

Státní cloud a pravidla hry (NIS2, SOC 2)



SPCSS

Státní pokladna
Centrum sdílených služeb

Poskytovatel státní části e-Government
cloudu a ICT služeb, včetně kybernetické
bezpečnosti, pro státní správu

2. 9. 2025

TLP: **GREEN**

Představení



Pavlína Havelková

Vedoucí odboru
kompetenčního centra
kybernetické bezpečnosti
Úsek bezpečnosti SPCSS



Kdo je SPCSS?

Státní pokladna Centrum sdílených služeb, s. p.

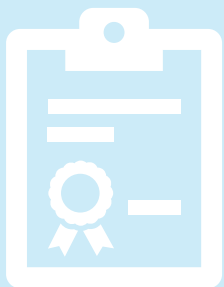
- Prvek kritické informační infrastruktury státu a zabezpečující **klíčové ICT systémy státu**
- Poskytovatel státní části **eGovernment Cloudu** (SeGC)
- Máme vysoce zabezpečená datová centra
- Splňujeme **nejvyšší bezpečnostní standardy**
- Nabízíme služby IaaS a PaaS v **nejvyšší bezpečnostní úrovni**



Požadavky na poskytovatele státního cloudu

Certifikační požadavky

- ČSN ISO/IEC 27001
- ČSN ISO/IEC 27017
- ČSN ISO/IEC 27018
- SOC 2[®] (Type II)



Bezpečnostní požadavky

- **NIS2 / nZKB**
- a doprovodná legislativa



Požadavky na poskytovatele státního cloudu

SPCSS

- **Zákon č. 365/2000 Sb.**
informační systémy
veřejné správy
- **Zákon č. 181/2018 Sb.**
kybernetická bezpečnost
- **Vyhláška č. 316/2021 Sb.**
požadavky pro zápis
do katalogu CC

OVS

- **Vyhláška č. 315/2021 Sb.**
bezpečnostní úrovně
pro používání CC
- **Vyhláška č. 190/2023 Sb.**
bezpečnostní pravidla
pro OVS využívající CC



Naše cesta



Certifikační požadavky

- 06/2016 Zakázka na výstavbu DC Zeleneč
- 02/2020 DC Zeleneč dle Tier 3
- 10/2021 Pre-assessment SOC 2
- 06/2023 Certifikace ISO 27017 a 27018
- 12/2023 Určení poskytovatelem státního cloudu
- 06/2024 Remediacce SOC 2
- 09/2024 Audit SOC 2[®] (Type II)
- 09/2025 Audit SOC 2[®] (Type II) a SOC 3[®]



Naše cesta



Schvalovací proces

- Prokazatelné naplnění VŠECH POŽADAVKŮ
- Žádost o zápis poskytovatele do katalogu CC
- Ověření poskytovatele ze strany DIA a NÚKIB
- Zápis poskytovatele do katalogu CC
- Žádost o zápis CC služeb
- Ověření služeb ze strany DIA a NÚKIB
- Zápis služeb do katalogu CC



SOC 2 Type 2 v praxi



Audit SOC 2 = soulad praxe vs dokumentace

- Ověření kontrolního rámce nad poskytovanými CC službami
- Naplnění Trust Services Criteria
 - Bezpečnost • Dostupnost • Důvěrnost
 - Integrita zpracování • Ochrana soukromí
- Testování účinnosti kontrol v čase
- Nezávislé ověření auditorem
- Roční perioda



Co znamená NIS2 / nZKB pro SPCSS?

- **Poskytovatel regulované služby v režimu vyšších povinností**
- **Poskytovatel strategicky významné služby**

Povinnosti

- Nové analýzy rizik
- Vnitropodnikové politiky
- Řízení dodavatelského řetězce
- Úprava veřejnoprávních smluv
- Nové hlášení incidentů

Rozdíly

- SPCSS se řídí přímo NIS2
- OVS se řídí nZKB

Není to 1:1



Co znamená nZKB pro OVS?

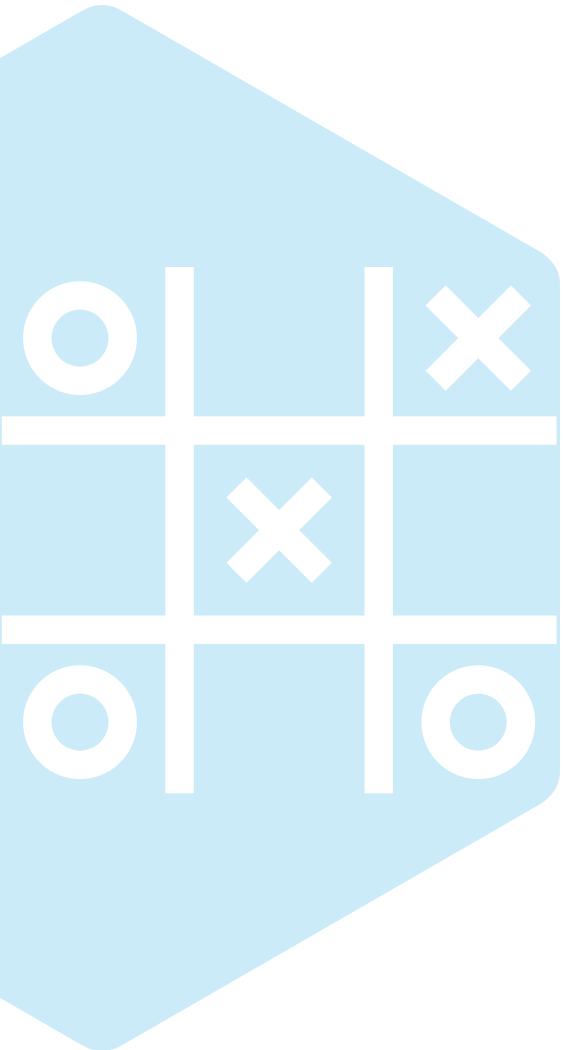


Práva zákazníka

- na **audit poskytovatele** cloudových služeb
- na informace
- na výběr jurisdikce
- ukončit službu a přenést data
- vyžadovat plnění **bezpečnostních požadavků**



Pravidla hry



Státní cloud = prověřené a standardizované služby

- Certifikovaný a auditovaný poskytovatel
 - Zákazník **NEMUSÍ** provádět vlastní audit
 - Veřejně dostupný SOC 3® Report
 - Nahlédnutí do SOC 2® Report
- Standardizované prostředí a služby
 - Politiky **NELZE** měnit dle požadavků zákazníků
- Vhodný výběr poskytovatele (z katalogu CC)
 - nebo **VLASTNÍ** datové centrum



Shrnutí

Výhody poskytovatele státního CC

- Pověřen vládou ČR
- Zápisy služeb pod
nejpřísnějším režimem
- Neděláme NIC jiného



Ještě
stihnete



- **15:40 Zámecký sál**
24/7 = KONTEJNEROVÁ PLATFORMA
BEZ LIMITŮ S ŘEŠENÍM ON-PREMISE
NEBO V CLOUDU
- **16:20 Zámecká kavárna**
HYBRIDNÍ CLOUD VE STÁTNÍ SPRÁVĚ:
NE "JESTLI", ALE "JAK"



Sledujte nás

spcss.cz/cloud



@spcss



@spcss_sp



@spcss_sp



SPCSSsp



SPCSS

Státní pokladna
Centrum sdílených služeb

Poskytovatel státní části e-Government
cloudu a ICT služeb, včetně kybernetické
bezpečnosti, pro státní správu