Požadavky služby datových center

## Zajištění služeb hostingových center, základní požadavky na DC

Technologie ISDS, které budou zajišťovat provoz následujících instancí ISDS - produkční, předprodukční, veřejný test. Produkční prostředí musí být umístěno ve dvou samostatných, navzájem propojených a geograficky nezávislých datových centrech. Součástí služeb datových center je i zajištění a provoz připojení k internetu, do CMS a k TSA. Datová centra musí splňovat všechny provozní a bezpečnostní parametry a mít platnou certifikaci Tier III nebo doložit auditní zprávou a čestným prohlášením soulad s požadavky na certifikaci Tier III.

Vývojové a interní testovací prostředí ISDS (dále VITP) bude hostováno v DC České pošty.

### **Politika fyzické bezpečnosti externích hostingových center**

Politika fyzické bezpečnosti je sestavena ve struktuře doporučené v [Vyhláška č. 82/2018; Příloha 5, odst. 1.15].

1. ***Pravidla pro ochranu objektů***
2. Výpočetní prostředky ISDS nesmí být umístěny v prostorech a lokalitách ohrožených záplavami nebo povodněmi.
3. Výpočetní prostředky musí být umístěny v prostoru vyhrazeném pouze pro výpočetní prostředky ISDS, např. v samostatné místnosti, kóji nebo skříni.
4. Fyzický přístup do vyhrazeného prostoru musí být chráněn proti neautorizovanému přístupu uzamčením vstupů a průlezů nebo signalizací s napojením na pult centrální ochrany hostingového centra.
5. Vyhrazený prostor a jeho vstupy nesmí být označeny jinak, než je obvyklé u sousedících prostorů.
6. Skla oken do místnosti/vyhrazeného prostoru musí být opatřena neprůhledným nátěrem nebo folií z vnitřní strany.
7. Dveře do objektu musí být s protipožární odolností nejméně 30 minut, zárubně pevně zasazené s betonovou výplní se závěsy z vnitřní strany objektu.
8. Okna objektu musí být zasazena do pevných rámů a musí být zajištěna venkovní nebo vnitřní mříží.
9. Ostatní vstupy a průlezy do objektu (včetně klimatizace) musí být vyzděny na plnou šířku zdi nebo zajištěny stejně jako okna (mřížemi, čidly).
10. ***Pravidla pro kontrolu vstupu osob***
11. Pro prostory, ve kterých jsou umístěny výpočetní prostředky ISDS, musí být zavedena pravidla pro kontrolu vstupu:
12. režim kontroly vstupu a výstupu osob,
13. podmínky a způsob kontroly pro vynášení aktiv,
14. režim manipulace s klíči.
15. ***Pravidla pro ochranu zařízení***
16. Objekt musí být vybaven ruční hasicí technikou, dimenzovanou podle zákonných norem.
17. V objektu musí být instalována kouřová a teplotní čidla s výstupem signalizace na pracoviště s nepřetržitou obsluhou nebo musí být instalovány automatické hasící prostředky.
18. V meziprostoru dvojité podlahy nebo bezprostředně pod volným potrubím a topidly ústředního topení je nutné instalovat čidla vlhkosti tak, aby na každé dva metry volné délky potrubí nebo topidla ústředního topení připadalo jedno čidlo.
19. Přístup k jističům a kabeláži napájení musí být umožněn jen oprávněným osobám.
20. Vypínače a jističe musí být zabezpečeny proti náhodnému a neúmyslnému vypnutí.
21. Všechny vypínače a jističe musí být označeny způsobem místně obvyklým (např. "světla", "zásuvky" apod.). Je-li přístup k rozvaděči mimo vyhrazený prostor ISDS, musí být označení prvků významově neutrální.
22. V místnosti musí být instalováno nouzové osvětlení napojené na nouzový zdroj napájení.
23. Musí být instalováno centrální zařízení pro nouzové napájení provozních systémů, které musí být v souladu s havarijním plánem a v souladu s časovým harmonogramem aktivace a deaktivace těchto zařízení.
24. ***Detekce narušení fyzické bezpečnosti***
25. Pokud prostory nejsou trvale sledovány ostrahou, musí být zabezpečeny hmotovými čidly anebo čidly pohybu.
26. Objekt musí být zapojen na elektronické zabezpečovací zařízení (dále jen EZS) a elektronické protipožární zabezpečení (dále jen EPS).
27. Signalizace EZS a EPS musí být vyvedena na pracoviště s nepřetržitým provozem.
28. Všechna čidla musí být vyvedena na samostatné smyčky, které umožní lokalizovat a rozlišit základní druhy incidentů.
29. Požární poplach musí být automaticky nebo prostřednictvím pracoviště s nepřetržitou obsluhou signalizován na Hasičský záchranný sbor.
30. V objektu musí být instalováno tlačítko tísňové signalizace, přístupné bez překážek z pultu operátora anebo od vstupních dveří.
31. Použití tísňové signalizace musí být signalizováno na pracoviště s nepřetržitou obsluhou.

## Technická specifikace

### **Racky**

1. ***Základní technické parametry Rack***

* 19“ rack o hloubce 1000 mm
* výška 42U

1. ***Minimální počty Rack***

* první hostingové centrum – 5x
* druhé hostingové centrum – 5x
* XXX – 1x

### **Požadavky a technická specifikace napájení**

* 230V
* dvě spínací jednotky PDU na rack, kde každá jednotka v racku bude na jiné napájecí větvi hostingového nebo datového centra
* všechny napájecí větve budou napojeny na elektromotorickou zálohu
* garantovaný příkon el. energie minimálně 8kW pro každý rack

### **Požadavky a technická specifikace chlazení**

* Garantovaná teplota 22°C ± 3°C
* Vlhkost v rozmezí 40% – 70%

### **Požadavky a technická specifikace datové konektivity**

1. ***Komunikace mezi dvěma DC ISDS (DC1 – DC2)***

* Komunikace mezi DC musí být postavena redundantně na dvou Dark fibre trasách nebo jiné technologii s obdobným výkonem, přibližně stejné délky.
* Každá z tras musí být zakončena moduly DWDM nebo zařízením odpovídajícím ke konkrétní technologii, které umožní požadovaný přenos mezi DC.
* Ethernet: minimálně 10x 10Gb
* FC: minimálně 4x 16G

1. ***Komunikace k CMS***

* Komunikace k CMS musí být postavena redundantně na 2 nezávislých Ethernet trasách.
* Ethernet: minimálně 2x 10Gb (z každého centra 1x 10 Gb)

1. ***Komunikace k TSA***

* Komunikace k TSA musí být postavena redundantně na 2 nezávislých Ethernet trasách ke všem TSA autoritám (TSA3 primární,TSA2 - záložní,TSA1 – pouze testování).
* Buď přes komunikaci k CMS jako je to v současnosti
* Nebo nezávislými linkami do DSČP EXTRANET
* Ethernet: minimálně 2x 1Gb (z každého centra 1x 1 Gb)

Umístění datových center:

xxx

xxx1

xxx

xxx

xxx

xxx