) vedoucí oddělení bezpečnosti satelitních služeb,

který je vedoucím zaměstnancem 1. stupně řízení.

(4) Sekce informačních systémů zejména

a) podílí se na tvorbě koncepce bezpečnostní politiky státu,
b) zajišťuje ověřování úrovně ochrany elektronických zařízení, jednacích oblastí, zabezpečených oblastí nebo objektů proti úniku utajovaných informací formou kompromitujícího vyzařování,
c) zajišťuje prosazování ochrany utajovaných informací v oblasti zpracování utajovaných informací v informačních a komunikačních systémech,
d) hodnocení bezpečnosti komunikačních a certifikaci informačních systémů, stínících komor, kryptografických pracovišť a kryptografických prostředků určených pro sběr, tvorbu, zpracování, ukládání, zobrazení a přenášení utajovaných informací,
e) podílí se v rozsahu své působnosti a v součinnosti s ostatními věcně příslušnými organizačními celky se na tvorbě bezpečnostní politiky Úřadu, spolupráci na mezinárodní úrovni a plnění mezinárodních závazků vyplývajících z členství České republiky v NATO, v EU a v jiných mezinárodních organizacích,
f) zajišťuje řízení kryptografické ochrany utajovaných informací u orgánů státu a podnikatelů,
g) zajišťuje výrobu a distribuci kryptografických materiálů k ochraně utajovaných informací,
h) zajišťuje rozvoj kryptologie, základní i aplikovaný výzkum a vývoj v oblasti kryptologie a kryptografických prostředků,
i) zajišťuje budování a chod komunikačních a informačních systémů Úřadu, včetně komunikačního a datového spojení Úřadu,
j) zajišťuje v rozsahu stanoveném ředitelem Úřadu ochranu utajovaných informací v Úřadu,
k) zajišťuje v rámci Úřadu kontrolu dodržování zásad ochrany utajovaných informací,

l) zajišťuje koncepci přípravy ke krizovému řízení státu v působnosti Úřadu a její soulad s koncepcí krizového řízení státu,
m) zajišťuje výzkum a vývoj v oblasti ochrany utajovaných informací v informačních a komunikačních systémech, a v oblasti bezpečnosti satelitních služeb,
n) vede operativní evidence výpočetní a spojové techniky Úřadu,
o) zajišťuje implementaci a provoz veřejně regulované služby (PRS) v České republice v rámci globálního navigačního družicového systému Galileo,
p) plní další úkoly stanovené ředitelem Úřadu, zvláštními právními předpisy a interními akty řízení v rámci jednotlivých odborů.

Čl. 33
Odbor bezpečnosti informačních a komunikačních technologií

(1) Odbor bezpečnosti informačních a komunikačních technologií, v jehož čele stojí ředitel odboru, se člení na

a) oddělení vývoje kryptografických prostředků,
b) oddělení certifikací informačních a komunikačních systémů,
c) oddělení certifikací kryptografických prostředků a pracovišť,
d) oddělení Tempest,
e) oddělení Národní distribuční středisko, jehož součástí je pracovní skupina CDA (Crypto Distribution Authority),
f) oddělení odborné podpory,
g) oddělení kryptologických analýz.

(2) Dalšími vedoucími zaměstnanci odboru bezpečnosti informačních a komunikačních technologií jsou

a) vedoucí oddělení vývoje kryptografických prostředků,
b) vedoucí oddělení certifikací informačních a komunikačních systémů,
c) vedoucí oddělení certifikací kryptografických prostředků a pracovišť,
d) vedoucí oddělení Tempest,
e) vedoucí oddělení Národní distribuční středisko,
f) vedoucí oddělení odborné podpory,
g) vedoucí oddělení kryptologických analýz,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor bezpečnosti informačních a komunikačních technologií zejména

a) vytváří koncepci rozvoje ochrany utajovaných informací v oblasti bezpečnosti informačních a komunikačních systémů, v oblasti kryptografické ochrany a ochrany před únikem utajovaných informací kompromitujícím vyzařováním, s vazbami na jiné obory a služby s celostátní a mezinárodní působností,
b) plní úkoly Národního střediska pro bezpečnost informačních systémů,
c) provádí certifikaci informačních systémů používaných k nakládání s utajovanými informacemi, zajišťuje styk s žadateli o certifikaci informačních systémů, poskytuje informace a konzultace související s certifikačním řízením a vede agendu s touto činností spojenou,
d) schvaluje projekty bezpečnosti komunikačních systémů používaných k nakládání s utajovanými informacemi,

e) zajišťuje poradenskou činnost při vývoji informačních a komunikačních systémů pro nakládání s utajovanými informacemi u orgánů státu,
f) zpracovává odborná vyjádření a stanoviska z oblasti ochrany utajovaných informací v informačních a komunikačních systémech a kryptografické ochrany, shromažďuje poznatky a zpracovává metodické materiály k jejich bezpečnosti,
g) koordinuje dílčí činnosti jím pověřených orgánů státu a jiných subjektů v oblasti certifikací,
h) zpracovává a vydává bezpečnostní standardy pro oblast bezpečnosti informačních a komunikačních systémů, kryptografické ochrany a ochrany před únikem utajovaných informací kompromitujícím vyzařováním,
i) vede přehled a evidenci certifikovaných informačních systémů, provádí následnou kontrolu dodržování podmínek certifikace v certifikovaných informačních systémech, posuzuje a schvaluje změny v certifikovaných informačních systémech,
j) zajišťuje plnění úlohy Úřadu jako orgánu pro bezpečnostní akreditaci informačních systémů nakládajících s utajovanými informacemi pro NATO a EU a jiné mezinárodní organizace,
k) provádí hodnocení informačních systémů nakládajících s utajovanými informacemi NATO a EU a jiných mezinárodních organizací,
l) provádí styk s orgány NATO a EU a jiných mezinárodních organizací pro zajištění akreditace informačních systémů a průběžnou kontrolní činnost v akreditovaných systémech podle požadavků NATO a EU a jiných mezinárodních organizací,
m) specifikuje, zadává a odborně řídí výzkumně-vývojové práce zajišťující implementaci bezpečnostních funkcí komunikačních a informačních systémů,
n) plní úkoly Národního střediska pro měření kompromitujícího vyzařování (National TEMPEST Authority),
o) navrhuje metody a postupy hodnocení elektrických a elektronických zařízení, jednacích oblastí, zabezpečených oblastí nebo objektů z hlediska úniku utajovaných informací prostřednictvím kompromitujícího vyzařování, zajišťuje styk s žadateli o provedení hodnocení elektrických a elektronických zařízení, jednacích oblastí, zabezpečených oblastí nebo objektů z hlediska úniku utajovaných informací prostřednictvím kompromitujícího vyzařování, poskytuje informace a konzultace potřebné k certifikaci informačních systémů nebo pro schválení projektu bezpečnosti komunikačních systémů, zabezpečuje a provádí školení a osvětovou činnost v oblasti kompromitujících vyzařování,
p) provádí analýzy a hodnocení elektrických a elektronických zařízení z hlediska úniku utajovaných informací prostřednictvím kompromitujícího vyzařování,
q) provádí zónové hodnocení prostorů určených pro zpracování utajovaných informací,
r) provádí analýzy a hodnocení kryptografických prostředků z hlediska ochrany proti kompromitujícímu vyzařování,
s) provádí certifikaci stínících komor určených pro ochranu utajovaných informací a vede jejich seznam,
t) koordinuje dílčí činnosti jím pověřených orgánů státu a jiných subjektů v oblasti hodnocení elektrických a elektronických zařízení, jednacích oblastí, zabezpečených oblastí nebo objektů z hlediska úniku utajovaných informací prostřednictvím kompromitujícího vyzařování,
u) provádí na žádost odpovědné osoby kontrolu, zda v jednací nebo zabezpečené oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací,
v) provádí specializovanou odbornou činnost při zabezpečování ochrany jednacích oblastí a zabezpečených oblastí a objektů proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování u orgánů státu a jiných subjektů,
w) provádí na žádost ředitele Úřadu specializovanou odbornou činnost při zabezpečování ochrany jednacích oblastí a zabezpečených oblastí a objektů proti úniku utajovaných informací

prostřednictvím nedovoleného použití technických prostředků určených k získávání informací nebo prostřednictvím kompromitujícího vyzařování,

x) plní úkoly Národního bezpečnostního komunikačního střediska (NCSA),

y) zabezpečuje a provádí certifikaci kryptografických prostředků a stanovuje bezpečnostní standardy v oblasti certifikace kryptografických prostředků, zajišťuje styk s žadateli o certifikaci kryptografických prostředků, poskytuje informace a konzultace související s certifikačním řízením a vede agendu s touto činností spojenou, vede seznam materiálu Úřadu kategorie CCI,

z) navrhuje metody a postupy certifikace kryptografických prostředků z hlediska hodnocení jejich ochrany proti kompromitujícímu vyzařování,

aa) provádí certifikaci kryptografických pracovišť, zajišťuje styk s žadateli o certifikaci kryptografických pracovišť, poskytuje informace a konzultace související s certifikačním řízením a vede agendu s touto činností spojenou,

bb) podílí se na zajišťování veřejných zakázek Úřadu v oblasti výzkumu, vývoje a výroby kryptografických prostředků,

cc) vytváří národní politiku kryptografické ochrany,

dd) provádí a zabezpečuje aplikovaný výzkum a vývoj kryptografických prostředků,

ee) provádí a zabezpečuje výzkum a vývoj v oblasti aplikované kryptografie,

ff) provádí analýzy a hodnocení šifrových systémů a kryptografických algoritmů určených k ochraně utajovaných informací,

gg) plní úkoly kryptografické ochrany vyplývající z členství ČR v EU a NATO,

hh) zajišťuje činnost Národního distribučního střediska (NDS), pokud jde o výrobu a evidenci kryptografického materiálu (KM) a materiálu k zajištění funkce kryptografického prostředku (MZF), distribuci a evidenci KM ČR, EU a KM na základě mezinárodní smlouvy prostřednictvím CDA CZ, distribuci a evidenci KM NATO a KM pro vojenské účely prostřednictvím NDA CZ (MO), a mezinárodní přepravu KM prostřednictvím kurýrní služby z/do ČR, na základě smlouvy,

ii) vede evidenci kryptografických dokumentů a pracovníků kryptografické ochrany,

jj) vede evidenci kompromitací klíčových a heslových materiálů, kryptografických prostředků a systémů,

kk) podílí se na zajištění servisu a údržbě kryptografických prostředků EU, NATO a smluvních stran,

ll) zajišťuje servis a údržbu speciálního zařízení pro výrobu klíčového materiálu a materiálu k zajištění funkce kryptografického prostředku,

mm) zajišťuje vývoj nových technologií a výrobních zařízení na výrobu klíčových materiálů a kryptografických prostředků a vývoj v oblasti jejich zabezpečení proti neoprávněné manipulaci při přepravě,

nn) provádí kontrolní činnost v oblasti KM EU na území ČR a poskytuje součinnost při provádění kontrol ze strany orgánů EU,

oo) provádí ověřování odborné způsobilosti pracovníků kryptografické ochrany (zkoušky zvláštní odborné způsobilosti) v rozsahu speciální obsluhy kryptografické ochrany a vydává osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany v rozsahu speciální obsluhy kryptografické ochrany,

pp) podílí se na výkonu státního dozoru ve vybraných oblastech ochrany utajovaných informací v rámci České republiky,

qq) vykonává kontrolu ve vybraných oblastech ochrany utajovaných informací dle zákona,

rr) podílí se ve své působnosti na metodické činnosti ve vybraných oblastech ochrany utajovaných informací v orgánech státu a u jiných subjektů,

ss) podílí se na tvorbě právních předpisů, interních aktů řízení a na uzavírání smluvních vztahů,

tt) schvaluje způsobilost materiálu k zabezpečení funkce kryptografického prostředku, a prostředků zajišťujících kryptografickou ochranu přenášené taktické informace,

uu) schvaluje projekty zástavby kryptografických prostředků do mobilních rozmístitelných systémů,
vv) provádí akademickou činnost a spolupracuje s akademickou sférou v oblasti teoretické a aplikované kryptologie, včetně postkvantové kryptografie a kvantových technologií, plní roli aplikačního garanta v těchto oblastech,
ww) provádí a koordinuje analýzy bezpečnosti kryptografických algoritmů,
xx) vyvíjí a schvaluje národní šifrové algoritmy a národní kryptografická schémata pro ochranu utajovaných informací,
yy) provádí styk s orgány NATO a EU a jiných mezinárodních organizací v oblasti kryptologie a kvantových technologií,
zz) provádí styk s orgány NATO a EU a jiných mezinárodních organizací pro zajištění mezinárodní certifikace (schválení) kryptografických prostředků těmito organizacemi,
aaa) v rámci České republiky vytváří metodiku pro distribuci kryptografického materiálu EU a smluvních stran,
bbb) poskytuje odbornou podporu v oblasti vědy, výzkumu a inovací, pokud jde o projekty týkající se ochrany utajovaných informací, kryptografické ochrany utajovaných a citlivých informací, ochrany před únikem informací prostřednictvím kompromitujícího vyzařování a v oblasti bezpečnosti satelitních služeb,
ccc) zadává veřejné zakázky v oblasti výzkumu a vývoje ve vybraných oblastech ochrany utajovaných informací, provádí hodnocení žádostí uchazečů na řešení jednotlivých projektů, podílí se na přípravě smluv s řešiteli výzkumných a vývojových projektů,
ddd) koordinuje sběr výzkumných záměrů pro všechny oblasti činnosti Úřadu, předkládá ke schválení Výzkumný záměr Úřadu a vypracovává Zprávu o plnění výzkumného záměru Úřadu za příslušný rok,
eee) vypracovává návrh rozpočtu pro oblast výzkumu a vývoje Úřadu a vede přehled čerpání finančních prostředků určených pro oblast výzkumu a vývoje,
fff) podílí se na legislativní tvorbě nových právních předpisů s celostátní působností ve vybraných oblastech ochrany utajovaných informací,
ggg) podílí se na přípravě nelegislativních materiálů předkládaných Úřadem vládě České republiky, Parlamentu České republiky, popřípadě dalším orgánům státu,
hhh) zajišťuje a provádí distribuci kryptografického materiálu EU a smluvních stran,
iii) podílí se na zajišťovaní servisu kryptografických prostředků EU a smluvních stran,
jjj) zabezpečuje a provádí ověřování odborné způsobilosti pracovníků, kteří se budou seznamovat s informacemi s krypto EU, a k tomu vydává příslušnou autorizaci,
kkk) provádí kontrolní činnost v oblasti kryptografického materiálu EU a poskytuje součinnost při provádění kontrol orgánů EU.

(4) Oddělení vývoje kryptografických prostředků plní zejména úkoly uvedené v odstavci 3 písm. bb), dd), ee) a mm). Podílí se na řešení úkolů xx) a yy).

(5) Oddělení certifikací informačních a komunikačních systémů plní zejména úkoly uvedené v odstavci 3 písm. b) až e), g), i) až m), x).

(6) Oddělení certifikace kryptografických prostředků a pracovišť plní zejména úkoly uvedené v odstavci 3 písm. g), x), y), z), aa), oo), pp), rr), tt), uu) a zz).

(7) Oddělení Tempest plní zejména úkoly uvedené v odstavci 3 písm. n) až w), z) a nn).

(8) Oddělení Národní distribuční středisko plní zejména úkoly uvedené v odstavci 3 písm. gg) až oo).

(9) Oddělení odborné podpory plní zejména úkoly uvedené v odstavci 3 písm. l, bb, ss, bbb) až ggg).

(10) Pracovní skupina CDA plní zejména úkoly uvedené v odstavci 3 písm. aaa), hhh) až kkk).

(11) Oddělení kryptologických analýz plní zejména úkoly uvedené v odstavci 3 písm. ff), vv) až yy).

(12) Všechna oddělení a pracovní skupiny odboru bezpečnosti informačních a komunikačních technologií se podílí na plnění úkolů uvedených v odstavci 3 písm. a), e), f), h), pp), qq), bbb), ccc) a ddd).

Čl. 34

Odbor informačních technologií

(1) Odbor informačních technologií, v jehož čele stojí ředitel odboru, se člení na

a) oddělení síťové infrastruktury a dohledu, v jehož rámci je ustavena pracovní skupina provozního dohledu,
b) oddělení serverové infrastruktury,
c) oddělení klientské podpory v rámci něhož je ustavena pracovní skupina uživatelské podpory,
d) oddělení podpory aplikací a rozvoje a
e) oddělení plánování, ekonomiky a logistiky v IT.

(2) Další vedoucími zaměstnanci odboru informačních technologií jsou

a) vedoucí oddělení síťové infrastruktury a dohledu,
b) vedoucí oddělení serverové infrastruktury,
c) vedoucí oddělení klientské podpory,
d) vedoucí oddělení podpory aplikací a rozvoje a
e) vedoucí oddělení plánování, ekonomiky a logistiky v IT,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor informačních technologií zejména

a) vytváří dlouhodobé strategie Úřadu v oblasti informačních systémů a jeho komunikační infrastruktury, koordinuje vývoj, provoz, inovace a údržbu informačních a komunikačních systémů Úřadu a zajišťuje jejich slučitelnost s celostátní informační politikou a dalšími mezinárodními požadavky,
b) zabezpečuje výstavbu, správu, provoz a údržbu informačních a komunikačních systémů Úřadu,
c) zabezpečuje výstavbu, správu, provoz a údržbu informačních a komunikačních systémů externích státních orgánů a jiných subjektů umístěných v Úřadu, které Úřad využívá pro plnění svých povinností,
d) spolupracuje s ostatními organizačními celky při uzavírání smluv Úřadu týkajících se vnitřních informačních systémů, komunikačních a dalších informačních systémů,
e) stanovuje vnitřní provozní podmínky včetně dokumentace pro provoz komunikačních a informačních systémů Úřadu,
f) vede operativní evidenci výpočetní a spojové techniky Úřadu, spolupracuje při její inventarizaci,
g) navrhuje vyřazování výpočetní a spojové techniky Úřadu a poskytuje součinnost při jejím vyřazení,
h) organizuje a provádí pořizování nové výpočetní a spojovací techniky a softwarových prostředků, v případě zadávání veřejných zakázek v této oblasti spolupracuje s odborem právním,

i) vyřizuje odůvodněné požadavky na spotřební materiál k výpočetní a spojové technice,
j) podílí se na tvorbě interních normativních aktů a na uzavírání obchodních smluv a vztahů ve své věcné působnosti,
k) zajišťuje objednávání, bezpečné ukládání, distribuci a správu uznávaných elektronických podpisů zaměstnanců Úřadu od vybraného akreditovaného poskytovatele,
l) zajišťuje nákup a správu kvalifikovaných systémových certifikátů a nákup časových razítek,
m) podílí se na zajištění technických prostředků pro Portál NÚKIB,
n) plní další pracovní úkoly uložené náměstkem ředitele.

(4) Všechna oddělení plní zejména úkoly stanovené v odstavci 3 písm. a) až n).

Čl. 35
Oddělení bezpečnosti satelitních služeb

(1) V čele oddělení bezpečnosti satelitních služeb stojí vedoucí oddělení.

(2) Oddělení bezpečnosti satelitních služeb zejména

a) vytváří a udržuje plán řízení PRS, který stanoví podmínky pro využívání PRS a výrobu zařízení PRS,
b) vypracovává a aktualizuje podrobné provozní předpisy umožňující správné využívání PRS,
c) určuje a spravuje skupiny uživatelů PRS, stanovuje a řídí jejich přístupová práva,
d) je kontaktním bodem pro trvalé spojení s bezpečnostním střediskem PRS,
e) bezpečnostnímu středisku PRS oznamuje všechny bezpečnostní incidenty narušující bezpečnost PRS,
f) zajišťuje management přístupových klíčů k PRS,
g) sleduje všechny aspekty ovlivňující bezpečnost PRS,
h) vyhodnocuje rizika a přijímá příslušná nápravná a preventivní opatření,
i) řídí a kontroluje výrobu, držení a používání přijímačů PRS fyzickými osobami na území České republiky a právnickými osobami se sídlem v České republice,
j) zajišťuje bezpečnostní akreditaci pro subjekty usazené na území ČR vyvíjející nebo vyrábějící přijímače PRS nebo bezpečnostní moduly,
k) provádí inspekce u všech subjektů nakládajících s položkami PRS a informacemi PRS a usazených na území ČR,
l) předkládá Evropské komisi a Agentuře Evropské unie pro kosmický program (EUSPA) zprávu o dodržování společných minimálních standardů,
m) zastupuje ČR v pracovních skupinách řešících problematiku bezpečnosti GNSS Galileo a PRS, GOVSATCOM, Secure Connectivity,
n) zajišťuje komunikaci s uživateli PRS, GOVSATCOM, Secure Connectivity,
o) plní další pracovní úkoly uložené náměstkem ředitele.

HLAVA V

ORGANIZAČNÍ CELKY PODŘÍZENÉ NÁMĚSTKOVI ŘEDITELE ÚŘADU POVĚŘENÉMU ŘÍZENÍM SEKCE STRATEGICKÝCH AGEND A SPOLUPRÁCE

Čl. 36
Sekce strategických agend a spolupráce

(1) Sekce strategických agend a spolupráce se člení na

a) odbor centrální analytiky,
b) odbor cvičení a vzdělávání,
c) odbor mezinárodní spolupráce a Evropské unie,
d) oddělení národních strategií a politik a
e) oddělení vědy, výzkumu a inovací.

(2) V čele sekce strategických agend a spolupráce stojí náměstkyně ředitele pověřená řízením této sekce, která je vedoucím zaměstnancem 3. stupně řízení.

(3) Dalšími vedoucími zaměstnanci sekce strategických agend a spolupráce jsou

a) ředitel odboru centrální analytiky,
b) ředitel odboru cvičení a vzdělávání,
c) ředitel odboru mezinárodní spolupráce a Evropské unie,

kteří jsou vedoucími zaměstnanci 2. stupně řízení,

d) vedoucí oddělení národních strategií a politik,
e) vedoucí oddělení vědy, výzkumu a inovací,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(4) Sekce strategických agend a spolupráce zejména

a) zajišťuje analýzu a monitoring kybernetických hrozeb, rizik a aktuálních trendů v kybernetické bezpečnosti,
b) zajišťuje zastupování České republiky v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti,
c) spolupracuje s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru,
d) zajišťuje pořádání a účast na kybernetických cvičeních na národní a mezinárodní úrovni,
e) provádí osvětovou a vzdělávací činnost v oblasti kybernetické bezpečnosti,
f) řídí a koordinuje výzkum a vývoj v oblasti kybernetické bezpečnosti,
g) zajišťuje v rozsahu své působnosti bezpečnostní politiku Úřadu, plnění mezinárodních závazků a spolupráci na mezinárodní úrovni při realizaci předpisů vyplývajících z členství České republiky v NATO, EU a v jiných mezinárodních organizacích,
h) připravuje Národní strategii kybernetické bezpečnosti a Akční plán k Národní strategii kybernetické bezpečnosti,
i) zpracovává Zprávy o stavu kybernetické bezpečnosti České republiky,
j) plní další úkoly a povinnosti stanovené ředitelem Úřadu v rozsahu právních předpisů v oblasti kybernetické bezpečnosti.

Čl. 37
Odbor centrální analytiky

(1) Odbor centrální analytiky, v jehož čele stojí ředitel odboru, se dále člení na

a) oddělení strategických analýz,
b) oddělení informačního šetření a
c) oddělení správy a analýzy dat.

(2) Dalšími vedoucími zaměstnanci odboru centrální analytiky jsou

a) vedoucí oddělení strategických analýz,
b) vedoucí oddělení informačního šetření,
c) vedoucí oddělení správy a analýzy dat.

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor centrální analytiky zejména

a) provádí analýzu a monitoring kybernetických hrozeb, rizik a aktuálních trendů v kybernetické bezpečnosti,
b) podílí se na výměně informací o bezpečnostních hrozbách v kybernetickém prostoru s orgány státní správy, povinnými subjekty (dle zákona o kybernetické bezpečnosti) a zahraničními partnery,
c) podílí se na rozvoji a implementaci pokročilé analytické kapacity CTI (Cyber Threat Intelligence) (ve spolupráci s odborem vládní CERT),
d) spolupracuje v oblasti kybernetických hrozeb, trendů a analýzy, sběru a správy dat s pracovišti veřejného a soukromého sektoru na národní i mezinárodní úrovni, která se podílejí na zajišťování bezpečnosti kybernetického prostoru,
e) podílí se na přednáškové a pedagogické činnosti Úřadu v oblasti kybernetických hrozeb, trendů a analýzy, sběru a správy dat pro veřejnost či odbornou veřejnost,
f) poskytuje konzultaci jiným organizačním celkům v oblasti kybernetických hrozeb a trendů,
g) podílí se na přípravě podkladů pro jednání se zahraničními partnery (ve spolupráci s odborem mezinárodní spolupráce a Evropské unie),
h) podílí se na přípravě podkladů pro žádost ředitele Úřadu o vyhlášení nouzového stavu a posuzuje, zda rozhodnutí nebo opatření obecné povahy vydaná Úřadem před vyhlášením nouzového stavu nejsou ve věcném rozporu s krizovými opatřeními vyhlášenými vládou České republiky, (ve spolupráci s odborem regulace, odborem kontroly a odborem vládní CERT),
i) poskytuje odboru cvičení a vzdělávání konzultace ke cvičením kybernetické bezpečnosti a těchto cvičení se účastní na národní i mezinárodní úrovni,
j) provádí informační šetření v oblasti cloud computingu a výstupy poskytuje odboru regulace pro účely vypracování stanoviska k bezpečnosti služeb cloud computingu a jejich poskytovatelů,
k) provádí informační šetření týkající se kontrolovaných subjektů a výstupy poskytuje odboru kontroly jako podklad pro provedení kontroly,
l) provádí další informační šetření regulovaných i neregulovaných subjektů v kontextu kybernetické bezpečnosti a výstupy poskytuje dalším organizačním celkům či partnerům mimo Úřad,
m) provádí vývoj a správu analytických a datových nástrojů,

n) poskytuje dalším organizačním celkům podporu v podobě datové analýzy či vývoje, správy a poskytování datových a analytických nástrojů,
o) podílí se na tvorbě obsahu k Portálu NÚKIB,
p) plní další pracovní úkoly uložené náměstkyní ředitele.

(4) Oddělení odboru centrální analytiky v rozsahu své odbornosti plní zejména následující úkoly

a) oddělení strategických analýz úkoly uvedené v odstavci 3 písm. a) až i) a o),
b) oddělení informačního šetření plní úkoly uvedené v odstavci 3 písm. j) až l),
c) oddělení správy a analýzy dat plní úkoly uvedené v odstavci 3 písm. m), n) a p).

Čl. 38
Odbor cvičení a vzdělávání

(1) Odbor cvičení a vzdělávání, v jehož čele stojí ředitel odboru, se člení na

a) oddělení cvičení a
b) oddělení vzdělávání.

(2) Dalšími vedoucími zaměstnanci odboru cvičení a vzdělávání jsou

a) vedoucí oddělení cvičení a
b) vedoucí oddělení vzdělávání,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor cvičení a vzdělávání zejména

a) zajišťuje preventivní, vzdělávací a osvětové aktivity Úřadu u všech cílových skupin, pořádá konference a semináře pro veřejnost, podporuje vzdělávací iniciativy a osvětové kampaně,
b) koordinuje vzdělávání zaměstnanců veřejné správy v oblasti kybernetické bezpečnosti a v oblasti utajovaných informací, ve spolupráci s Ministerstvem vnitra, kraji, obcemi a dalšími institucemi prosazuje kybernetickou bezpečnost jako nutnou součást vstupních školení pro úředníky státní správy i samosprávy,
c) vytváří a spravuje e-learningovou platformu pro masové vzdělávání cílových skupin, podporuje a rozvíjí i další moderní výukové metody vedoucí ke zvýšení úrovně vzdělanosti v oblasti kybernetické bezpečnosti,
d) podporuje vzdělávací a jiné instituce při šíření osvěty v oblasti kybernetické bezpečnosti u žáků a studentů všech stupňů, u pedagogů, usiluje o zařazení tématiky kybernetické bezpečnosti do rámcových vzdělávacích programů a studijních programů, podílí se na tvorbě metodických a didaktických materiálů pro učitele i žáky,
e) podporuje u studentů rozvoj talentu v oblasti kybernetické bezpečnosti, spolupracuje při zprostředkování stáží studentů v rámci Úřadu,
f) podílí se ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy České republiky na zvýšení počtu škol zaměřených na kybernetickou bezpečnost, na zvýšení počtu studentů a absolventů oborů a studijních programů zaměřených na kybernetickou bezpečnost, a na vytvoření profesních kvalifikací pro kybernetickou bezpečnost,
g) podílí se ve spolupráci s Ministerstvem práce a sociálních věcí České republiky na zvýšení podpory a kapacity systému rekvalifikací v oblasti kybernetické bezpečnosti,
h) zajišťuje v souladu se zákonem o uznávání výsledků dalšího vzdělávání, roli autorizačního orgánu pro povolání v oblasti kybernetické bezpečnosti,

i) provádění kontroly autorizovaných osob a s ní související úkony a spolupráci s odborem právním na projednávání přestupků vyplývající z kontroly a ukládání nápravných opatření ve správním řízení navazujícím na výkon kontroly,
j) organizuje cvičení kybernetické bezpečnosti na národní úrovni a podílí se na přípravách cvičení na mezinárodní úrovni, kdy přispívá k plnění úkolů Úřadu, které vyplývají z členství České republiky v NATO a EU a případně dalších mezinárodních dohod,
k) koordinuje zapojení zaměstnanců příslušných celků Úřadu do exekuce cvičení (zejména těch mezinárodních), koordinuje zapojení expertů z ostatních partnerských národních organizací a institucí do mezinárodních cvičení,
l) poskytuje podporu regulovaným subjektům a partnerům v oblasti příprav jejich vlastních cvičení kybernetické bezpečnosti, organizuje a obsahově se podílí na školeních a workshopech v rámci konceptu train-the-trainer pro zájemce z řad regulovaných subjektů a partnerů,
m) kontinuálně rozvíjí koncept cvičení a tréninků kybernetické bezpečnosti na základě nejnovějších trendů a poznatků v oboru a s využitím zjištění z proběhlých cvičení aktivně vyhledává a rozvíjí možnosti spolupráce se zahraničními partnery v relevantních oblastech,
n) sdílí poznatky ze cvičení a osvětových aktivit s ostatními celky Úřadu,
o) plní další pracovní úkoly uložené náměstkem ředitele.

(4) Oddělení vzdělávání plní úkoly uvedené v odstavci 3 písm. a) až i).

(5) Oddělení cvičení plní úkoly uvedené v odstavci 3 písm. j) až m).

Čl. 39
Odbor mezinárodní spolupráce a Evropské unie

(1) Odbor mezinárodní spolupráce a Evropské unie, v jehož čele stojí ředitel odboru, se člení na

a) oddělení multilaterální spolupráce I,
b) oddělení multilaterální spolupráce II a
c) oddělení bilaterální spolupráce.

(2) Dalšími vedoucími zaměstnanci odboru mezinárodní spolupráce a Evropské unie jsou

a) vedoucí oddělení multilaterální spolupráce I,
b) vedoucí oddělení multilaterální spolupráce II,
c) vedoucí oddělení bilaterální spolupráce,

kteří jsou vedoucími zaměstnanci 1. stupně řízení.

(3) Odbor mezinárodní spolupráce a Evropské unie zejména plní tyto úkoly

a) aktivně usiluje o rozvoj mezinárodní spolupráce v oblasti působnosti Úřadu,
b) navazuje, udržuje a rozvíjí kontakty se zahraničními partnery, shromažďuje a zpracovává o nich informace s cílem jejich optimálního využití v rámci Úřadu,
c) stanovuje a průběžně vyhodnocuje priority pro bilaterální spolupráci Úřadu se zahraničními partnery,
d) koordinuje a v součinnosti s relevantními celky Úřadu připravuje podklady pro jednání se zahraničními partnery na úrovni vedení Úřadu,
e) připravuje, koordinuje a prosazuje pozice ČR k návrhům právních úprav EU a při klíčových jednáních v EU, jiných mezinárodních organizacích i bilaterálně,
f) koordinuje a podílí se na plnění úkolů Úřadu, které vyplývají z členství České republiky v EU a NATO,

g) zajišťuje plnění informačních povinností a dalších závazků vůči Evropské komisi a jiným orgánům zřizovaným předpisy Evropské unie v oblasti kybernetické bezpečnosti,
h) v rámci Úřadu zpracovává nebo koordinuje zpracování dokumentů podléhajících projednání ve Výboru pro Evropskou unii podřízeném vládě České republiky a odpovídá za jejich projednání v resortní koordinační skupině,
i) podílí se, ve spolupráci s příslušnými národními gestory, na mezinárodní spolupráci v ostatních mezinárodních organizacích (zejména OSN, OBSE, ITU, OECD),
j) koordinuje aktivity Úřadu v oblasti mezinárodní rozvojové spolupráce (*Cyber Capacity Building),*
k) účastní se relevantních koordinačních jednání Ministerstva zahraničních věcí v otázkách kybernetické bezpečnosti a zahraničně-bezpečnostní politiky,
l) shromažďuje, třídí a zpracovává informace v souvislosti se zahraničními styky Úřadu (zejména zápisy z jednání, zprávy a zápisy z pracovních cest, cizozemské právní předpisy) a poskytuje je na vyžádání k využití organizačním celkům Úřadu,
m) přijímá a vyhodnocuje informace o aktivitách Úřadu ve vztahu k zahraničí, poskytované organizačními celky Úřadu,
n) přispívá k šíření osvěty široké veřejnosti v oblasti působení České republiky v mezinárodních organizacích ve věcech kybernetické bezpečnosti,
o) s výjimkou případů spadajících do věcné působnosti jiných organizačních celků koordinuje program zahraničních návštěv, ve vhodných případech v součinnosti s Kabinetem ředitele,
p) podílí se na přípravě interních aktů řízení,
q) v součinnosti se Sekcí personalistiky, práva a provozu koordinuje, organizuje a řídí proces vysílání zaměstnanců Úřadu do zahraničí jakožto Cyber attaché nebo národních expertů, nebo za účelem krátkodobých stáží, pracovních výměnných pobytů a dalších pracovně-vzdělávacích aktivit,
r) koordinuje, zařizuje a administrativně pokrývá možnost vzdělávání zaměstnanců v zahraničních kurzech, zejména EU a NATO, a to v součinnosti s dalšími relevantními celky,
s) přispívá k tvorbě a propagaci pozice ČR k výkladu aplikace mezinárodního práva v kyberprostoru,
t) přispívá ke správné implementaci unijního a mezinárodního práva,
u) koordinuje úkoly Úřadu při sjednávání mezinárodních smluv a právně nezávazných dokumentů o spolupráci a v souvislosti s jejich prováděním, včetně koncepcí, přípravy podkladových materiálů, realizace expertních jednání, zajišťování vnitrostátního procesu schvalování a publikace,
v) poskytuje odboru cvičení a vzdělávání konzultace ke cvičením kybernetické bezpečnosti a těchto cvičení se účastní na národní i mezinárodní úrovni,
w) spolupracuje s dalšími organizačními celky na zajištění připravenosti Úřadu v případě kybernetických krizí a krizových situací a přispívá ke koordinaci jejich řešení, zejména zastupováním v relevantních orgánech EU a NATO, které se kybernetickým krizovým řízením zabývají,
x) podílí se na přípravě Prague Cyber Security Conference zejména připravuje a realizuje program a po obsahové stránce zajišťuje bilaterální jednání,
y) plní další pracovní úkoly uložené náměstkem ředitele.

(4) Oddělení multilaterální spolupráce 1 plní zejména úkoly uvedené v odstavci 3 písm. a), b), e), f), g), h), i), k), s), t) a u).

(5) Oddělení multilaterální spolupráce 2plní zejména úkoly uvedené v odstavci 3 písm. a), b), e), f), g), h), k), s), t), u) a w).

(6) Oddělení bilaterální spolupráce plní zejména úkoly uvedené v odstavci 3 písm. a), b), c), d), e), j), l), m), n), o).

Čl. 40
Oddělení národních strategií a politik

(1) V čele oddělení národních strategií a politik stojí vedoucí oddělení, který je vedoucím zaměstnancem 1. stupně řízení.

(2) Oddělení národních strategií a politik zejména

a) vyhodnocuje trendy v oblasti kybernetické bezpečnosti a na jejich základě připravuje strategie a politiky v oblasti kybernetické bezpečnosti a vyhodnocuje jejich plnění,
b) připravuje pro ředitele Úřadu podklady ke koncepcím, strategiím, politikám a trendům v oblasti kybernetické bezpečnosti,
c) zpracovává koncepce návrhů právních úprav, interních aktů řízení Úřadu a materiálů nelegislativní povahy předkládaných vládě České republiky a jejím orgánům,
d) zpracovává věcná stanoviska k výzkumu a vývoji v oblasti kybernetické bezpečnosti,
e) podílí se na budování komunity expertů v oblasti kybernetické bezpečnosti, včetně organizace odborných setkání a konferencí,
f) podílí se na organizaci a účastní se cvičení kybernetické bezpečnosti a poskytuje k nim odboru cvičení a vzdělávání konzultace,
g) vykonává publikační a přednáškovou činnost v oblasti koncepcí, strategií, politik a trendů kybernetické bezpečnosti,
h) poskytuje právní poradenství a připravuje právní stanoviska sekci strategických agend a spolupráce v oblasti koncepcí, strategií, politik a trendů kybernetické bezpečnosti a odboru vládní CERT v celém rozsahu jeho působnosti,
i) podílí se na tvorbě obsahu k Portálu NÚKIB,
j) podílí se na přípravě a realizaci konference CyberCon, zejména sestavuje koncepci a určuje směřování konference a strukturu účastníků a odpovídá za programovou část,
k) plní další pracovní úkoly uložené náměstkem ředitele.

Čl. 41
Oddělení vědy, výzkumu a inovací

(1) V čele oddělení výzkumu, vývoje a inovací stojí vedoucí oddělení, který je vedoucím zaměstnancem 1. stupně řízení.

(2) Oddělení vědy, výzkumu a inovací zejména

a) řídí a koordinuje výzkum a vývoj Úřadu,
b) vypracovává a naplňuje ve spolupráci s organizačními celky Úřadu cíle Národního plánu výzkumu a vývoje v oblasti kybernetické a informační bezpečnosti a dalších koncepčních dokumentů,
c) zodpovídá za plnění úkolů dle článku č. 7 Nařízení Evropského Parlamentu a Rady (EU) 2021/887, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center,

d) poskytuje koordinační, metodickou a administrativní podporu při zapojování Úřadu do výzkumných projektů financovaných prostřednictvím veřejné podpory na výzkum, vývoj a inovace a programů Evropské komise Horizont Evropa a Digitální Evropa,
e) posuzuje a schvaluje v rámci své působnosti výsledky projektů financovaných z prostředků veřejné podpory na výzkum, vývoj a inovace.

ČÁST ČTVRTÁ

VZTAHY ÚŘADU K ZAHRANIČNÍM PARTNERŮM

Čl. 42

Vztahy Úřadu k zahraničním partnerům vyplývají z jeho působnosti a postavení a uskutečňují se zejména s

a) příslušnými úřady cizích států, odpovědnými za kybernetickou bezpečnost a za vybrané oblasti ochrany utajovaných informací,
b) orgány NATO, EU a dalších mezinárodních organizací, jichž je Česká republika členem,
c) patentovými úřady cizích států.

ČÁST PÁTÁ

SPOLEČNÁ, ZRUŠOVACÍ A ZÁVĚREČNÁ USTANOVENÍ

Čl. 43

(1) V rámci organizační struktury ředitel Úřadu zřizuje a ruší organizační celky, pracovní skupiny a zvláštní týmy složené ze zaměstnanců z různých organizačních celků.

(2) Organizovat, řídit a kontrolovat práci zaměstnanců zařazených v pracovních skupinách a týmech a dávat jim k tomu účelu závazné pokyny, je oprávněn rovněž zaměstnanec, který není vedoucím zaměstnancem podle čl. 5 odst. 2, ale je k těmto činnostem pověřen.

(3) Platné interní normativní akty Úřadu budou vykládány s přihlédnutím k organizační změně dle Rozhodnutí ředitele Úřadu „O provedení organizační změny“.

(4) V případě kompetenčního sporu o tom, kterému organizačnímu celku náleží věc do působnosti, rozhodne s konečnou platností náměstek Sekce personalistiky, práva a provozu. V případech, kdy je jednou ze stran kompetenčního sporu Sekce personalistiky, práva a provozu, určí rozhodce ředitel Úřadu dle vlastního uvážení tak, aby byla zachována neutralita rozhodování.

Čl. 44

(1) Vedoucí zaměstnanci zodpovídají za optimální nastavení kontrolního systému včetně identifikace rizik a přijetí opatření k jejich vyloučení nebo zmírnění, jsou povinni průběžně zjišťovat, posuzovat, usměrňovat a vyhodnocovat všechna rizika spojená s činností jimi řízeného organizačního celku, plnit funkci příkazců operací v určeném rozsahu své působnosti podle této směrnice a dalších interních aktů řízení a zajišťovat výkon předběžné, průběžné a následné řídící kontroly při hospodaření s finančními prostředky.

(2) Organizační celky, mezi nimiž není vztah nadřízenosti a podřízenosti, jsou povinny při vyřizování své agendy mezi sebou spolupracovat. V případě kompetenčního sporu ředitel Úřadu určí organizační celek odpovědný za splnění úkolu.

Čl. 45

(1) Vedoucí zaměstnanci jsou povinni v době své nepřítomnosti zajistit řádný chod jimi řízeného organizačního celku.

(2) Vedoucí zaměstnanci odpovídají za vypracování popisů pracovních činností u přímo podřízených zaměstnanců.

(3) Vedoucí zaměstnanci mohou pověřit některého z podřízených zaměstnanců organizováním, řízením a kontrolou práce jiných zaměstnanců, včetně oprávnění dávat jim k tomu účelu závazné pokyny.

Čl. 46
Přílohy

Nedílnou součástí tohoto Organizačního řádu jsou přílohy:

Příloha č. 1 – Organizační schéma Úřadu
Příloha č. 2 – Číselník organizačních celků Úřadu se zavedenou zkratkou celku

Čl. 47
Zrušovací ustanovení

Tato směrnice ruší směrnici ředitele Národního úřadu pro kybernetickou a informační bezpečnost č. S14/2025 „Organizační řád“.

Čl. 48
Účinnost

Tato směrnice nabývá účinnosti dnem 1. července 2026.

Ing. Lukáš Kintr

ředitel Národního úřadu pro kybernetickou a informační bezpečnost

Příloha – Organizační struktura

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Ředitel: Ing. Lukáš Kintr

Sekce personalistiky, práva a provozu

- Odbor právní

Zajišťuje kompletní právní servis pro provozní činnosti Úřadu a zabezpečuje plnění rozličných povinností vyplývajících z postavení Úřadu jakožto ústředního správního orgánu. Odbor právní je zároveň administrátorem výběrových a zadávacích řízení na veřejné zakázky, což zahrnuje mimo jiné i tvorbu a evidenci smluvní dokumentace. V neposlední řadě odbor právní zodpovídá za řízení o přestupcích v rozsahu působnosti svěřené Úřadu, resp. zastřešuje i další správní řízení vedená Úřadem.

  - Oddělení právní a přestupkové agendy
  - Oddělení právní agendy a dvoustupňového rozhodování
  - Oddělení veřejných zakázek
  - Pověřenec pro ochranu osobních údajů

- Odbor provozně ekonomický (OPE)
  - Oddělení investic

  Zadává a vede tvorbu investičních projektů a zajišťuje jejich realizaci. Předkládá návrhy na stavební činnost a opravy investičního charakteru majetku Úřadu a tyto navrhuje do rozpočtu příslušného roku. Připravuje a zajišťuje projektovou dokumentaci včetně projednání pro jednotlivé akce a to v rámci předprojektové, projektové a realizační činnosti. Podává jménem Úřadu žádosti o územní rozhodnutí a stavební povolení a ostatní nutná povolení související s realizací projektů. Připravuje a realizuje stavby a opravy majetku města investičního charakteru, které budou realizovány na základě stavebního povolení. Vykonává funkci investora na stavbách všeho druhu, které připravil a které realizuje. Zajišťuje všechny náležitosti spojené s uvedením staveb do provozu.

  - Oddělení rozpočtu

Oddělení rozpočtu zajišťuje přípravu návrhu rozpočtu kapitoly rozpočtu 378-NÚKIB, příprava návrhu střednědobého výhledu a návrhu závěrečného účtu této kapitoly, včetně zpracování podkladů dodávaných od věcně příslušných organizačních celků a sledování jeho čerpání. Dále je to podílení se na plnění úkolů funkce finančního manažera při financování projektů Úřadu, provádění rozpisu rozpočtu Úřadu na daný rozpočtový rok a v souladu se zákonem č. 320/2001 Sb., o finanční kontrole, v platném znění, plní funkci správce rozpočtu kapitoly 378-NÚKIB. Do náplně oddělení rozpočtu také náleží funkce zastupování Úřadu před Ministerstvem financí a odpovědnost za ekonomické výstupy Úřadu předávané ISSP a na Ministerstvo financí.

- Oddělení účetnictví

Oddělení účetnictví zajišťuje pro věcně příslušné organizační celky účtování správních poplatků a pokut v působnosti Úřadu, organizuje a metodicky usměrňuje inventarizaci majetku. V souladu se zákonem č. 320/2001 Sb., o finanční kontrole, plní funkci hlavní účetní kapitoly 378-NÚKIB. Dále zabezpečuje provádění účetní uzávěrky za daná účetní období, odpovědnost za účetní výstupy Úřadu, zajišťuje chod pokladny Úřadu, agendu tuzemských i zahraničních pracovních cest (ZPC) v rozsahu daném interními normativními akty, agendy související se ZPC a zajišťuje platební styk – bezhotovostní, hotovostní, zprostředkovává styk s bankami a agendu platebních karet ve spolupráci s ČNB.

- Oddělení provozu a služeb

Koordinuje a zabezpečuje materiálně technické zabezpečení Úřadu vyjma prostředků informační a komunikační techniky, vede evidenci movitého a nemovitého majetku Úřadu a provádí jeho inventarizaci. Dále koordinuje a zabezpečuje služby spojené se správou nemovitého majetku, podílí se na koordinaci provozu v objektech Úřadu, zajišťuje styk s vnějšími organizacemi ve správě budov (dodávky energií, vody, plynu, tepla atd.) a zajišťuje revizní zprávy na technologická zařízení. Dozoruje nad údržbou veškerého majetku. Zajišťuje provoz a servis služebních automobilů.

    - Pracovní skupina autoprovozu

- Oddělení personálních věcí a vzdělávání

Vykonává činnosti v oblasti personalistiky, vzdělávání, platové a sociální politiky v souladu se zákoníkem práce a prováděcích předpisů. Kontroluje dodržování pracovněprávních předpisů a zajišťuje evidenci zaměstnanců. Vede přijímací řízení s uchazeči o zaměstnání. Zabezpečuje stáže pro studenty vysokých škol. Podílí se na vytváření pracovně právních předpisů a interních aktů řízení.

- Odbor plánování, řízení a fondů
    - Oddělení plánování a řízení
    - Oddělení projektová kancelář

Zajišťuje efektivní řízení širokého portfolia projektů NÚKIB v průběhu celého životního cyklu. Naplňuje tyto funkce: podílí se přímo na realizaci a řízení projektů, popř. projektům asistuje metodicky. Vydává závazné pokyny i metodické materiály pro organizaci, pomáhá ověřovat kvalitu řízení projektů. Zajišťuje a podporuje vzdělávání v oblasti projektového řízení.

- Pracovní skupina EU fondů

Podílí se na tvorbě politiky ČR v oblasti spolufinancování kybernetické bezpečnosti z EU-fondů. Asistuje ve využití příležitostí čerpání prostředků z EU – vlastní organizaci i za její hranice.

Odbor bezpečnosti

- Oddělení spisové a archivní služby

Zajišťuje v rámci Úřadu činnosti podatelny a spisovny, registru utajovaných informací, specializovaného a bezpečnostního archivu. Dále v rámci Úřadu metodicky řídí spisovou službu, podílí se na vytváření interních aktů řízení a dalších dokumentů v oblasti spisové služby a ochrany utajovaných informací, podílí se na provádění kontrol spisové služby a dodržování zásad ochrany utajovaných informací.

- Oddělení fyzické bezpečnosti

Zajišťuje v rámci Úřadu zabezpečení ochrany utajovaných informací z pohledu fyzické bezpečnosti v souladu s podmínkami stanovenými legislativními předpisy, zvláště pak zákona č. 412/2005 Sb., o ochraně ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů a Vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Podílí se na tvorbě projektů fyzické bezpečnosti, vytváří bezpečnostní interní dokumenty a vyjadřuje se k bezpečnostní a projektové dokumentaci při rekonstrukčních a stavebních realizacích objektů Úřadu. Řídí a zabezpečuje činnosti při mimořádných bezpečnostních událostech. Spravuje systémy technické ochrany, přístupové a klíčové systémy. Řeší bezpečnostní incidenty a provádí kontrolní činnost v oblasti fyzické bezpečnosti. Spolupracuje s Ochrannou službou Policie České republiky při výkonu ochrany objektů Úřadu.

- Oddělení informační bezpečnosti

Vykonává bezpečnostní správu informačních a komunikačních systémů nakládajících s utajovanými informacemi Úřadu, vede jejich dokumentaci a evidenci dle příslušné legislativy. Zajišťuje plánování a rozvoj informačních a komunikačních systémů Úřadu nakládajících s utajovanými informacemi a ověřuje podmínky pro provoz a soulad s požadavky na jejich certifikaci. Spolupracuje s manažerem a architektem kybernetické bezpečnosti, kterým poskytuje součinnost v oblasti kybernetické bezpečnosti.

- Oddělení personální bezpečnosti a krizového řízení

Vykonává a zajišťuje připravenost Úřadu na řešení krizových situací ve spolupráci s ostatními organizačními celky Úřadu. Reaguje na aktuální krizové stavy a podílí se na tvorbě legislativy v oblasti krizového řízení v rámci Úřadu. Účastní se meziresortních jednání a iniciativ v oblasti krizového řízení a podílí se na jejich implementaci do praxe. Zajišťuje a provádí činnosti na úseku personální bezpečnosti v rozsahu stanoveném zákonem a interními akty.

- Architekt kybernetické bezpečnosti
- Manažer kybernetické bezpečnosti

Sekce strategických agend a spolupráce

- Odbor mezinárodní spolupráce a Evropské unie
  - Oddělení multilaterální spolupráce I a II

  Zajišťují v působnosti Úřadu agendy EU a NATO, agendu jiných mezinárodních organizacích jako OSN, OECD, OBSE nebo ITU, rozvojovou spolupráci a řešení otázek mezinárodního práva veřejného. Připravují, koordinují a prosazují pozice ČR k návrhům právních úprav EU a při klíčových jednáních v EU. Dále koordinují úkoly Úřadu při sjednávání mezinárodních smluv a právně nezávazných dokumentů o spolupráci a v souvislosti s jejich prováděním.

  - Oddělení bilaterální spolupráce

  Udržuje a rozvíjí bilaterální spolupráci s partnery Úřadu a stanovuje priority pro tato jednání. Vede evidenci o jednáních se zahraničními partnery a vyhodnocuje je. Připravuje a koordinuje přípravu podkladů pro ředitele Úřadu a poskytuje mu podporu při jednáních. Ve spolupráci s ostatními organizačními celky se podílí na přípravách a organizaci mezinárodních akcí.

- Odbor cvičení a vzdělávání
  - Oddělení cvičení

  Zabývá se koordinací a přípravou širokého spektra technických a netechnických cvičení kybernetické bezpečnosti na národní i mezinárodní úrovni (např. Cyber Czech, Cyber Coalition, Locked Shields, CMX). Velkou část agendy tvoří příprava cvičení kybernetické bezpečnosti, která jsou zaměřená na regulované subjekty a partnerské instituce, včetně cvičení zaměřených na celé sektory a odvětví. Stejně tak se oddělení podílí na dalších aktivitách jako například přednáškové činnosti či konzultacích cvičení pro výše zmíněné subjekty.

  - Oddělení vzdělávání

  Zajišťuje vzdělávací a osvětové aktivity, pořádá konference a školení na téma kybernetické bezpečnosti, připravuje a provozuje tematické e-learningové kurzy. Primární cílovou skupinou vzdělávání jsou zaměstnanci veřejné správy a další osoby, které zastávají role

podle Zákona o kybernetické bezpečnosti. Sekundární cílovou skupinu tvoří osoby identifikované jako „zranitelné v kyberprostoru“. Jsou jimi žáci a studenti všech stupňů vzdělávání a senioři. Oddělení ve velké míře spolupracuje s dalšími rezorty a klíčovými hráči v oblasti vzdělávání, kdy je podporuje při šíření osvěty v oblasti kybernetické bezpečnosti a podílí se na společných aktivitách. Oddělení rovněž plní roli autorizačního orgánu pro povolání v oblasti kybernetické bezpečnosti (v souladu se zákonem č. 179/2006 Sb., o ověřování a uznávání výsledků dalšího vzdělávání a o změně některých zákonů).

- Odbor centrální analytiky
  - Oddělení strategických analýz

Provádí analýzu a monitoring kybernetických hrozeb, rizik a aktuálních trendů v kybernetické bezpečnosti. Posuzuje jejich politický a bezpečnostní kontext či dopady incidentů. V návaznosti na to poskytuje analytickou podporu v rámci NÚKIB, rozhodujícím činitelům v české státní správě a zahraničním partnerům. Ve spolupráci s CERT rozvíjí pokročilou analytickou kapacitu v podobě Cyber Threat Intelligence (CTI).

  - Oddělení informačního šetření

Na základě zpravodajství z otevřených zdrojů (OSINT) poskytuje analytickou podporu příslušným organizačním celkům. Dále též poskytuje analytickou podporu externím partnerům v rámci úzce vymezených agend.

  - Oddělení správy a analýzy dat

Poskytuje dalším organizačním celkům podporu v podobě datové analýzy nebo vývoje, správy a poskytování datových a analytických nástrojů.

- Oddělení národních strategií a politik

Zabývá se přípravou dlouhodobé strategie a poskytuje analýzu, a potřebnou expertízu, včetně věcných i právních doporučení k zajištění, aby NÚKIB, potažmo ČR plnila všechny stanovené cíle v oblasti zajišťování kybernetické bezpečnosti, a to co nejefektivnějším způsobem. Podílí se na tvorbě kybernetických bezpečnostních politik a zajišťuje jejich efektivní koordinaci a harmonizaci napříč veřejnou sférou a dalšími subjekty. Mimo jiné usiluje o budování koherentní národní komunity kybernetické bezpečnosti v ČR a intenzivně spolupracuje s partnery ze státní i soukromé sféry na národní i mezinárodní úrovni.

- Oddělení vědy, výzkumu a inovací

Zabývá se koordinací výzkumných a inovačních aktivit v oblasti kybernetické a informační bezpečnosti. Vytváří Národní plán výzkumu a vývoje v kybernetické a informační bezpečnosti a ve spolupráci s partnery realizuje kroky k jeho naplňování. Provozuje Národní koordinační centrum dle Nařízení Evropského parlamentu a Rady 2021/887, kterým se zřizuje Evropské průmyslové,

technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center. Zapojuje se do řešení výzkumných projektů a podněcuje účast výzkumné komunity na přeshraničních projektech.

Sekce informačních systémů

- Odbor bezpečnosti informačních a komunikačních technologií

  - Oddělení vývoje kryptografických prostředků

  Provádí a zabezpečuje základní a aplikovaný výzkum a vývoj v oblasti kryptografie, kryptoanalýzy a kryptografických prostředků, vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany. Dále zabezpečuje vývoj kryptografických schémat pro použití v kryptografických prostředcích ochrany utajovaných informací (UI), provádí analýzy a hodnocení šifrových systémů a kryptografických algoritmů určených k ochraně UI a podílí se na zajišťování veřejných zakázek Úřadu v oblasti výzkumu, vývoje a výroby kryptografických prostředků.

  - Oddělení certifikací informačních a komunikačních systémů

  Plní úkoly Národního střediska pro bezpečnost informačních systémů, provádí certifikaci informačních systémů používaných k nakládání s utajovanými informacemi (UI), schvaluje projekty bezpečnosti komunikačních systémů používaných k nakládání s UI, zajišťuje plnění úlohy Úřadu jako orgánu pro bezpečnostní akreditaci informačních systémů nakládajících s UI pro NATO a EU a jiné mezinárodní organizace, provádí hodnocení informačních systémů nakládajících s UI NATO a EU a jiných mezinárodních organizací, provádí styk s orgány NATO a EU a jiných mezinárodních organizací pro zajištění akreditace informačních systémů a průběžnou kontrolní činnost v akreditovaných systémech podle požadavků NATO a EU a jiných mezinárodních organizací.

  - Oddělení certifikací kryptografických prostředků a pracovišť

  Zabezpečuje a provádí certifikaci kryptografických prostředků (KP) a stanovuje bezpečnostní standardy v oblasti certifikace KP, provádí certifikaci kryptografických pracovišť (KPr) a stanovuje bezpečnostní standardy v oblasti certifikace KPr. Ověřuje a schvaluje implementaci a zasazení kryptografických prostředků. Schvaluje způsobilost materiálu k zajištění funkce KP, schvaluje projekty zástavby KP do mobilních a dočasně rozmístitelných systémů. Provádí styk s orgány NATO, EU a jiných mezinárodních organizací pro zajištění mezinárodní certifikace (schválení) KP těmito organizacemi. Podílí se na výkonu kontroly ve vybraných oblastech ochrany utajovaných informací v rámci České republiky. Podílí se, případně vykonává inspekce NATO a EU v oblasti kryptografické ochrany utajovaných informací. Podílí se na ověřování a schvalování způsobilosti kryptografických pracovišť pro manipulaci s kryptografickým materiálem EU. Zabezpečuje a provádí ověřování odborné

způsobilosti pracovníků kryptografické ochrany (zkoušky zvláštní odborné způsobilosti). Provádí metodickou a poradní činnost v oblasti kryptografické ochrany utajovaných informací.

- Oddělení TEMPEST

Plní úkoly Národního střediska pro měření kompromitujícího elektromagnetického vyzařování, provádí analýzy a hodnocení elektrických a elektronických zařízení z hlediska úniku utajovaných informací (UI) prostřednictvím elektromagnetického vyzařování, provádí zónové hodnocení prostorů určených pro zpracování UI, certifikaci stínících komor určených k ochraně UI, analýzy a hodnocení kryptografických prostředků z hlediska ochrany proti kompromitujícímu vyzařování, kontrolu, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací.

- Oddělení kryptografických analýz
- Oddělení odborné podpory
- Oddělení Národní distribuční středisko

Zajišťuje a plní úkoly Národního střediska pro distribuci kryptografického materiálu (NDA), zabezpečuje a provádí ověřování odborné způsobilosti pracovníků kryptografické ochrany (zkoušky zvláštní odborné způsobilosti) a vydává osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany, zajišťuje a provádí výrobu klíčových materiálů pro provoz kryptografických prostředků distribuci klíčových materiálů a kryptografických prostředků, zajišťuje servis a údržbu speciálních zařízení pro výrobu klíčových materiálů a kryptografických prostředků.

    - Pracovní skupina CDA

- Odbor informačních technologií

- Oddělení síťové infrastruktury a dohledu

Zabývá se systémovou podporou aplikací ERP, Personalistiky, mezd a Spisové služby. Zabezpečuje instalaci systémů, uživatelskou podporu, správu, optimalizaci a údržbu databází pro výše uvedené systémy. Řeší strategické a rozvojové záměry v oblasti informačních systémů (JIS, nové lokality, GDPR, atd.). Provozuje Registrační certifikační autoritu pro x509 zaměstnanecké certifikáty. Vydává serverové x509 certifikáty (CESNET) a certifikáty pro FW (sondy). Realizuje a aktualizuje DRP plán klíčových aplikací.

    - Pracovní skupina provozního dohledu

- Oddělení serverové infrastruktury

Zabývá se instalací, přípravou, správou a optimalizací serverové infrastruktury. Dále se zabývá správou virtualizačního prostředí, poštovních služeb, datových úložišť a též správou fyzického

serverového vybavení, udržuje též v provozu interně vyvinuté nástroje pro zabezpečenou komunikaci. Udržuje veškeré možné komunikační cesty úřadu.

- Oddělení podpory aplikací a rozvoje
- Oddělení klientské podpory

Zabývá se podporou uživatelů v oblasti IT. Řeší problémy s hardwarem i softwarem koncových stanic a příslušenství uživatelů. Zabezpečuje nákup potřebného IT vybavení. Předává podklady pro evidenci majetku.

    - Pracovní skupina speciálních prostředků

- Oddělení plánování, ekonomiky a logistiky v IT

- Oddělení bezpečnosti satelitních služeb

Zodpovídá za implementaci a provoz veřejně regulované služby (PRS) systému Galileo v ČR a koordinuje veškeré aktivity spojené s přístupem k informacím a technologiím PRS. V souladu s platnou evropskou legislativou (1104/2011/EU) plní funkci Příslušného orgánu PRS (Competent PRS Authority), přičemž zejména zodpovídá za organizaci přístupu a přidělení přístupových práv oprávněným uživatelům, ochranu a distribuci utajovaných informací PRS, zpracování provozních a bezpečnostních předpisů pro využití PRS a vyhodnocení potenciálních rizik pro PRS, včetně definování příslušných nápravných a preventivních opatření. Je kontaktním místem pro trvalé spojení s bezpečnostním střediskem PRS, kterému oznamuje všechny bezpečnostní incidenty narušující bezpečnost PRS a rušivé elektromagnetické interference na frekvencích vyhrazených pro PRS.

Sekce Národního centra kybernetické bezpečnosti (NCKB)

- Odbor vládní CERT (GovCERT)
    - Oddělení Incident Handling
    - Pracovní skupina Threat Intelligence and Information Sharing
    - Oddělení analýzy kybernetických incidentů
        - Pracovní skupina Threat Hunting
    - Oddělení penetračního testování

Specializuje se na identifikaci a zlepšení bezpečnostních aspektů pomocí technik penetračního testování. Hlavním cílem je zajištění odolnosti vůči potenciálním kybernetickým hrozbám a bezpečnostním rizikům. K dosažení těchto cílů odborníci z Oddělení penetračního testování provádí praktické prověření zabezpečení pomocí simulovaných kybernetických

útoků). V současné době jsou nabízeny služby externích a interních penetračních testů, wifi sítí, phishingové a vishingové kampaně, fyzické testy, testy zahlcení (dos), a po domluvě také nestandardní testy specifických zařízení nebo konzultace k nasazení nových technologií.

- Pracovní skupina testování síťových služeb, zranitelností a operačních technologií

Zaměřuje se na interní penetrační testy a testování služeb vyskytujících se v síťových infrastrukturách. Hlavním cílem je identifikace možných slabiny, které by mohly být využity útočníky po získání přístupu do vnitřních sítí organizací.

- Oddělení bezpečnosti operačních technologií

Zabývá se problematikou kybernetické bezpečnosti průmyslově orientovaných technologií a řídících systémů, které jsou součástí nejen určené Kritické infrastruktury ČR. Podílí se na procesu regulace a kontroly subjektů provozujících operační technologie. V souvisejících oblastech jsou otevřeni k technickým konzultacím.

- Oddělení DevSecOps

Hlavní agendou oddělení DevSecOps (Development Security Operations) je vývoj, nasazení a zabezpečení aplikací, přičemž je kladen důraz na použití nejmodernějších technologií. Tyto činnosti jsou vykonávány jak pro vnitřní potřebu odboru Vládní CERT, tak i pro potřeby spolupráce s externími subjekty. Odborníci oddělení DevSecOps také ve velké míře zajišťují technickou část kontrol povinných subjektů dle Zákona o kybernetické bezpečnosti. Dále aktivně participují na tvorbě nových metodik a standardů a posuzování bezpečnosti cloudových služeb a poskytovatelů.

- Pracovní skupina pro rozvoj a správu Portálu NÚKIB
- Pracovní skupina aplikační bezpečnosti

- Odbor regulace

Zabývá se problematikou upravenou zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a zároveň oblastí EU certifikací kybernetické bezpečnosti obsažené v nařízení (EU) č. 2019/881, aktu o kybernetické bezpečnosti. Na každodenní bázi komunikuje s regulovanými subjekty, ať už ve věci regulace, EU certifikací nebo poskytování metodické podpory. Podílí se na přípravě legislativy v oblasti kybernetické bezpečnosti, včetně návrhu certifikačních schémat. Hraje klíčovou roli při určování a ochraně kritické informační infrastruktury, významných informačních systémů a systémů základních služeb v rámci České republiky. V oblasti EU certifikací kybernetické bezpečnosti (dále jen EU certifikace KB) pak v souladu s aktem o kybernetické bezpečnosti plní úlohu vnitrostátního orgánu certifikace kybernetické bezpečnosti.

- Oddělení regulace soukromého sektoru

Zajišťuje určování provozovatelů základních služeb. Aplikuje, udržuje a vykládá vyhlášku č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. Zajišťuje určování kritické informační infrastruktury v soukromém sektoru. Poskytuje výklad a podporu v oblasti regulace soukromého sektoru. Komunikuje s příslušnými regulátory.

- Oddělení regulace veřejného sektoru

Zajišťuje identifikaci významných informačních systémů. Aplikuje, udržuje a vykládá vyhlášku č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Zajišťuje určování kritické informační infrastruktury ve veřejném sektoru. Poskytuje výklad a podporu v oblasti regulace veřejného sektoru. Komunikuje s příslušnými regulátory.

- Oddělení regulace dodavatelů informačních technologií

Zajišťuje posuzování nabídek cloud computingu podle zákona o informačních systémech veřejné správy a zákona o kybernetické bezpečnosti. Aplikuje, udržuje a vykládá tzv. cloudové vyhlášky. Konzultuje posuzování dopadů narušení systémů pro účely procesů cloud computingu u orgánů veřejné moci. Poskytuje výklad a podporu v oblasti regulace využívání cloud computingových služeb orgány veřejné moci. Komunikuje s příslušnými regulátory.

  - Pracovní skupina bezpečnosti dodavatelského řetězce

- Pracovní skupina Evropských certifikací

V roli vnitrostátního orgánu certifikace kybernetické bezpečnosti dohlíží na dodržování pravidel zahrnutých v evropských schématech certifikace KB a tato pravidla vymáhá. Má za úkol v příslušných případech autorizovat subjekty posuzování shody a delegovat vydávání EU certifikátů KB. Řeší stížnosti související s EU certifikáty KB. Zastupuje ČR v rámci Evropské skupiny pro certifikaci KB. Poskytuje výklad a podporu v oblasti EU certifikací KB. Komunikuje s příslušnými stakeholdery.

- Odbor kontroly

Provádí kontroly dodržování požadavků zákona o kybernetické bezpečnosti u regulovaných subjektů. Současně s odborem regulace se podílí na přípravě legislativy v oblasti kybernetické bezpečnosti a poskytuje metodickou podporu regulovaným subjektům. Dále na kontrolní činnosti spolupracuje s dalšími kontrolními orgány, jejichž kontrolní činnost má přesah do oblasti kybernetické bezpečnosti.

- Oddělení kontroly 1
- Oddělení kontroly 2
- Oddělení kontroly 3

- **Odbor Kabinet ředitele (OKŘ)**

- Oddělení komunikace
- Oddělení vládní agendy a legislativy

Koordinuje a realizuje pravomoci Úřadu v legislativním procesu a poskytuje výkladová stanoviska k právním předpisům v působnosti Úřadu. Zastřešuje přípravu nelegislativních materiálů předkládaných vládě, Bezpečnostní radě státu, Výboru pro kybernetickou bezpečnost nebo jiným orgánům státu, popřípadě tyto materiály zpracovává samostatně. Dále zajišťuje vládní agendu a strategickou komunikaci s ministerstvy a ostatními ústředními orgány státní správy.

- Pracovní skupina sekretariát ředitele

- Bezpečnostní ředitel
- Auditor kybernetické bezpečnosti
- Interní auditor
- **Rozkladová komise ředitele NÚKIB**
  - JUDr. Barbora Schrötterová (*Předsedkyně RK, zaměstnankyně NÚKIB)*
  - prof. JUDr. Radim Polčák, Ph.D. (*Externista)*
  - JUDr. Ing. Jiří Nováček (*Externista)*
  - JUDr. Bc. Petr Kadlec (*Externista)*
  - RNDr. Radim Ošťádal, Ph.D. (*Externista)*
  - Mgr. Iveta Pospíšilíková (*Externistka)*
  - Mgr. Marcela Káňová, Ph.D. (*Externistka)*
  - Ing. Martin Konečný (*Externista)*
  - Mgr. Pavel Štěpáník, LL.M. (*Externista)*
  - Mgr. Martin Švéda LL.M. (Zaměstnanec NÚKIB)
  - Mgr. Mgr. Katarína Haukvitzová (*Zaměstnankyně NÚKIB*)

NÚKIB

Etický kodex zaměstnanců Národního úřadu pro kybernetickou a informační bezpečnost

Preambule

Základními hodnotami, které má každý zaměstnanec Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Úřad“), je ctít zákonnost všech postupů, dodržovat rovný přístup ke všem fyzickým a právnickým osobám a vytvářet, udržovat a prohlubovat důvěru veřejnosti ve veřejnou správu.

Úřad usiluje o zachování a rozvíjení vysoké úrovně etiky a profesionality, usiluje o to, být významnou součástí zajišťování bezpečnosti České republiky (dále jen „ČR“), zejména v plnění role gestora a národní autority v oblasti kybernetické bezpečnosti a výkonu státní správy v této oblasti včetně provozu technického dohledového pracoviště Vládní CERT[1], v plnění role gestora ochrany utajovaných informací ČR v informačních a komunikačních systémech a role garanta ochrany utajovaných informací v informačních a komunikačních systémech cizí moci, ve výkonu role národní distribuční autority ČR v oblasti kryptografické ochrany a ve výkonu státní správy v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo.

Účelem Etický kodex zaměstnanců Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „Kodex“) je vymezit a podporovat žádoucí standardy chování zaměstnance Úřadu (dále jen „zaměstnanec“) ve vztahu k veřejnosti a spolupracovníkům.

Každý zaměstnanec je povinen při rozhodování dodržovat a ctít zákonnost všech postupů a rovný přístup ke všem fyzickým i právnickým osobám, zachovává věrnost zásadám práva a spravedlnosti vyplývajícím z evropského kulturního a historického dědictví, jedná v duchu nedotknutelných hodnot lidské důstojnosti a svobody, zachovává úctu a loajalitu k České republice, jakož i k Úřadu a ostatním zaměstnancům veřejné správy.

[1] Označení pro tzv. Computer Emergency Response Team.

Článek 1
Zákonnost

(1) Zaměstnanci plní pracovní úkoly v souladu s ústavním pořádkem, se zákony a ostatními právními předpisy, s právem Evropské unie, jakož i s mezinárodními smlouvami, kterými je Česká republika vázána.
(2) Při plnění úkolů jedná zaměstnanec pouze v rozsahu jemu svěřené pravomoci orgánu veřejné správy a v souladu s jejím účelem.

Článek 2
Rozhodování

(1) Zaměstnanec při rozhodování, vztahujícímu se k plnění jeho pracovních povinností, vždy usiluje o výběr nejvhodnějšího řešení v mezích právních norem a to s ohledem na veřejný zájem a na rozhodné okolnosti konkrétního případu. Dbá na to, aby rozhodnutí nemohlo být z objektivního hlediska vnímáno jako nespravedlivé. Do práv osob zaměstnanec zasahuje jen za podmínek stanovených zákonem a v nezbytném rozsahu nutném k dosažení účelu sledovaného veřejným zájmem, v jehož ochraně mu byla pravomoc svěřena.
(2) Při volbě nejvhodnějšího postupu zaměstnanec respektuje v mezích právních předpisů též koncepce, priority a cíle Úřadu, jeho interní dokumentaci a pokyny nadřízených vydané v souladu s tímto Kodexem.

Článek 3
Takt a slušnost

(1) Zaměstnanci jednají s kolegy, veřejností i se všemi ostatními zdvořile a se vzájemným respektem. Vyhýbají se především jakýmkoli znevažujícím komentářům z důvodu odlišných názorů, přesvědčení, kultury, etnického původu, pohlaví nebo osobního života, které by mohly urážet kolegy nebo veřejnost, či narušovaly dobré vztahy na pracovišti.
(2) Zaměstnanci respektují soukromí svých kolegů. Vztahy na pracovišti nesmí negativně ovlivnit práci Úřadu a plnění povinností jeho zaměstnanců.
(3) Od zaměstnanců se očekává, že udržují dobré pracovní vztahy a atmosféru tolerance. Zaměstnanec věnuje přiměřenou péči pracovnímu prostředí, udržuje pořádek a čistotu, a to jak na vlastním pracovišti, tak ve všech společných prostorách Úřadu.
(4) Netaktní, předpojaté i povýšené vystupování při jednání se zaměstnanci součinnostních organizací veřejné správy nebo s občany je hrubým prohřeškem.
(5) Za hrubý prohřešek se také považuje šikana na pracovišti sexuální obtěžování a jiné obdobné chování.
(6) Jednání nebo opomenutí z důvodu diskriminace je u zaměstnanců nepřípustné.

Článek 4
Profesionalita

(1) Zaměstnanec vykonává práci na vysoké odborné úrovni. Za kvalitu práce a rozvíjení své odbornosti je osobně odpovědný, své vzdělání si průběžně prohlubuje a doplňuje a sleduje vývoj v oblasti, která je náplní jeho práce.
(2) Zaměstnanec jedná profesionálně, nestranně a nezávisle, objektivně, čestně, bez nepřiměřeného projevu emocí a bez sledování osobního prospěchu tak, aby neohrozil dobrou pověst, vážnost a důvěryhodnost Úřadu. Při všem svém jednání nesmí zaměstnanec preferovat osobní či skupinové zájmy, ani se nechat ovlivnit pozitivními nebo negativními vztahy ke konkrétním osobám.
(3) Zaměstnanec jedná korektně se spolupracovníky i zaměstnanci jiných organizací, respektuje jejich znalosti a zkušenosti, také respektuje znalosti a zkušenosti jiných odborníků a účinně je využívá i pro svůj odborný růst. Zachovává kooperativní a kolegiální prostředí, dbá na pozitivní rozvoj vztahů a podporuje vzájemnou otevřenost a vstřícnost.
(4) Zaměstnanec včas poskytuje při plnění úkolů pravdivé a úplné informace v souladu s právními předpisy.

Článek 5
Loajalita

(1) Zaměstnanci jsou loajální k zájmům veřejné správy a Úřadu.
(2) Pokud se zaměstnanec ocitne v situaci, kdy mu svědomí nedovoluje plnit uložené úkoly, musí o této situaci informovat svého, je-li to z povahy situace možné, přímého nadřízeného, který je povinen takovou situaci řešit.
(3) Zaměstnanci jsou povinni neuposlechnout pokynu nadřízeného, pokud je v rozporu se zákonem nebo podzákonným právním předpisem, o takové situaci musí neprodleně informovat ředitele Úřadu nebo jeho náměstky.

Článek 6
Nestrannost

(1) Zaměstnanec dbá na to, aby jeho rozhodování bylo objektivní a nestranné a aby přijaté řešení bylo vždy v souladu s veřejným zájmem. Při všem svém jednání nesmí zaměstnanec preferovat osobní či skupinové zájmy ani se nesmí nechat ovlivnit pozitivními či negativními osobními vztahy ke konkrétním osobám. Zaměstnanec se zdrží také všeho, co by mohlo ohrozit důvěru v nestrannost jeho rozhodování.
(2) Ve shodných nebo podobných případech jedná zaměstnanec tak, aby mezi jednotlivými postupy nevznikaly rozdíly, jež není možno odůvodnit objektivními skutečnostmi, zejména konkrétními okolnostmi daného případu.
(3) Zaměstnanec vystupuje vůči účastníkům právních vztahů objektivně tak, aby je neuváděl v omyl o jejich právech a povinnostech, informuje je srozumitelně; veškerá hodnocení provádí profesionálně, objektivně, bez emocí a bez sledování osobního prospěchu a v souladu s právem a spravedlností.

(4) Zaměstnanci oznamují přímému nadřízenému všechny případy, kdy by mohlo dojít k ohrožení nestranného jednání a rozhodování (osobní předsudky, nevhodné předchozí jednání klienta apod.), vedoucí zaměstnanci musí takové situace řešit tak, aby nestrannost Úřadu nemohla být zpochybněna.

Článek 7
Rychlost a efektivita

Zaměstnanec plní své úkoly osobně, svědomitě, bez zbytečných průtahů a v souladu se zásadou hospodárnosti. Zároveň zachovává zásadu spolupráce s cílem dosáhnout nejlepších výsledků, aby třetím stranám ani Úřadu nevznikaly zbytečné náklady.

Článek 8
Střet zájmů

(1) Zaměstnanec předchází situacím, které by mohly ohrozit důvěru v jeho nestrannost, nezávislost a spravedlivost a ve kterých by byl vystaven možnému střetu svých osobních zájmů s veřejným zájmem na řádném výkonu práce, přičemž za osobní zájem se považuje každá případná výhoda pro zaměstnance, osoby jemu blízké a fyzické a právnické osoby, se kterými má osobní, obchodní, pracovní nebo politické vztahy. Ustanovení právních předpisů upravujících vyloučení z projednávání věci nejsou tímto Kodexem dotčena.
(2) Zaměstnanec nesmí ohrozit veřejný zájem nebo „dobré jméno Úřadu“ tím, že se bude odvolávat na své postavení nebo na svou funkci ve věcech, které nesouvisejí s výkonem práce, nebo že bude zneužívat své postavení a informace, o nichž se dozvěděl při výkonu práce.
(3) Zaměstnanec se nezúčastní žádné činnosti, která se neslučuje s řádným výkonem jeho pracovních povinností nebo tento výkon omezuje. Dále se vyhýbá činnostem a jednáním, které by mohly snížit důvěru veřejnosti ve veřejnou správu.
(4) V případě, že se zaměstnanec při plnění úkolů ocitne v situaci, kdy je vystaven nebo by mohl být vystaven možnému střetu zájmů, ohlásí tuto skutečnost bez zbytečného odkladu vedoucímu zaměstnanci.

Článek 9
Korupce, lobbing

(1) Zaměstnanec nesmí při svém rozhodování a v souvislosti s rozhodováním přijímat ani vyžadovat dary či jiná zvýhodnění pro sebe nebo někoho jiného, popřípadě jakýmkoli jiným způsobem připustit ovlivnění plnění jemu svěřených úkolů v oblasti veřejné správy, objektivního hodnocení věci a nestranného rozhodování. Dary nebo výhody poskytované zaměstnanci zaměstnavatelem tímto nejsou dotčeny.
(2) Zaměstnanec jedná tak, aby se při plnění jemu svěřených úkolů v oblasti veřejné správy nedostal do postavení, ve kterém byl zavázán nebo se cítil být zavázán oplatit službu či laskavost, která mu byla prokázána.

(3) Zaměstnanec se vyvaruje vztahů vzájemné závislosti a nepatřičného vlivu jiných osob (klientelismus, nepotismus), které by mohly ohrozit jeho nestrannost.
(4) Zaměstnanec podle zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „zákoník práce“), nesmí v souvislosti s výkonem svého zaměstnání přijímat dary, s výjimkou darů poskytovaných Úřadem nebo na základě právních předpisů. V případě, že je zaměstnanci podle zákoníku práce v souvislosti s výkonem jeho zaměstnání nabídnuta jakákoliv neoprávněná výhoda, musí ji odmítnout a o nabídce neprodleně informovat bezprostředně nadřízeného zaměstnance.
(5) Za dary se nepovažují plnění z pouhé společenské úsluhy či plnění poskytovaná při společenských či protokolárních příležitostech, jsou-li jim úměrná svým účelem i hodnotou. Za dary se rovněž nepovažují drobné reklamní a propagační předměty.
(6) Ve všech případech, kdy by mohla vzniknout pochybnost, zda zaměstnanec postupuje v souladu s tímto článkem, informuje zaměstnanec svého bezprostředně nadřízeného a postupuje dle jeho pokynů.
(7) Předpokládá-li zaměstnanec jednání s rizikem korupce nebo podvodu nebo jednání s prvky lobbingu, vede je za přítomnosti minimálně jednoho svého spolupracovníka. O takovém jednání vyhotoví zaměstnanec záznam, v němž uvede jméno a příjmení osob, s nimiž jednal, jméno, popřípadě jména, a příjmení dalších osob, které byly jednání přítomny, popis a účel jednání a případně důvod, pro který předpokládá riziko korupce nebo podvodu. Záznam předá zaměstnanec bezprostředně nadřízenému zaměstnanci.
(8) Vedoucí zaměstnanec tyto záznamy posoudí, a zjistí-li, že jednáním druhé strany dle výše uvedeného odstavce mohlo dojít ke spáchání trestného činu, podá oznámení orgánu činného v trestním řízení. Předáním záznamu vedoucímu zaměstnanci se zaměstnanec nezprostí povinností vyplývajících z trestněprávních předpisů. Obdobně se postupuje v případě oznámení zaměstnance podle zákoníku práce.

Článek 10
Nakládání se svěřenými prostředky

(1) Zaměstnanec vynakládá v souladu s právními předpisy, veškeré úsilí, aby zajistil maximální efektivní a ekonomické spravování a využívání finančních zdrojů a zařízení, které mu byly svěřeny, jakož i služeb, které mu byly poskytnuty. S těmito svěřenými prostředky nakládá efektivně a hospodárně.
(2) Zaměstnanec si pro svou vlastní potřebu nepřivlastňuje žádné finanční prostředky ani majetek Úřadu a vědomě nepřispívá k tomu, aby tak činil někdo jiný.
(3) V případě, že zaměstnanec zjistí škodu vzniklou Úřadu, postupuje dle příslušného interního normativního aktu Úřadu.

Článek 11
Mlčenlivost

(1) Zaměstnanec zachovává mlčenlivost o skutečnostech, které se dozvěděl v souvislosti s plněním úkolů veřejné správy, jež by mohly poškodit nebo ohrozit činnost

zaměstnavatele. Povinnost mlčenlivosti se nevztahuje na skutečnosti, které zakládají podezření na protiprávní jednání.

(2) Zaměstnanec je povinen zachovat mlčenlivost o skutečnostech, které se dozvěděl při výkonu úřední činnosti, zejména o osobních údajích, důvěrných informace nebo utajovaných informacích v rozsahu stanoveném právními předpisy, pokud není této povinnosti v souladu s právními předpisy zproštěn.

(3) Zaměstnanec není povinen zachovat mlčenlivost o takových skutečnostech, které naznačují, že v rámci Úřadu dochází ke korupci, špatnému hospodaření nebo jinému porušování právních předpisů a o kterých měl oprávněné důvody se domnívat, že jsou pravdivé, pokud tyto skutečnosti sdělí orgánu nebo osobě, která je schopna přijmout nezbytná preventivní nebo nápravná opatření (tzv. whistleblowing). Za orgány nebo osoby, které jsou schopny přijmout nezbytná preventivní nebo nápravná opatření se považují jak interní (vedoucí zaměstnanci), tak externí (především Policie ČR nebo Stálá komise pro kontrolu činnosti Úřadu) orgány a osoby. Sdělení takové skutečnosti výše uvedeným postupem není porušením tohoto Kodexu a zaměstnavatel nesmí zaměstnance za takový postup jakýmkoliv způsobem postihovat nebo znevýhodňovat.

(4) Zaměstnanec je povinen dbát na ochranu utajovaných informací stejně jako na ochranu důvěrných informací a osobních údajů, zabezpečit jejich uložení a znepřístupnění apod.

Článek 12
Informování veřejnosti

Informace o činnosti Úřadu, jakož i další informace určené veřejnosti, sděluje za Úřad zaměstnanec, který je k tomu určen.

Článek 13
Veřejná činnost

(1) Zaměstnanec jedná při výkonu veřejné správy politicky nestranným způsobem a nevykonává veřejnou činnost, která by mohla narušit důvěru veřejnosti v jeho schopnost nestranně plnit úkoly veřejné správy.

(2) Zaměstnanec veřejné správy se v soukromém životě vyhýbá takovým činnostem, chování a jednání, která by mohla snížit důvěru ve veřejnou správu v očích veřejnosti nebo dokonce zavdat příčinu k ovlivňování zaměstnance. Jedná tak, aby jeho chování přispívalo k dobré pověsti Úřadu.

Článek 14
Reprezentace

(1) Zaměstnanec svým jednáním a vystupováním podporuje důvěryhodnost a vážnost Úřadu.

(2) Zaměstnanec vystupuje kultivovaně, vyjadřuje se spisovně a dbá na odpovídající verbální i neverbální komunikaci.

(3) Zaměstnanec používá pozdrav jako jednoduchý, elementární společenský kontakt, který je základním projevem zdvořilosti.

(4) Zaměstnanec jedná s každým ohleduplně, způsobem přiměřeným jeho sociálním schopnostem a komunikačním potřebám, a respektuje jeho individualitu. Veškerá jednání s dotčenými osobami vede zaměstnanec taktně a způsobem, který respektuje důstojnost těchto osob.
(5) Zaměstnanec vystupuje vůči třetím osobám tak, aby je neuváděl v omyl o jejich právech a povinnostech, a informuje je jasně, přesně, úplně, pravdivě a srozumitelně. Je si vědom, že třetí osoby mají právo znát jeho jméno, popřípadě jména, příjmení zaměstnanců a název organizačního útvaru Úřadu, pokud poskytnutí těchto informací nebude vyhodnoceno jako nepřiměřené s ohledem na zajištění bezpečnosti zaměstnanců.
(6) Zaměstnanec dbá na čistotu, dodržování hygieny a úpravu svého zevnějšku, užívá v zaměstnání oděv, který je adekvátní jeho práci a odpovídá vážnosti Úřadu v dané situaci, a to jak u příležitostí v rámci oficiální reprezentace Úřadu, tak při běžném chodu Úřadu a každodenním styku s nadřízenými i kolegy včetně těch, s nimiž sdílí kancelář. Jsou-li pro jednání předepsána pravidla oblékání (např. business formal), zaměstnanec je dodržuje a užívá odpovídající oděv.
(7) Zaměstnanec dodržuje pravidla jednotného vizuálního stylu Úřadu, stejně jako pravidla komunikační strategie.
(8) Zaměstnanec Úřadu si je vědom, že pokoutní šíření neopodstatněných sdělení (klepů, fám apod.) i uvnitř organizace, je závažným etickým a bezpečnostním prohřeškem.

Článek 15
Uplatnitelnost a vymahatelnost

Kodex navazuje na základní práva a povinnosti zaměstnanců uvedené v zákoníku práce, pracovním řádu a dalších právních předpisech. Zásadní porušování Kodexu zaměstnancem Úřadu může být kvalifikováno jako porušení pracovního řádu a tím i zákoníku práce, který ukládá dodržovat vnitřní právní předpisy zaměstnavatele.

Článek 16
Vedoucí zaměstnanec

(1) Vedoucí zaměstnanec vykonává jako manažer se spoluodpovědností za řízení své manažerské funkce: vede, organizuje a kontroluje zaměstnance, které řídí a motivuje je k eticky žádoucímu jednání.
(2) Vedoucí zaměstnanci usilují o zlepšení pracovních podmínek a o odpovídající pracovní prostředí v souladu se zásadami profesionality a bezpečnosti s cílem ochrany fyzické i morální integrity zaměstnanců. Odpovídají za odborné vzdělávání a přípravu zaměstnanců a neustálé zlepšování profesionálního a etického standardu pracoviště.
(3) Vedoucí zaměstnanec jedná a hodnotí práci zaměstnanců, které řídí, spravedlivě, podle zásluh. Nesmí jednat předpojatě na základě osobních vztahů či sympatií.
(4) Vedoucí zaměstnanec jedná se zaměstnanci, které řídí, zdvořile. Nároky, které na ně klade, a úkoly, které jim svěřuje, jsou vždy přiměřené a odůvodněné a v souladu s pracovními povinnostmi zaměstnance a s jeho náplní práce.

(5) Vedoucí zaměstnanci odpovídají za plnění standardů Kodexu v rámci svého pracoviště a za řešení problémů vznikajících při uplatňování jeho jednotlivých ustanovení. Sami se důsledně vyhýbají situacím a jednáním, které by byly neslučitelné s požadavky Kodexu.
(6) Od vedoucích zaměstnanců se očekává, že udržují dobré pracovní vztahy a atmosféru tolerance a vzájemného respektu mezi svými podřízenými i mezi jednotlivými organizačními celky Úřadu. Nejen ukládají a kontrolují úkoly, ale jsou otevřeni dotazům, připomínkám, námitkám či stížnostem. Konflikty na pracovišti řeší proaktivně, bez zbytečného odkladu, citlivě a nestranně.

Článek 17
Společenská odpovědnost organizace

(1) Otázka společenské odpovědnosti Úřadu by měla být neodmyslitelnou součástí práce všech jeho zaměstnanců, kteří podnikají kroky k tomu, aby naše okolí žilo kvalitnějším životem. Zaměstnanci se podílí na aktivitách v rámci ekonomické, environmentální a sociální oblasti, snaží se být ohleduplní k životnímu prostředí.

(2) Úřad pečuje o své zaměstnance, udržuje se zaměstnanci dobré vztahy, stejně jako s ostatními subjekty, se kterými přichází do kontaktu. Jeho cílem je nejen spokojenost zaměstnanců, ale i občanů i dalších subjektů, se kterými spolupracuje.

Článek 18
Závěrečná ustanovení

(1) Zaměstnanec si uvědomuje, že selhání jednotlivce v oblasti etiky má dopad na veřejnou správu jako celek, a proto jde ostatním příkladem.
(2) Respektování zásad etiky je věcí profesionální ctí zaměstnance. Bez jejich dodržování a dodržování Kodexu nelze dostávat profesionální povinnosti zaměstnance Úřadu.
(3) Poukáže-li zaměstnanec oprávněně na chování v rozporu s tímto Kodexem, nebude mít jeho jednání negativní důsledky v pracovněprávních vztazích.
(4) Vedoucí zaměstnanci jsou povinni seznámit s Kodexem podřízené zaměstnance a Kodexu bude zveřejněn na webových stránkách Úřadu.
(5) Tento Kodex nabývá platnosti dne 01. 06. 2020.

Ing. Karel Řehka, v.r.
ředitel Národního úřadu pro kybernetickou a informační bezpečnost

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Pořadové číslo:	Platí od:	Ruší:
S07/2024	**15. 5. 2024**	
Č.j.: 3589/2024-NÚKIB-E/200		
Druh vnitřního aktu řízení:		

SMĚRNICE

ŘEDITELE NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

Název:

Ochrana oznamovatelů

ČÁST PRVNÍ
-
OBECNÁ USTANOVENÍ

Čl. 1
Předmět úpravy

Tato směrnice upravuje

a) příslušnost, postavení, oprávnění a povinnosti osoby určené v Národním úřadě pro kybernetickou a informační bezpečnost (dále jen „Úřad“) k přijímání a vyřizování oznámení o možném protiprávním jednání podle zákona č. 171/2023 Sb., o ochraně oznamovatelů (dále jen „zákon o ochraně oznamovatelů“) (dále jen „příslušná osoba“),

b) práva a povinnosti osoby, proti které oznámení o možném protiprávním jednání podle zákona o ochraně oznamovatelů (dále jen „oznámení“) směřuje (dále jen „dotčená osoba“), a

c) povinnosti ředitele Úřadu, náměstků ředitele a příslušné osoby při přijímání a vyřizování oznámení (dále jen „osoba zúčastněná na prošetřování“).

Čl. 2
Příslušnost a působnost

(1) Příslušná osoba přijímá a vyřizuje oznámení, které podal zaměstnanec Úřadu, nebo osoba vykonávající v Úřadu dobrovolnickou činnost, odbornou praxi nebo stáž (dále jen „oznamovatel“).

(2) Oznámení obsahuje informace o možném protiprávním jednání, k němuž došlo nebo má dojít na Úřadu, nebo u osoby, se kterou oznamovatel byl nebo je v kontaktu v souvislosti s výkonem zaměstnání, dobrovolnické činnosti, odborné praxe nebo stáže na Úřadu, a které

a) má znaky trestného činu,

b) má znaky přestupku, za který zákon stanoví sazbu pokuty, jejíž horní hranice je alespoň 100 000 Kč,

c) porušuje zákon o ochraně oznamovatelů, nebo

d) porušuje jiný právní předpis nebo předpis Evropské unie v oblasti

i. finančních služeb, povinného auditu a jiných ověřovacích služeb, finančních produktů a finančních trhů,

ii. daně z příjmů právnických osob,

iii. předcházení legalizaci výnosů z trestné činnosti a financování terorismu,

iv. ochrany spotřebitele,

v. souladu s požadavky na výrobky včetně jejich bezpečnosti,

vi. bezpečnosti dopravy, přepravy a provozu na pozemních komunikacích,

vii. ochrany životního prostředí,

viii. bezpečnosti potravin a krmiv a ochrany zvířat a jejich zdraví,

ix. radiační ochrany a jaderné bezpečnosti,

x. hospodářské soutěže, veřejných dražeb a zadávání veřejných zakázek,

xi. ochrany vnitřního pořádku a bezpečnosti, života a zdraví,

xii. ochrany osobních údajů, soukromí a bezpečnosti sítí elektronických komunikací a informačních systémů,

xiii. ochrany finančních zájmů Evropské unie, nebo

xiv. fungování vnitřního trhu včetně ochrany hospodářské soutěže a státní podpory podle práva Evropské unie.

(3) Oznámení obsahuje údaje o jménu, příjmení a datu narození, nebo jiné údaje, z nichž je možné dovodit totožnost oznamovatele; má se za to, že údaje o totožnosti oznamovatele jsou pravdivé. Oznámení nemusí obsahovat údaje podle věty první, pokud bylo podáno osobou, jejíž totožnost je příslušné osobě známa.

(4) Za oznámení podle odstavce 1 se nepovažuje část oznámení, která obsahuje

a) informace, jejichž oznámení by mohlo bezprostředně ohrozit

i. svrchovanost, územní celistvost a demokratické základy České republiky,

ii. vnitřní pořádek a bezpečnost,

iii. ve větším rozsahu životy a zdraví osob,

iv. ochranu informací o veřejných zakázkách v oblasti obrany nebo bezpečnosti, ledaže je zadávání těchto zakázek upraveno předpisem Evropské unie,

v. plnění mezinárodních závazků v oblasti obrany,

vi. významné bezpečnostní operace,

vii. bojeschopnost ozbrojených sil České republiky, nebo

b) informace o činnosti zpravodajských služeb České republiky,

c) informace, jejichž oznámení by představovalo porušení povinnosti zachovávat mlčenlivost duchovních v souvislosti s výkonem zpovědního tajemství nebo práva obdobného zpovědnímu tajemství.

Čl. 3

Postavení příslušné osoby

(1) Postavení, znalosti, schopnosti, dovednosti a vlastnosti příslušné osoby nesmí zavdávat důvod k pochybnosti o tom, že svou činnost vykonává řádně a nestranně.

(2) Příslušné osobě nelze udělovat pokyny, ani její činnost jinak ovlivňovat způsobem, který by mařil nebo ohrožoval její řádný výkon. Kontrola řádného výkonu činnosti příslušné osoby nadřízeným představeným nebo nadřízeným vedoucím zaměstnancem není za současného zachování

požadavku nestrannosti a důvěrnosti informací souvisejících s oznámením podle této směrnice první větou dotčena.

(3) Příslušná osoba bezodkladně předá oznámení k vyřízení jiné příslušné osobě, lze-li vzhledem k jejímu poměru vůči oznamovateli nebo k informacím uvedeným v oznámení důvodně pochybovat o její nestrannosti.

(4) Pokud nelze oznámení předat k vyřízení jiné příslušné osobě, uvědomí o této skutečnosti příslušná osoba oznamovatele a poučí ho o právu podat oznámení prostřednictvím vnějšího oznamovacího systému v působnosti Ministerstva spravedlnosti.

ČÁST DRUHÁ
-
PŘIJÍMÁNÍ A VYŘIZOVÁNÍ OZNÁMENÍ

Čl. 4
Přijímání oznámení

Příslušná osoba přijímá oznámení

a) písemně,
b) ústně, a to telefonicky nebo prostřednictvím systému hlasových zpráv; oznámení lze přijmout i osobně, na žádost oznamovatele v přiměřené lhůtě, nejdéle však do 14 dnů ode dne, kdy o to oznamovatel požádal. Nelze-li lhůtu dodržet z důvodů na straně oznamovatele, poznamená příslušná osoba tuto skutečnost do spisu.

Čl. 5
Vyřizování oznámení

(1) Příslušná osoba bezodkladně písemně vyrozumí oznamovatele o přijetí oznámení, nejdéle však do 7 dnů ode dne přijetí oznámení. Věta první se nepoužije, jestliže

a) příslušné osobě není oznamovatel znám,
b) je zřejmé, že by takovým postupem byla prozrazena totožnost oznamovatele, nebo
c) o to oznamovatel požádal.

(2) Příslušná osoba posoudí důvodnost informací uvedených v oznámení a písemně vyrozumí oznamovatele o výsledcích posouzení do 30 dnů ode dne přijetí oznámení. V případech skutkově nebo právně složitých lze tuto lhůtu prodloužit až o 30 dnů, nejvýše však dvakrát. O prodloužení lhůty a důvodech pro její prodloužení je příslušná osoba povinna oznamovatele písemně vyrozumět před jejím uplynutím. Věta druhá odstavce 1 se použije obdobně.

(3) Pokud oznámení neobsahuje všechny potřebné informace či údaje, vyzve příslušná osoba oznamovatele k jejich doplnění.

(4) Není-li při posuzování důvodnosti zjištěno protiprávní jednání podle čl. 2 odst. 2, poučí příslušná osoba oznamovatele ve lhůtě podle odstavce 2 o právu podat oznámení Ministerstvu spravedlnosti a příslušnému orgánu veřejné moci.

(5) Bylo-li při posuzování důvodnosti zjištěno možné protiprávní jednání, příslušná osoba, je-li to

možné s ohledem na zachování důvěrnosti totožnosti oznamovatele a osoby podle čl. 8 odst. 2 písm. a) až h), bez zbytečného odkladu navrhne řediteli Úřadu opatření k předejití nebo nápravě protiprávního stavu.

(6) Příslušná osoba písemně vyrozumí oznamovatele o výsledku každé fáze vyřizování oznámení bezprostředně po tom, co byla ukončena, nejdéle však do 90 dnů ode dne přijetí oznámení. Kromě výsledku posouzení důvodnosti informací uvedených v oznámení informuje zejména o

a) ochraně, která oznamovateli na základě podaného oznámení náleží,

b) zjištěném protiprávním jednání,

c) navržených preventivních nebo nápravných opatřeních a důvodech jejich navržení,

d) přijatých preventivních nebo nápravných opatřeních a jejich důvodnosti, byla-li ve lhůtě podle tohoto odstavce přijata, a

e) jiném způsobu vyřízení oznámení.

(7) Dojde-li oznámení, jež má přijímat a vyřizovat příslušná osoba, jiné osobě nebo organizačnímu celku Úřadu, bezodkladně musí být postoupeno k vyřízení příslušné osobě, a to způsobem, který zajistí zachování důvěrnosti obsahu oznámení i totožnosti oznamovatele. Z evidence dokumentů i ze spisu musí být zároveň vymazány veškeré informace týkající se takového oznámení, pokud je to možné.

(8) Dojde-li příslušné osobě podání, k jehož přijetí není příslušná, bezodkladně jej postoupí příslušnému organizačnímu celku Úřadu. Před postoupením podání příslušná osoba upozorní podatele na skutečnost, že se nejedná o oznámení podle zákona o ochraně oznamovatelů a předmětná úprava se neuplatní. Příslušná osoba znečitelní nebo jinak utají informace a osobní údaje, ze kterých lze totožnost podatele dovodit, ledaže podatel s postoupením těchto informací a údajů souhlasí.

(9) Tímto předpisem není dotčena povinnost podle § 8 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů a § 73 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů.

Čl. 6

Evidence a uchovávání oznámení

(1) Příslušná osoba vede v elektronické podobě evidenci údajů o přijatých oznámeních, a to v rozsahu

a) datum přijetí oznámení,

b) jméno, příjmení, datum narození a kontaktní adresa oznamovatele, nebo jiné údaje, z nichž je možné dovodit totožnost oznamovatele, jsou-li jí tyto údaje známy,

c) shrnutí obsahu oznámení a identifikace dotčené osoby, je-li jí její totožnost známa,

d) datum ukončení posouzení důvodnosti oznámení příslušnou osobou a jeho výsledek,

e) navržená a přijatá preventivní nebo nápravná opatření.

(2) Příslušná osoba uchovává oznámení a dokumenty související s oznámením po dobu 5 let ode dne přijetí oznámení.

(3) Do evidence podle odstavce 1 a k oznámením a dokumentům uchovávaným podle odstavce 2 tohoto článku má přístup pouze příslušná osoba.

Čl. 7

Zpracování osobních údajů

(1) Na zpracování osobních údajů v souvislosti s oznámením se nevztahuje povinnost posouzení vlivu zpracování osobních údajů na ochranu osobních údajů.

(2) Osobní údaje se ve vztahu k oznámení zpracovávají na základě čl. 6 odst. 1 písm. c) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“).

(3) Zvláštní kategorie osobních údajů podle čl. 9 odst. 1 GDPR je možné ve vztahu k oznámení zpracovávat na základě čl. 9 odst. 2 písm. e), f) nebo g) GDPR.

(4) Informační povinnost podle čl. 13 a 14 GDPR je třeba plnit za současného zachování důvěrnosti podle této směrnice.

(5) Výkon práva na přístup k osobním údajům podle čl. 15 GDPR lze subjektu údajů v souladu s čl. 23 GDPR umožnit pouze za předpokladu, že bude zachována důvěrnost totožnosti oznamovatele a dalších osob uvedených v oznámení.

(6) Žádost o přístup k osobním údajům týkající se oznámení předá osoba pověřená výkonem agendy ochrany osobních údajů k vyřízení příslušné osobě.

(7) Zjistí-li příslušná osoba, že v souvislosti s oznámením nejsou žádné údaje vedeny nebo, že se uplatní výjimka z povinnosti takovou informaci poskytnout, žádost dle odst. 6 bez dalšího odloží.

(8) Povinnost oznámit porušení zabezpečení osobních údajů subjektu údajů se za současného zachování důvěrnosti podle této směrnice vztahuje rovněž na příslušnou osobu.

ČÁST TŘETÍ

-

OCHRANA PŘED ODVETNÝMI OPATŘENÍMI A PRÁVA A POVINNOSTI PŘÍSLUŠNÉ OSOBY A DALŠÍCH OSOB

Čl. 8

Ochrana oznamovatele a dalších osob

(1) Odvetným opatřením se rozumí jednání nebo jeho opomenutí v souvislosti s prací nebo jinou obdobnou činností oznamovatele podle § 2 odst. 3 a 4 zákona o ochraně oznamovatelů, které bylo vyvoláno učiněním oznámení a které oznamovateli nebo osobě podle odstavce 2 písm. a) až h) tohoto článku může způsobit újmu; při splnění těchto podmínek je odvetným opatřením zejména

a) rozvázání pracovního poměru nebo neprodloužení pracovního poměru na dobu určitou,

b) zrušení právního vztahu založeného dohodou o provedení práce nebo dohodou o pracovní činnosti,

c) odvolání z místa vedoucího zaměstnance,

d) snížení mzdy, platu nebo odměny nebo nepřiznání osobního příplatku,

e) přeložení nebo převedení na jinou práci nebo na jiné pracovní místo,

f) pracovní posudek,

g) neumožnění odborného rozvoje,

h) změna pracovní doby,

i) vyžadování lékařského posudku nebo pracovně lékařské prohlídky,

j) výpověď nebo odstoupení od smlouvy, nebo

k) zásah do práva na ochranu osobnosti.

(2) Odvetnému opatření nesmí být vystaven oznamovatel ani

a) osoba, která poskytla pomoc při zjišťování informací, které jsou obsahem oznámení, podání oznámení nebo posouzení jeho důvodnosti,

b) osoba, která je ve vztahu k oznamovateli osobou blízkou,

c) osoba, která je zaměstnancem nebo kolegou oznamovatele,

d) osoba oznamovatelem ovládaná,

e) právnická osoba, v níž má oznamovatel účast, osoba ji ovládající, jí ovládaná osoba nebo osoba, která je s touto právnickou osobou ovládaná stejnou ovládající osobou,

f) právnická osoba, jejíhož voleného orgánu je oznamovatel členem, osoba ovládající, ovládaná nebo osoba ovládaná stejnou ovládající osobou,

g) osoba, pro kterou oznamovatel vykonává práci nebo jinou obdobnou činnost podle § 2 odst. 3 a 4 zákona o ochraně oznamovatelů, nebo

h) svěřenský fond, jehož je oznamovatel nebo právnická osoba podle písmene e) nebo f) zakladatelem nebo obmyšleným nebo ve vztahu k němuž jsou oznamovatel nebo právnická osoba podle písmene e) nebo f) osobou, která podstatným způsobem zvýší majetek svěřenského fondu smlouvou nebo pořízením pro případ smrti.

(3) Měl-li oznamovatel oprávněné důvody se domnívat, že oznámení bylo nezbytné pro odhalení porušení podle čl. 2 odst. 2 této směrnice, nepovažuje se oznámení za porušení bankovního tajemství, smluvní povinnosti mlčenlivosti, povinnosti mlčenlivosti podle daňového řádu ani povinnosti zachovávat mlčenlivost podle právních předpisů upravujících práci nebo jinou obdobnou činnost, s výjimkou povinnosti

a) zajistit ochranu utajovaných informací dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, a informací, jejichž vyzrazení by zjevně mohlo ohrozit probíhající trestní řízení nebo ochranu zvláštních skutečností upravujícího krizové řízení podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů,

b) mlčenlivosti při výkonu činnosti notáře, notářského kandidáta a koncipienta, státního zástupce, asistenta a právního čekatele, advokáta a advokátního koncipienta, soudního

exekutora, exekutorského kandidáta a koncipienta, soudce, soudce Ústavního soudu, asistenta soudce, justičního kandidáta a mlčenlivosti zaměstnance notáře, soudního exekutora, advokáta a zaměstnance společnosti, prostřednictvím které advokát vykonává advokacii jako společník podle zákona upravujícího výkon advokacie, nebo obdobné zahraniční společnosti, nebo další osoby, která se v rámci takové společnosti podílí na poskytování právních služeb,

c) mlčenlivosti při poskytování právní pomoci v řízení před soudem nebo jiným orgánem veřejné moci, nebo

d) mlčenlivosti při poskytování zdravotních služeb dle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.

(4) Oznámení a jednání oznamovatele nebo osoby podle odstavce 2 písm. a) až h) tohoto článku v souvislosti se zjišťováním informací, které se později staly obsahem oznámení, se nepovažuje za porušení smluvní nebo zákonné povinnosti, s výjimkou případů, kdy je jednáním v souvislosti se zjišťováním takových informací spáchán trestný čin; to neplatí, pokud oznamovatel nebo osoba podle odstavce 2 písm. a) až h) tohoto článku neměli oprávněný důvod se domnívat, že oznámení bylo nezbytné pro odhalení porušení podle čl. 2 odst. 2 této směrnice.

Čl. 9

Oprávnění příslušné osoby

(1) Příslušná osoba je při posuzování důvodnosti oznámení oprávněna

a) požadovat prokázání totožnosti dotčené osoby nebo osoby zúčastněné na prošetřování předložením zaměstnaneckého identifikačního průkazu,

b) požadovat sdělení údajů a předložení nebo zpřístupnění listin, audiovizuálních a digitálních záznamů a jiných věcí, které mohou souviset s oznámením,

c) požadovat vysvětlení od zaměstnanců Úřadu, které je potřebné k posouzení důvodnosti skutečností uvedených v oznámení,

d) pořizovat si z předložených nebo zpřístupněných listin elektronické obrazy, výpisy, opisy nebo kopie,

e) pořizovat si kopie předložených nebo zpřístupněných audiovizuálních a digitálních záznamů,

f) pořizovat se souhlasem dotčené osoby nebo osoby zúčastněné na prošetřování zvukový nebo obrazově zvukový záznam jejich ústního projevu,

g) vstupovat do všech prostor na Úřadu, které mohou souviset s oznámením, není-li jiným interním normativním aktem Úřadu stanoveno jinak.

(2) Příslušná osoba je při prošetřování dále oprávněna požadovat od dotčené osoby nebo od osoby zúčastněné na prošetřování ústní vysvětlení, jehož podání mohou odmítnout; o této skutečnosti je příslušná osoba poučí. O průběhu a obsahu vysvětlení sepíše příslušná osoba záznam, nebo pořídí zvukový nebo obrazový záznam. Záznam podepisuje příslušná osoba a osoba, která vysvětlení poskytla. Tím není dotčena povinnost zachovávat důvěrnost podle této směrnice.

(3) Příslušná osoba je dále oprávněna požadovat od zaměstnanců Úřadu v přiměřené lhůtě zpracování písemného odborného stanoviska ke skutkovým a právním otázkám souvisejícím s oznámením; tím není dotčena povinnost zachovávat důvěrnost podle této směrnice.

Čl. 10
Povinnosti příslušné osoby

(1) Příslušná osoba vykonává svou činnost osobně.

(2) Příslušná osoba postupuje při výkonu své činnosti nestranně.

(3) Příslušná osoba zachovává důvěrnost totožnosti oznamovatele i osoby podle čl. 8 odst. 2 písm. a) až h) této směrnice, jakož i informací, které by k odhalení jejich totožnosti mohly vést; to neplatí, udělí-li k postupu, který by mohl ohrozit zachování důvěrnosti totožnosti, oznamovatel nebo osoba podle čl. 8 odst. 2 písm. a) až h) této směrnice písemný souhlas. Tím není dotčen čl. 5 odst. 4 této směrnice.

(4) Příslušná osoba může nezbytně širokému okruhu jiných osob odhalit totožnost dotčené osoby tehdy, je-li to nezbytné k řádnému prošetření informací uvedených v oznámení nebo k navržení nebo uložení preventivního nebo nápravného opatření.

(5) Příslušná osoba rovněž zachovává důvěrnost informací, jejichž prozrazení by mohlo zmařit nebo ohrozit účel podávání oznámení, zejména řádné prošetření informací uvedených v oznámení a předejití nebo nápravu protiprávního stavu.

(6) Informace a osobní údaje, o kterých se zachovává důvěrnost, neposkytuje příslušná osoba ani na základě žádosti podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

(7) Příslušná osoba předloží řediteli Úřadu do 1. března následujícího kalendářního roku písemnou zprávu o své činnosti za uplynulý kalendářní rok. Nedojde-li takovým postupem k porušení důvěrnosti podle této směrnice, ve zprávě uvede alespoň

a) celkový počet oznámení,

b) počet oznámení, která byla předána k prošetření jiné příslušné osobě, včetně odůvodnění,

c) počet oznámení, která byla předána příslušnému orgánu veřejné moci,

d) počet probíhajících prošetření,

e) počet ukončených prošetření,

f) počet oznámení, u kterých informace v nich uvedené nebylo možné prošetřit, včetně odůvodnění,

g) počet oznámení spadajících do věcné působnosti podle čl. 2 odst. 2 této směrnice,

h) počet oznámení spadajících do osobní působnosti podle čl. 2 odst. 2 této směrnice a

i) zjištěné nedostatky, navržená preventivní nebo nápravná opatření a přijatá preventivní nebo nápravná opatření.

Čl. 11

Povinnosti dalších osob

(1) Dotčená osoba a osoba zúčastněná na prošetřování jsou povinny umožnit příslušné osobě výkon jejich oprávnění, nestanoví-li tato směrnice jinak.

(2) Důvěrnost podle této směrnice je povinna zachovávat každá osoba, která k chráněné informaci nebo osobnímu údaji získá přístup.

ZÁVĚREČNÁ USTANOVENÍ

Čl. 12

Přílohy

Nedílnou součástí této směrnice je příloha:

Příloha č. 1 – Formulář pro podání oznámení podle zákona o ochraně oznamovatelů

Příloha č. 2 – Informace pro oznamovatele.

Čl. 13

Účinnost

Tato směrnice nabývá účinnosti dnem 15. května 2024.

v z. Ing Tomáš Krejčí

Ing. Lukáš Kintr
ředitel Národního úřadu pro kybernetickou a informační bezpečnost