Provozní řád sítě 21Net

INTEGROVANÝ OPERAČNÍ PROGRAM

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
ŠANCE PRO VÁŠ ROZVOJ

ROP Střední Morava

Zlínský kraj

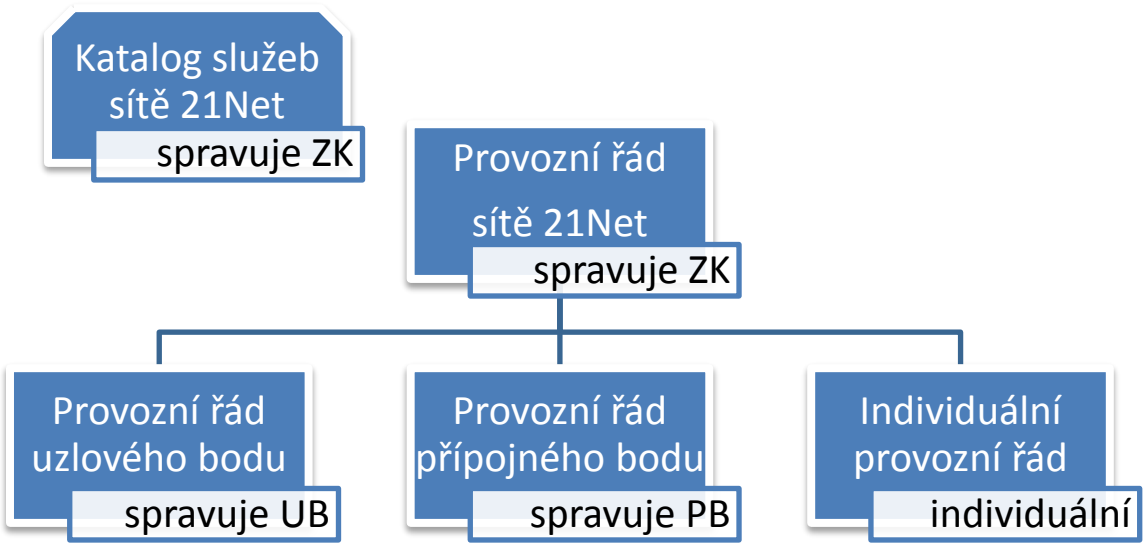
AutoCont

1.OBSAH

1. Popis dokumentu

Tento dokument popisuje podmínky, za kterých bude komunikační infrastruktura Zlínského kraje 21Net provozována a používaná jednotlivými subjekty a jejími uživateli. V dokumentu jsou dále popsány pozice a povinnosti uživatelů krajské sítě a stejně tak správců a vlastníků.

Struktura dokumentů:



Provozní řád sítě 21Net je dokument, který definuje společné podmínky fungování krajské infrastruktury. Stanovuje pravidla pro připojování subjektů, způsob čerpání služeb a další provozní úkony.

Katalog služeb sítě 21Net je dokument, ve kterém budou průběžně udržovány služby nabízené subjektům sítě 21Net, včetně příslušných SLA (service level agreement). Služby nabízí převážně ZK a externí poskytovatelé služeb, podrobnosti ohledně katalogu služeb sítě 21Net jsou uvedeny v příslušné kapitole níže.

Provozní řád uzlového bodu je dokument, ve kterém jsou popsány specifika konkrétního uzlového bodu. Jedná se převážně o popis místních podmínek z pohledu organizačního a technického zabezpečení. Vzhledem k důležitosti uzlového bodu pro chod velké části infrastruktury, jsou v tomto dokumenty detailně popsány způsoby přístupu servisních organizací k aktivním prvkům sítě 21Net, dále také popisy propojení s TC příslušného ORP a jeho MAN. Šablona tohoto dokumentu je uvedena v příloze č. 3 – Smlouva o připojení ke Komunikační infrastruktuře Zlínského kraje 21Net.

Provozní řád přípojného bodu vychází z identické šablony dokumentu jako Provozní řád uzlového bodu, nicméně z povahy přípojného bodu nejsou požadavky na rozpracovanost dokumentu tak vysoké.

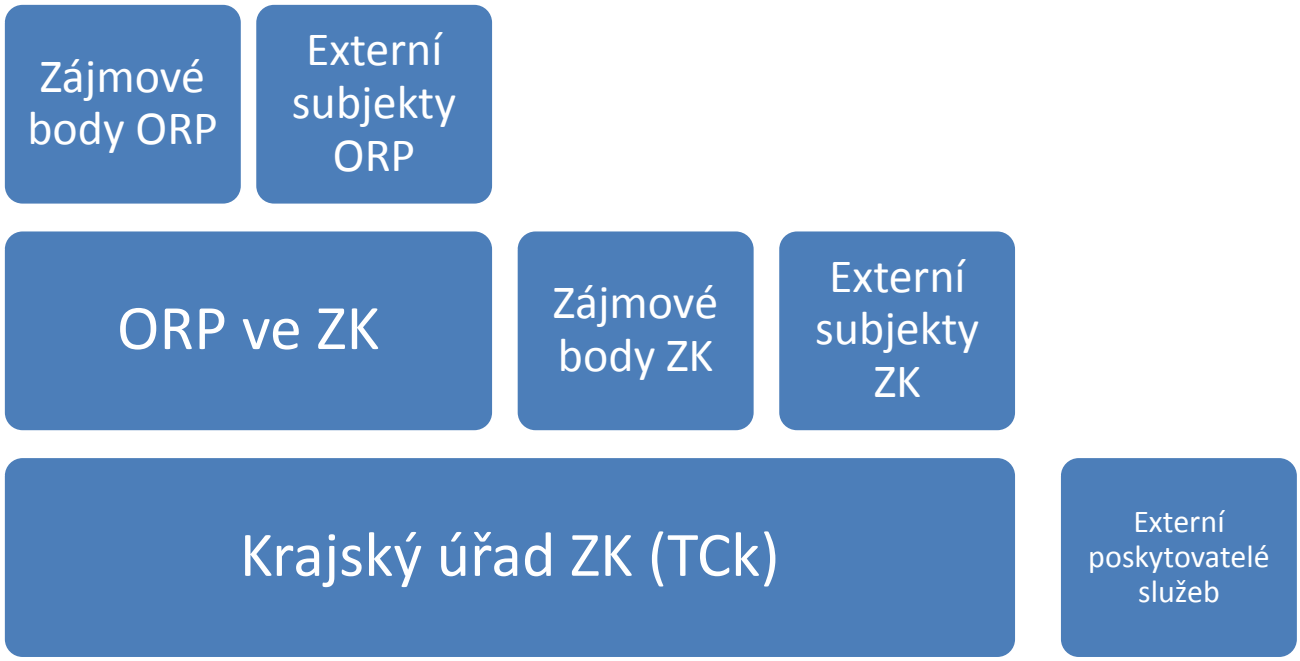
Individuální provozní řád je zpracován pro ostatní přípojné body, převážně se jedná o externí poskytovatele služeb. V tomto dokumentu je kladen důraz na popis kontaktních osob, popis předávacích rozhraní a specifikaci SLA.

2. Důvody budování sítě 21Net

Základním účelem výstavby sítě 21Net je vzájemné propojení jednotlivých technologických center (eGoncenter) v obcích s rozšířenou působností (TC ORP) s technologickým centrem Zlínského kraje (TCk) a vzájemné propojení ORP, bezpečné a bezplatné připojení těchto obcí do mezirezortních sítí skrze aktivní i pasivní část sítě 21Net. Takové síťové spojení zároveň obcím umožní přístup do sítí KIVS a zejména do centrálního místa služeb (CMS) provozovaného pod MVČR, rovněž i přístup do dalších akademických sítí, nebo do veřejných sítí, jako např. internet. Existence jednotné komunikační infrastruktury také umožní realizaci další navazujících projektů Zlínského kraje, jako například informační, vyrozumívací a varovací systém (IVVS) Zlínského kraje.

3. Kategorizace připojených subjektů

21Net rozlišuje tyto kategorie připojovaných subjektů:



3.1 Krajský úřad ZK

Krajský úřad vystupuje v roli správce sítě 21Net, zodpovídá za chod centrálních a společných částí infrastruktury, určuje koncepci rozvoje sítě a upravuje Provozní řád sítě 21Net. Krajský úřad má také roli auditora a řeší případné spory mezi zainteresovanými subjekty.

3.2 Externí poskytovatelé služeb

Pod tímto pojmem je myšleno připojení subjektů, které do sítě převážně vkládají služby. Jedná se o poskytovatele služeb (ISP, VoIP operátoři, …), také však o připojení do centrálních agendových systémů MV ČR, v první řadě jde o připojení k Centrálnímu místu služeb (CMS).

3.3 ORP Zlínského kraje

Obce s rozšířenou působností (ORP) jsou důležitou součástí sítě 21Net, jelikož uzlové body jsou umístěny převážně v jejich prostorách. Důležité je také propojení TCk s TC ORP. Předpokládá se, že v rámci připojení ORP dojde k připojení větší části infrastruktury, než jen samotného úřadu. Jedná se primárně o metropolitní sítě ORP, organizace zřizované ORP a infrastruktury poskytovatelů služeb uvnitř prostředí ORP (ISP operátoři, VoIP operátoři, …).

3.4 Zájmové body ZK

Zájmem ZK je poskytnout vytipovaným zájmovým bodům připojení do sítě 21Net a následně začít poskytovat služby těmto organizacím centrálně. Jedná se o organizace zřizované ZK, ale také o další organizace, u nichž má ZK zájem o připojení.

4. Organizační požadavky

Na subjekty připojující se k síti 21Net jsou kladeny požadavky vztahující se k definovaným funkcím a rolím, jejich odpovědnostem a povinnostem. Tyto požadavky jsou dále specifikovány z hlediska provozního a bezpečnostního.

4.1 Řízení provozu, definice rolí:

Role	Popis role	Úroveň
Vlastník sítě 21Net	představitel nejvyššího managementu (statutární orgán), podléhá rozhodnutí Rady, která podepisuje hejtman	• ZK
Správce sítě 21Net	výkonný představitel zastávající funkci administrátora sítě na centrální úrovni, provádí supervizi a zadává požadavky servisní organizaci	• ZK
Externí servisní organizace	smluvní partner Správce sítě 21Net zajišťující v rámci SLA požadované služby pro síť 21Net, příp. i pro další přípojná místa	• ZK
Bezpečnostní správce	zástupce managementu pro oblast bezpečnosti IT; výkon činností bezpečnostního správce může být delegován na externí subjekty	• ZK • ZO • ORP
Správce lokální sítě	administrátor sítě na lokální úrovni (jednotlivá přípojná místa)	• ZO • ORP
Správce objektu	osoba zajišťující fyzické zabezpečení objektu (lokality) na všech úrovních, zodpovídá za technický stav prostor a součinných systémů	• ZK • ZO • ORP
Proškolený uživatel	kontaktní osoba pro komunikaci s administrátorem sítě,	• ZO

	systémem HelpDesk, příp. externí servisní organizací v rámci SLA	• ORP
Uživatel	běžný uživatel sítě na všech úrovních	• ZK • ZO • ORP

4.1.1 Vlastník sítě 21Net

Z majetkoprávního pohledu se jedná o nejvyššího manažera sítě 21Net. Jemu podléhají všechny předešlé role a jemu jsou přímo odpovědní Správci sítě 21Net vč. externí organizace zajišťující monitoring. Rozhoduje o postupu v rozvoji sítě a schvaluje smlouvy pro zajištění chodu sítě. Má na starost finanční plánování v souvislosti se sítí 21Net a TC ZK. Sestavuje tým správců sítě 21Net.

4.1.2 Správce sítě 21Net

Správcem sítě 21Net se rozumí určený tým odpovědných pracovníků z řad KÚ, který je pověřen vykonávání supervize nad infrastrukturou. Určují směrování rozvojových požadavků, řeší sporné otázky a vyhodnocují kvalitu služeb servisní organizace (dodržování SLA).

4.1.3 Externí servisní organizace

Jedná se o organizaci, které je svěřena správa všech technologií sítě 21Net. Organizace je zodpovědná za udržování sítě v chodu se stanovenými SLA. Zaměstnanci organizace musí znát přístupové údaje k veškeré spravované technologii a k technologii musí mít zajištěn fyzický přístup, nebo jeho zajištění musí mít zprostředkované. Může kontaktovat Lokálního správce pro poskytnutí součinnosti při zjišťování, nebo odstraňování závad. Tato skupina nastavuje možnosti přístupu pro uživatele k síti a jejím aplikacím na základě žádosti přijímané od Lokálních správců, nebo přímo od uživatelů, popřípadě ze systému helpdesk KÚ, nebo z některé nadřízené role. Bezpečnostní otázky předává na Bezpečnostního správce, popřípadě vykonává patřičná opatření na základě jím definovaných postupů, nebo politik. Tato skupina je přímo odpovědná Vlastníkovi sítě.

4.1.4 Bezpečnostní správce

Osoba nespadající do správců sítě ani v jednom z předchozích bodů. Jedná se osobu nebo organizaci, vlastníkem sítě 21Net pověřenou. Bezpečnostní správce bude odpovědný za tvorbu bezpečnostních a havarijních plánů a jejich údržbu v souvislosti s provozem sítě 21Net. Bezpečnostní správce definuje politiky přístupu k aplikacím a síťovým prostředkům pro jednotlivé uživatelské role. Jeho role je spíše manažerská, nežli výkonná. Výstupy jeho práce budou podléhat schválení Vlastníkem sítě 21Net a následně budou předány k implementaci na Správce sítě 21Net a servisní organizaci.

4.1.5 Správce lokální sítě

Je osoba odpovědná za chod v místním uzlu sítě 21Net, přípojném místu ORP nebo ZO. Zodpovídá za minimální softwarové bezpečnostní vybavení koncových uživatelů. Od uživatelů ve své lokalitě přijímá požadavky na změnu jejich oprávnění, nebo přístupu k síti 21Net a ty pak následně deleguje Správci sítě 21Net prostřednictvím helpdesku KÚ. Ve většině případů bude první kontaktní osobou pro danou lokalitu ze strany správců sítě 21Net. Nejčastěji se bude jednat o již pověřeného správce místních IT prostředků, nebo technologického centra ORP nespadajícího pod 21Net. Tento uživatel může požádat o přístup ke čtení provozních dat koncových zařízení sítě 21Net např. za účelem statistického zjišťování SNMP údajů z předávacího rozhraní sítě 21Net. K umístěné technologii bude mít fyzický přístup, nebo tento přístup bude mít zajištěn prostřednictvím Správce objektu.

4.1.6 Správce objektu

Jedná se o osobu nebo oprávněný subjekt, který je vlastníkem nebo správcem dané budovy. Z pohledu sítě 21Net je držitelem přístupu k souboru techniky sítě 21Net v dané budově nebo přímo do technologického centra ORP. Tato osoba nebo subjekt musí být kontaktovatelná/ý za účelem umožnění přístupu, event. musí zajistit trvalý přístup Správci lokální sítě nebo přímo Správci sítě 21Net či pověřené Externí organizaci ke správě instalované techniky v požadovaném režimu 24x7x365. Správce objektu má možnost rozhodovat o věcech spojených s instalací techniky. Veškeré nutné stavební či jiné úpravy objektu s ním musí být předem konzultovány.

4.1.7 Proškolený uživatel

Uživatel s hlubší znalostí IT prostředí. Tato role se může překrývat s rolí lokálního správce. Proškolený uživatel má oprávnění zadávat požadavky na helpdesk KÚ. Tento uživatel je také kontaktní osobou v lokalitě, která se používá pro ověření funkčnosti služeb. Považuje se za osobu poučenou. Jeho proškolení zajistí přímo lokální správce sítě připojovaného subjektu.

4.1.8 Uživatel

Koncový uživatel, který má právo přístupu k síti. Smí využívat přidělené prostředky sítě a pracovat v poskytnutých aplikacích. Ze své pozice nemá právo měnit nebo upravovat konfiguraci sítě, ani jinak zasahovat do chodu sítě jako takové. Své požadavky na případné změny v oprávnění nebo přístupu k aplikacím deleguje na svého Správce lokální sítě, respektive Správce sítě 21Net výhradně prostřednictvím systému helpdesk KÚ.

4.1.9 Naplnění rolí

Vlastník sítě 21Net – Zlínský kraj

Správce sítě 21Net – Ing. Tomáš Martinek

Externí servisní organizace – */bude doplněno/*

Bezpečnostní správce 21NET - Ing. Fux Jiří

Naplnění rolí a kontaktní údaje osob připojených subjektů jsou uvedeny v přílohách Smlouvy o připojení ke Komunikační infrastruktuře Zlínského kraje 21Net č. 3 a 4.

4.2 Kontaktní informace

4.2.1 Písemný styk

Pro komunikaci v listinné podobě je vyžadováno adresovat komunikaci na:

RNDr. Ivo Skrášek
Oddělení informatiky
Odbor Kancelář ředitele
Krajský úřad Zlínského kraje
třída Tomáše Bati 21, 761 90 Zlín

Pro elektronické podávání požadavků je preferovaný způsob zadávání pomocí webového formuláře, v případě nutnosti však lze použít emailovou adresu helpdesk.21net@kr-zlinsky.cz

Pro ostatní komunikaci, jako např. pokládání dotazů ohledně 21NET, lze použít emailovou adresu info.21net@kr-zlinsky.cz

4.2.2 Telefonický styk

Pro hlášení závad lze použít telefonní číslo +420 577 0xx xxx*(bude doplněno)*, nicméně pouze v případech, kdy nelze použít hlášení pomocí webového formuláře helpdeskového systému.

Pro ostatní záležitosti informačního charakteru je možné kontaktovat Ing. Tomáše Martinka, +420 577 043 266.

4.2.3 Portál 21Net

Pro centrální distribuci informací zřídil krajský úřad ZK portál 21Net, na kterém jsou detailní informace o topologii sítě, je určen pro umístění provozních řádů a dalších dokumentů. Jedná se také o místo, kde budou umisťovány aktuální informace o stavu sítě, jedná se například o plánované výpadky, změny stavu sítě apod.

Portál je dostupný na URL http://www.21net.cz

4.2.4 Elektronické kontaktní místo – Helpdesk

Helpdeskový systém slouží jako **primární místo** pro zadávání požadavků, jak je popsáno v kapitole níže. Helpdeskový systém je provozován externí servisní organizací a je dostupný na URL http://www.21net/helpdesk/.

4.2.5 Katalog služeb sítě 21Net

Katalog služeb sítě 21Net je umístěn na URL http://www.21net.cz/katalog-sluzeb/

4.2.6 Formuláře pro písemný styk

Formuláře sloužící pro písemnou komunikaci jsou umístěny na http://www.21net.cz/forms/

4.3 Provozní postupy

4.3.1 Žádost o připojení k síti 21Net

O připojení subjektu do sítě 21Net žádá zodpovědná osoba organizace pomocí příslušného formuláře (viz. příloha č. 1) emailem na adresu helpdesk.21net@kr-zlinsky.cz. Po schválení žádosti předkládá správce sítě 21Net návrh na uzavření smlouvy mezi subjektem a ZK k rukám rady ZK. Schválením rady ZK dochází k uzavření smlouvy a následně k připojení subjektu do sítě 21Net (realizuje externí servisní organizace v součinnosti s připojovaným subjektem).

4.3.2 Žádost o přístup ke službě

Připojené organizace mohou požádat o přístup ke službám, které jsou uvedeny v katalogu služeb sítě 21Net na URL http://www.21net.cz/katalog-sluzeb/. Žádost musí být realizována prostřednictvím helpdesku sítě 21Net. Přístup ke konkrétním službám schvaluje provozovatel služby uvedený v katalogu služeb (dle konkrétní služby může být nutno uzavření smluvního vztahu s provozovatelem, toto zajišťuje připojovaný subjekt samostatně). Po schválení provozovatelem je požadavek předán externí servisní organizaci k realizaci.

4.3.3 Servisní požadavek

Servisním požadavkem se rozumí hlášení závady, nedostupnosti připojení, popřípadě snížení kvality poskytovaných služeb. Servisní požadavky se hlásí na helpdesku sítě 21Net, primárně pomocí webového formuláře, v případě nutnosti lze také emailem nebo telefonicky. Požadavky jsou řešeny dle reakčních časů jednotlivých služeb uvedených v katalogu služeb. Způsob řešení požadavků je blíže popsán v kapitole č. 6.

4.3.4 Změnové požadavky

Změnovým požadavkem se rozumí požadavek na změnu parametrů služby, změnu kontaktních informací, požadavek na součinnost ze strany správce sítě 21Net a další nekritické požadavky. Změnové požadavky se hlásí na helpdesku sítě 21Net, primárně pomocí webového formuláře, v případě nutnosti lze také emailem nebo telefonicky. Požadavky jsou řešeny dle reakčních časů jednotlivých služeb uvedených v katalogu služeb. Způsob řešení požadavků je blíže popsán v kapitole č. 6.

4.3.5 Předávání provozních informací

Tento typ požadavku slouží k informování správce sítě 21Net o provozních informacích na straně připojeného subjektu. Nejčastěji se jedná o plánované výpadky napájení a podobně.

5. Smluvní požadavky

5.1 Smlouvy a dohody pro připojení k síti 21Net

V rámci plnění služeb je požadováno, aby přípojná místa uzavřela s vlastníkem sítě 21Net Smlouvu o připojení ke Komunikační infrastruktuře 21Net. Tato smlouva upravuje mimo jiné následující oblasti:

- závazek řídit se při přístupu k síti 21Net v souladu s provozním řádem sítě 21Net
- poskytování součinnosti servisním organizacím ZK
- udržování aktuálních provozních řádů uzlového bodu/přípojného bodu
- dohody o úrovni poskytovaných služeb, tzv. SLA
- katalog služeb sítě 21Net

6. Servis a SLA požadavky

Pro udržení nepřetržitého chodu sítě musí existovat systém střídání pověřených pracovníků dohledu z týmu Správců sítě 21Net, nebo pověřené Externí organizace, jež bude tuto činnost smluvně zajišťovat. Takový pracovník musí být vybaven patřičnými technickými prostředky pro případné servisní zásahy. Musí mít k dispozici seznam telefonních kontaktů na všechny Lokální správce a Správce objektů, kde je technologie situována.

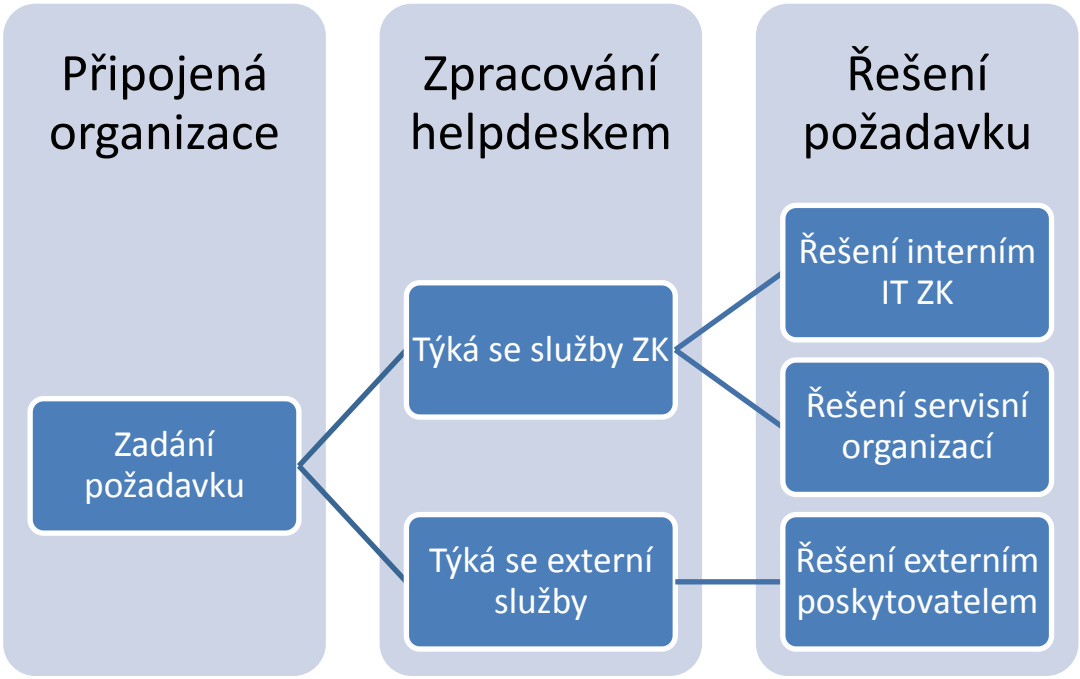
Pokud se jedná o závadu techniky nebo služby, která je zároveň kryta některým typem SLA smlouvy, bude tento požadavek na odstranění delegován na servisní organizaci. Delegaci provede vždy odpovědný pracovník ze skupiny Správců sítě 21NET.

Plánované odstávky musejí být avizovány minimálně 3 pracovní dny dopředu, v případě závažných oprav může být tento čas zkrácen, a proto musí být zřízeno místo, nejlépe internetová nebo intranetová webová stránka, pomocí které budou uživatelé o problémech notifikováni. Na témže místě musejí být uvedeny aktuální závady a průběh jejich řešení. Plánované odstávky musejí být také oznámeny e-mailem zaslaným na Správce lokální sítě.

6.1 Způsoby zadávání požadavků

Požadavky jsou zadávány oprávněnou osobou na helpdesku sítě 21NET pomocí výše uvedených kontaktů.

Helpdesk sítě 21NET je jediným kontaktním místem, provozovatel helpdesku rozděluje (automaticky nebo manuálně) jednotlivé požadavky na příslušné řešitele. Proces zpracování vypadá následovně:



6.2 Základní podpora, SLA 8x5 NBD

Základní zajištění chodu. Svým rozsahem pokrývá pracovní dobu v pracovních dnech pro nahlášení závady s nejzazší reakcí na podnět v dalším pracovním dnu.

Pracovní doba je definována takto:

- pondělí, středa 7:30 – 17:00
- úterý, čtvrtek, pátek 7:30 – 16:00

Do této kategorie požadavků spadají nekritické hlášení, rozvojové a změnové požadavky

6.3 Zvýšená podpora, SLA 24x7x365

Řešitelem v těchto případech bude smluvně vázaná servisní organizace, určená Vlastníkem sítě 21Net, nebo výrobce nebo dodavatel dané služby.

Do této kategorie spadají požadavky, které mají přímý dopad na chod sítě 21Net. Požadavky jsou zakládány dohledovým systémem sítě 21Net, správcem sítě 21Net, popřípadě lokálními správci uzlových bodů.

6.4 Odpovědnost za provoz

Za provoz sítě během běžné pracovní doby je odpovědný správce sítě 21Net, ten však může svou zodpovědnost delegovat na externí servisní organizaci.

7. Technické požadavky

7.1 Technické podmínky pro připojení k síti 21Net

7.1.1 Hardwarové požadavky

V každé přípojné lokalitě bude zakončen optický propoj, ke kterému bude připojen aktivní prvek sítě 21Net (ve vlastnictví ZK), ten bude předávacím rozhraním a oddělujícím prvkem mezi infrastrukturou připojovaného subjektu a sítě 21Net. Fyzickým médiem bude rozhraní ethernet 10/100/1000Base-T, individuálně však lze dohodnout také předání na optickém ethernet rozhraní.

7.1.2 Funkční požadavky

Předpokládá se, že jednotlivé služby sítě 21Net budou při výstupu ze sítě 21Net odděleny pomocí technologií VLAN (protokol 802.1q), je proto požadováno, aby koncový prvek připojovaného subjektu tuto technologii podporoval a aby dodržoval oddělení těchto virtuálních sítí. Centrálně byl stanoven rozsah ID VLAN od 2000 do 2599, pro jednodušší zprovoznění připojení je doporučeno, aby připojovaný subjekt tyto ID nepoužíval.

7.1.3 IP adresní plán

V rámci celé síti 21Net byl definován adresní plán, z něhož budou připojovaným subjektů přidělovány IP adresy pro komunikaci se službami sítě 21Net. Adresní blok, který byl pro toto vyhrazen: 10.20.0.0-10.25.99.0. Je vyžadováno, aby žádný ze subjektů nepoužíval tento rozsah adres, pokud jej však již používá, je vyžadováno použití překladu adres tak, aby byly vnitřní adresy subjektu izolovány od adresného prostoru 21Net.

7.1.4 Monitoring koncových bodů

Na koncových bodech, musí být zajištěno, že centrální monitoring sítě 21Net bude testovat dostupnost těchto zařízení nebo monitorovat jejich dostupnost a kvalitu spojení. Požaduje se proto, aby na koncových zařízeních byly konfigurovány následující přístupy pro správu sítě 21Net:

Požadované přístupy pro správu sítě 21Net:

- Odezva na ICMP typ 8 – echo ping.
- SNMP – přístup RO ke komunitě Public. Kontrola dostupnosti zařízení, grafy provozu.

Další možné požadavky se odvíjí od konkrétních typů koncových zařízení a jejich možností. Konfiguraci těchto prvků provede Lokální správce, případně Správci sítě 21Net po dohodě, popřípadě tímto pověřená organizace.

7.1.5 Doporučení pro použití aktivních prvků

Pro připojení k síti 21Net je doporučeno využití firewallu o dostatečném výkonu (vzhledem k zamýšleným odběrům služeb). Vhodné je, aby firewall podporoval NAT, dynamický směrovací protokol OSPF a VLAN sítě (alespoň 5 aktivních VLAN). Přesné doporučení nelze stanovit, konkrétní konfigurace je přímo závislá na datových tocích a nastavené bezpečnostní úrovni.

Pro použití v prostředí byly otestovány následující aktivní prvky:

1. Cisco ASA5505 – pro přípojky do rychlosti 50Mb/s
2. Foftinet Fortigate 60C – pro přípojky do rychlosti 50Mb/s
3. Juniper SRX210 – pro přípojky do rychlosti 50Mb/s

Pro výběr aktivního prvku pro vyšší rychlosti, popřípadě při jakýchkoli nejasnostech se lze obrátit na správce sítě 21Net pomocí výše uvedených kontaktů.

7.2 Ochrana dat o provozu sítě

Zařízení ve vlastnictví kraje musí být pravidelně zálohována, tyto zálohy zajišťuje servisní organizace. U aktivních prvků toto předpokládá zálohu s každou změnou konfigurace daného prvku. Zálohy spravuje servisní organizace, která je také uchovává na svých zálohovacích systémech. Kopie záloh jsou bezodkladně předány správci sítě 21Net (min. 1x týdně).

Konkrétní procesy záloh odpovídají stanovené Bezpečnostní politice.

7.3 Kontroly a revize zařízení

Je vyžadováno, aby subjekt, kde je umístěno zařízení ve vlastnictví ZK umožnil přímý přístup k těmto technologiím za účelem fyzické kontroly a inventarizace. O těchto návštěvách bude Vlastník budovy, popřípadě Lokální správce dopředně informován, u jejich provádění může být přítomen. Periodu kontrol stanoví Vlastník sítě 21Net ve spolupráci se Správci sítě 21Net, nebo tímto pověřenou Externí organizací. Fyzické kontroly budou přednostně prováděny v pracovní dny v době 7:00 – 16:00, pokud nebude dohodnuto jinak.

Revize elektrických zařízení je správce objektu připojené organizace povinen provádět dle požadavků příslušných vyhlášek a zákonů, nebo dle požadavků výrobce, tam kde zákon periodu přímo neurčuje.

8. Bezpečnostní požadavky

Tato kapitola slouží jako souhrn požadavků, které jsou kladeny na všechny připojované subjekty. Cílem je definovat bezpečnostní standard pro jednotlivé typy bodů. Detailní nastavení pro specifické body je popsáno v příslušných provozních řádech jednotlivých bodů a to i včetně výjimek oproti globálním požadavkům.

8.1 Požadavky na uzlové body

8.1.1 Definice bezpečnostního perimetru

Bezpečnostním perimetrem je myšlen souhrn fyzických, technických a technologických opatření, která tvoří hranice chráněného objektu v lokalitě. Tímto objektem je tzv. zabezpečená místnost, ve které se nachází infrastruktura sítě – přípojný bod k síti 21Net. Správce lokální sítě přípojného bodu ve spolupráci s Bezpečnostním správcem a Správcem objektu musí zajistit, aby zabezpečená místnost s veškerou infrastrukturou splňovala stanovené minimální provozně-bezpečnostní požadavky v následujících oblastech, přičemž u každé z nich musí být definovány role a odpovědnosti.

8.1.2 Prostředky objektové ochrany

- lokalita musí být umístěna mimo záplavové území,
- zabezpečená místnost musí být umístěna uvnitř zděné budovy na pevném základě odolném proti chvění/otřesům,
- zabezpečená místnost musí být umístěna v nadzemním podlaží (nikoliv pod úrovní terénu),
- objekt, v němž se nachází zabezpečená místnost, musí mít zajištěnu nepřetržitou vnější ostrahu nebo musí být alespoň elektronické zabezpečení napojeno na pult centrální ochrany bezpečnostní služby s povinností zásahu na místě v případě poplachu,
- musí být zajištěna ochrana před neoprávněným vniknutím mechanickými zábranami (mříže na oknech až do výšky 2. nadzemního podlaží včetně, mříže na vstupních dveřích nebo bezpečnostní dveře včetně rámu),

- vstupní dveře, resp. dveře *rack*ových skříní musí být opatřeny bezpečnostním zámkem (v případě sdílené místnosti),
- musí být nainstalován EZS a čidla pohybu s napojením na dispečink (centrální dohledový systém) na vstupních dveřích (příp. RMS *rack*ových skříní), na oknech, vstupu/výstupu kabeláže/komunikačních kanálů (umožňuje-li jejich rozměr vstup do místnosti),
- vedení kabeláže/rozvodů do/ze zabezpečené místnosti musí být zabezpečeno např. zasekáním ve zdi, umístěním do krytého žlabu nebo alespoň v lištách,
- musí být nainstalován EPS včetně automatizovaného zhášecího systému s napojením na dispečink (centrální dohledový systém),
- v uzlových bodech musí být nainstalován kamerový systém se záznamem určený k zajištění bezpečnosti technologického vybavení v zabezpečené místnosti.

8.1.3 Fyzický přístup a jeho zabezpečení

- musí být vedena průkazná evidence personálního obsazení rolí s povoleným fyzickým přístupem (včetně servisních organizací, údržby a úklidu),
- musí být vedena průkazná evidence „klíčového hospodářství“ (bezpečné uložení, přidělování, blokování a odebírání klíčů, čipů/přístupových karet, vstupních kódování),
- musí být vedena průkazná evidence fyzického vstupu všech osob (např. prostřednictvím EZS),
- musí být zajištěn nepřetržitý přístup oprávněných osob do zabezpečené místnosti.

8.1.4 Bezpečnost prostředí

- musí být zajištěn dostatečný zdroj stabilní dodávky elektrické energie (v souladu se specifikací technického řešení),
- pro případ přerušení dodávek musí být zajištěn záložní zdroj elektrické energie (např. diesel-agregát s automatizovaným nebo manuálním spuštěním),
- musí být implementován nepřerušitelný zdroj energie (UPS) o dostatečné kapacitě k udržení provozu minimálně po dobu potřebnou k automatizovanému nebo manuálnímu spuštění a náběhu náhradního zdroje elektrické energie, včetně automatizovaného systému upozornění (tzv. alerting) a zasílání hlášení prostřednictvím protokolu SNMP,
- musí být instalována klimatizace a další vybavení, zajišťující bezprašné a suché prostředí, vytápění, resp. chlazení a větrání místnosti odpovídající provozním požadavkům,
- v celé místnosti musí být zajištěno dostatečné osvětlení (pracovní, nouzové),
- musí být zajištěno provádění pravidelných revizí elektrických zařízení ve lhůtách stanovených dle příslušných předpisů (zákony, vyhlášky, normy, technická dokumentace zařízení, doporučení výrobce/dodavatele).

8.1.5 Bezpečnost infrastruktury

Fyzická úroveň bezpečnosti infrastruktury je daná její lokací. Bylo stanoveno, že technologie bude uložena v zamykatelných racích. Každá lokalita bude navíc vybavena tzv. RMS systémem pro monitoring prostředí, nebo jenom daného racku. Na RMS systém musí být vybaven environmentálními čidly – kouřové, vlhkostní, teplotní. Systém RMS musí komunikovat s centrálním dohledovým systémem.

Technologická místnost, popřípadě rack s technologii musí být dohlížen centrálním kamerovým systémem. Technologické centra TC ZK budou vybaveny počtem min. 3 IP kamer, ostatní síťové uzly jsou vybaveny jednou kamerou, kontrolující prostor technologického racku sítě 21Net. V případě pohybu osoby v prostoru racku je pořízen a uschován kamerový záznam, alespoň po dobu jednoho kalendářního měsíce zpět.

Při zjištění změny prostředí (kouř, voda, teplota) je vygenerován alert na Správce sítě 21Net prostřednictvím centrálního monitoringu.

- Síťová komunikace podléhá kontrole provozu. Veškerá komunikace přicházející z perimetru sítě je skenována pomocí nástrojů IPS/IDS.

- Vnitřní komunikace v síti 21Net podléhá také monitoringu. Nasazeny jsou systémy logující uskutečněná spojení a to i směrem do jiných sítí včetně sítí veřejných. Zároveň dochází ke kontrole těchto spojení, zda nevybočují ze standardního rámce běžného, bezpečného chování. V případě, že je zjištěna zásadní změna, nebo rozdíl v počtu toků oproti normálu, je vygenerována výstraha, která je předána k analýze a případnému vyřešení správcům sítě 21Net, nebo dohlížející Externí organizaci. V případě zjištěné nežádoucí komunikace uživatele, bude tento vyrozuměn a přístup k síti mu může být do vyřešení problému omezen, nebo dokonce odepřen.

Z pohledu uživatele sítě, se v případě sítě 21Net jedná o uzavřený, bezpečný komunikační celek, fungující na základě definovaných pravidel a bezpečnostních politik. Skrze tuto síť je obcím umožněn bezpečný přístup k externím zdrojům pomocí celé řady mechanizmů kontroly, přičemž je jedno zda se jedná o mezirezortní sítě, akademické sítě nebo Internet. V synergii se sítí 21Net může být k přenosu dat využito i jiných projektů, například projekty Střecha nebo ITS NGN.

8.1.6 Kontinuita provozu

Pro zajištění požadavku nepřetržitého provozu sítě je nezbytné, aby správce lokální sítě zajistil (na základě smlouvy a za předem stanovených podmínek) možnost vzdáleného monitoringu klíčových prvků/komponent sítě správcem sítě 21Net. Další požadavky vyplývají z nutnosti zajistit minimalizaci, resp. prevenci výpadků sítě na všech úrovních:

- musí být zabezpečeny specifikované kapacitní nároky na provoz sítě, případně implementovány redundantní/duplicitní/záložní/virtuální prvky podporující sledování výkonu, příp. rozdělení/převzetí zátěže apod.,
- musí být zajištěn dostatečný servis a údržba klíčových prvků sítě externími smluvními dodavateli služeb v takovém rozsahu, který odpovídá požadavkům na provoz sítě,
- musí být implementován systém pro zálohování systému/konfigurace minimálně po každé změně v nastavení,
- musí být dokumentován postup zálohování a obnovy ze záloh, evidence záloh, testování správnosti/čitelnosti záloh, bezpečné úložiště záložních médií a bezpečná likvidace nepotřebných záloh (ať už fyzických médií, nebo dat),
- musí být veden (a také zálohován) provozní deník zařízení se záznamem každé změny týkající se chodu sítě 21Net,
- musí být dokumentovány procesy, postupy, odpovědné role, reakce a činnosti následující po přerušení provozu.

8.2 Požadavky na přípojné body

Je požadováno, aby umístění infrastruktury síti 21Net v přípojném bodě bylo chráněno proti zneužití a proti zcizení. Umístění musí být zdokumentováno a zaneseno do příslušného provozního řádu.

9. Sledování a monitoring

Nasazení kontrolních a monitorovacích systémů a mechanizmů v síti 21Net je nutné z hlediska bezpečnosti a kontinuity provozu napříč všemi úrovněmi sítě, avšak tyto systémy jsou vyhodnocovány jednotně na centrální úrovni. K těmto systémům je vždy přiřazena osoba, nebo Externí organizace, odpovědná za vyhodnocování jejich výstupů. Je-li výstupem z monitoringu servisní incident, musí být bezodkladně předán k řešení. V případě bezpečnostního incidentu, je předán k dalšímu prošetření Správcům sítě 21Net, kteří uváží další postup k účinnému odstavení narušitele. O této události spraví Bezpečnostního správce.

9.1 Bezpečnost datového provozu

Základním předpokladem k bezpečnému provozu v síti 21Net je mimo zajištění síťových přenosových systémů pasivních i aktivních ochrana koncových uživatelů a jejich pracovních stanic. Volba konkrétních produktů pro ochranu stanic je na Lokálních správcích, popřípadě na doporučení Správců sítě 21Net.

Základním požadavkem vůči ORP je, že operační systémy na stanicích musejí být pravidelně aktualizovány a záplatovány. Tyto aktualizace by neměly být starší jednoho měsíce. Zároveň se požaduje, aby na stanicích byl zapnutý personální firewall, za dostatečný se považuje integrovaný v systému. Správu uživatelské bezpečnosti vzhledem k malware hrozbám by měl zajistit a kontrolovat Lokální správce, například formou patřičných GPO politik či jiným technickým způsobem, tak aby tato nastavení nemohl koncový uživatel negativně ovlivňovat. Na stanici musí být instalován produkt zajišťující ochranu stanice před malware hrozbami, ideálně ve spojitosti s antivirovým programem. Doporučuje se nasazení centrální správy těchto systémů v lokalitě, tak aby bylo možné zajištění požadované bezpečnosti pomocí politik pod kontrolou Lokálního správce.

V přípojných lokalitách bude povinností uživatelů mít nainstalovaný a aktivní personální firewall, antivir a antispam ochranu s aktuálními definicemi a nainstalované bezpečnostní aktualizace operačního systému. Nicméně v těchto lokalitách typicky není Lokální správce a nelze garantovat, že uživatel bude mít i přes tuto povinnost zapnutý personální firewall na své stanici, musí zde být proto aplikována omezující bezpečnostní pravidla pomocí ACL na přípojném prvku k síti 21Net, tak aby se zamezilo vstupu nežádoucích datových toků. Za bezpečnost a aktuálnost systému své, připojené stanice je pak odpovědný její uživatel.

9.2 Nutné vybavení organizace

Připojená organizace musí zajistit použití prostředků pro zajištění nutné bezpečnosti stanic svých uživatelů. Na stanicích ORP musí být instalován alespoň antivirový systém, který nesmí mít virové definice starší 3 dny nazpět. Doporučeno je, aby se jednalo o antivirový systém schopný reagovat i na malware hrozby, variantně může být nasazen samostatný software k tomu určený, tzv. antimalware. Opět je doporučeno tuto otázku řešit centrálně, tedy nasazením takového AV systému, nad kterým jsou aplikovatelné politiky a zamezí tak možnosti negativního zásahu ze strany uživatele. Do nutného vybavení i v tomto případě spadá aktualizovaný operační systém stanic, viz předchozí bod. Za nastavení vedoucí k požadované úrovni vybavení je odpovědný Lokální správce.

V místech bez Lokálních správců je za vybavení své stanice odpovědný přímo uživatel. Musí na své stanici zajistit stejnou úroveň jaká je popsaná výše.

9.3 Nepodporovaný obsah

Všichni uživatelé sítě 21Net musejí být poučeni o povinnosti respektovat při užívání sítě pouze stanovený účel, způsob a povolený obsah související s jejich určením a činností.

Nezákonným obsahem jsou míněny např. zveřejňované materiály, resp. činnost v síti týkající se:

- pohlavního zneužívání dětí či nezákonných sexuálních praktik,
- podněcování k teroristickým činům,
- nezákonného velebení násilí, terorismu, rasismu a xenofobie
- podněcování k rasové nenávisti,
- propagace násilí,
- páchání trestných činů podvodů či padělání,
- podněcování k násilnému a jinak závažnému nezákonnému chování,
- napadení informačních systémů (útoky typu „denial of service“ a hacking).

Nepodporovaným obsahem jsou míněny jakékoliv materiály, které přímo či nepřímo nesouvisí s účelem, určením a povoleným obsahem sítě 21Net.

Porušení uvedené povinnosti se rovná závažnému porušení smluvních závazků/dohod, případně i zákona se všemi důsledky a sankcemi z toho vyplývajícími. V případě detekce takového porušení je vlastník sítě 21Net, resp. správce sítě oprávněn po posouzení charakteru, případně s ohledem na význam, hrozbu, dopad a četnost opakování zjištěného porušování této povinnosti:

- upozornit určenou kontaktní osobu příslušného přípojného místa/uživatele na porušení povinnosti, a vyzvat k zásahu/okamžité nápravě/odstranění nežádoucího stavu,
- zajistit neprodleně nápravu vlastními silami, není-li možné např. z technických důvodů toto požadovat po uživateli,
- oznámit toto porušení dle jeho charakteru příslušnému orgánu/roli (např. informovat vlastníka sítě 21Net, správce sítě, bezpečnostního správce, orgány činné v trestním řízení),
- pozastavit plnění nebo i odstoupit od smlouvy o poskytování služeb s přípojným místem, pokud toto porušování trvá, nebo dokud nebylo odstraněno,
- okamžitě odepřít/zablokovat přístup tomuto uživateli, zejména jedná-li se o činnost ohrožující provoz a bezpečnost sítě,
- požadovat náhradu škod způsobených dopadem takového jednání.

Vlastník sítě 21Net neodpovídá za vlastní porušení účelu a určení sítě 21Net kterýmkoliv z uživatelů přípojných míst.

9.4 Inspekce datových toků

Vlastník 21Net si vyhrazuje právo na inspekci datových toků pro účely detekce nepovoleného obsahu, popřípadě jiných anomálií.

10. Sankce

V případě zjištění porušení podmínek specifikovaných v provozních řádech, je správce 21Net oprávněn dočasně omezit čerpání služby, popřípadě ji úplně odepřít a to až do odstranění závad.

11. Přílohy

Příloha č. 1 – Šablona žádosti o připojení ke 21Net

Žádost o připojení subjektu k síti 21Net

Identifikační údaje

Připojovaný subjekt	
Se sídlem	
Adresa přípojného bodu	
Pověřený zástupce	Starosta
Technický garant	IT správce

Kontaktní osoby

Níže uvedené osoby jsou k dispozici při zprovozňování připojení

1. externí správce, kontakt
2. elektrikář, kontakt
3. správce budovy, kontakt
4. …

Níže uvedené osoby jsou oprávněny kontaktovat helpdesk sítě 21Net dle podmínek provozního řádu sítě 21Net

1. jméno, email, tel, interní funkce, role vůči síti 21Net (lokální správce/proškolený uživatel)
2. jméno, email, tel, interní funkce, role vůči síti 21Net (lokální správce/proškolený uživatel)
3. jméno, email, tel, interní funkce, role vůči síti 21Net (lokální správce/proškolený uživatel)

Odůvodnění

Žádáme o připojení k síti 21Net z následujících důvodů (předpokládáme čerpání následujících služeb):

- vykonáváme činnost xxx a potřebujeme přístup do agendy zzz
- předpokládáme čerpáni služeb TCk
- předpokládáme čerpání služby připojení k internetu

Prohlašujeme, že jsme se seznámili s provozním řádem sítě 21Net (dostupný na http://www.21net.cz)

Zároveň souhlasíme s vedením aktuální evidence informací o přípojném bodě následujícím rozsahu (šedě jsou zvýrazněny povinné položky, ostatní pole jsou volitelná):

Druh informace	Popis	Nápověda
Identifikace přípojného bodu (PB)		interní označení (např. UH56_ORP)
Adresa umístění PB		kompletní adresa
Druh budovy PB		např. sídlo městského úřadu, škola,…
Identifikace provozovatele PB		jméno, IČ, sídlo, statutární zástupce, kontakt
Standardní provozní doba PB		
Bližší specifikace		např. 2 patro, č. dveří 205

umístění PB		
Podrobný popis přístupu k PB		např. po vstupu do hlavního vchodu je nutno projít přes turniket ve vrátnici a prokázat se OP, dále pak po schodech na levé straně do druhého patra, kde na konci chodby po pravé straně jsou dveře s označením 205, kterými se po otevření pomocí čipové karty vejde do serverovny
Kontaktní informace na správce budovy		
Kontaktní informace na správce serverovny		pokud existuje
Kontaktní informace na bezpečnostního technika		
Stavební materiál budovy		panel, cihla,…
Půdorysný plán budovy		
Půdorysný plán serverovny		+ vyznačení kde je umístěn rack a plánovaný přívod konektivity/elektriky do racku
Fotodokumentace		objektu z venku, vstupních dveří do objektu, vstupu do serverovny, serverovny, umístění racku, detail racku i zařízení, všechny možné vstupy (dveře, okna, větrací šachty,…)
Je objekt v zátopové zóně		
Hrozí u objektu vyšší nebezpečí živlů?		např, kolem teče řeka, sousedí s továrnou na výrobu výbušných látek,…
Existují nějaké jiné fyzické či enviromentální hrozby?		např. objekt je poddolován, kolem objektu jsou vysoké stromy, objekt nemá hromosvod, dveře do serverovny se nezamykají, po objektu se pohybují externí lidé bez evidence na vrátnici, zdi serverovny jsou ze sádrokartonu a do vedlejší místnosti je volný přístup,...
Přibližný dojezdový čas či vzdálenost HZS		
Přibližný dojezdový čas či vzdálenost ostrahy		Bezpečnostní agentura, PČR, najmutý strážný,…
Kdo a v jakém režimu objekt střeží v pracovní době		Informace o bezpečnostní agentuře, PČR apod. včetně kontaktních informací, případně o vrátném a spojení na něj
Kdo a v jakém režimu objekt střeží mimo pracovní dobu		Informace o bezpečnostní agentuře, PČR apod. včetně kontaktních informací, případně o vrátném a spojení na něj
Za jakých podmínek se dá do objektu dostat		kam telefonovat, co je kontrolováno (OP, osobní průkazka), příp. evidováno (zápis do knihy návštěv, elektronická čtečka OP,…)
Kdo má přístup do		jak v pracovní době tak mimo ní

objektu, kdo přístupy schvaluje		
Jaké je pasivní zabezpečení vstupu do serverovny		pasivní prvky (dveře, zámky, mříže, okna)
Jaké je aktivní zabezpečení vstupu do serverovny		aktivní prvky (PCO, EZS, EPS, CCTV) + typy a u CCTV jakým způsobem se zaznamenává (kontinuelně, motion detection,…). Jou technologie připojeny na UPS?
Druh přístupu		bezpečnostní klíč, čipová karta, snímač zornice, atp. (jak pro vstup do serverovny, tak do racku)
Je rack vyhrazen výhradně pro PB		je/není (jaké cizí technologie jsou v něm obsaženy)
Jak je zabezpečen provoz technologií		např. klimatizace, UPS, dieselagregát, přívod el. proudu z více zdrojů, zhášecí systém + jejich typy (jsou tyto technologie vlastníka budovy a nebo součástí PB)
Popis serverovny (technologické místnosti)		jaké jsou zde cizí technologie, počet racků a hrubý popis vybavení (servery, diskové pole, UPS, tel. ústředna apod.)
Je (příp. jaká) dostupná stávající dokumentace k fyzické bezpečnosti		popis fyzického/objektového zabezpečení, tj. správa budovy/místnosti, fyzický přístup, přístup třetích stran, servis, úklid, revize, EZS, EPS, ostraha apod.
Je (příp. jaká) dostupná stávající dokumentace k organizační bezpečnosti		popis organizačního zajištění, tj. jaká je hierarchie řízení PB, zaměstnanci, příp. externí pracovníci, dodavatelé služeb, kompetence, pravomoci a odpovědnosti
Je (příp. jaká) dostupná stávající dokumentace k technické bezpečnosti		popis ICT bezpečnosti, tj. technické/technologické bezpečnostní prvky systému
Je (příp. jaká) dostupná stávající dokumentace k personální bezpečnosti		popis personálního zabezpečení, tj. řízení lidských zdrojů, nábor, změna, zrušení prac. poměru zaměstnanců-obsluhy, školení, kdo definuje a jaké požadavky na kvalifikaci, odbornost
Kdo je kompetentní osobou pro řešení havárií?		Bezpečnostní manažer, správce objektu, ...
Jsou nějaké exaktní požadavky na použití norem/standardů pro havarijní plánování?		Např. je vyžadováno havarijní plánování v souladu s normou ČSN BS 25999, BS 25777...?
Existuje nějaká strategie pro havarijní plánování?		např. strategické materiály z krizového řízení?
Jaké jsou požadavky na zajištění provozu?		Např. legislativní podmínky, smluvní závazky, lhůty, SLA, ...?

pozn.: šedé pole je povinná položka

KATALOG SLUŽEB SÍTĚ 21NET Verze 0.02

Popis služby			
Název	**Popis a cíle**	**Service level manažer**	**Poznámka**
01-Připojení do TCk	Připojení subjektu ke službám TCk	Ing. Tomáš Martinek	
02-Připojení do CMS	Připojení subjektu ke službám CMS	Ing. Tomáš Martinek	
03-Připojení do IVVS	Připojení subjektu ke službám IVVS		
04-Připojení k PACS	Připojení subjektu ke službám PACS		

01-Připojení subjektu ke službám TCk

Karta služby				
Oblast	**Položka**	**Popis / počet**	**Jednotka**	**Hodnota**
Základní informace	**Název**	01-Připojení subjektu ke službám TCk		
Základní informace	**Platí od**	1.1.2013		
Základní informace	**Platí do**			
Základní informace	**Odpovídá - service level manažer**	Ing. Tomáš Martínek tomas.martinek@kr-zlinsky.cz		
Základní informace	**Vykonává**	servisní organizace XYZ		
Základní informace	**Konzultován**	Správce sítě 21Net		
Základní informace	**Schvaluje**	Rada ZK		
Základní informace	**Informován**	Uživatel a nadřízený		
Základní informace	**Umístění dokumentů**	http://www.21net.cz/		
Základní informace	**Hlášení požadavků**	http://www.21net.cz/helpdesk		
Základní informace	**Základní dostupnost služby**	24x7		
Základní informace	**Poznámky a výjimky**			
Základní informace	**Výklad pojmů a související dokumenty**	Provozní řád sítě 21Net http://www21net.cz		
Metriky - garance	**Dostupnost**	Plánovaná měsiční dostupnost lokality	%	99,5
Metriky - garance	**Garantovaný repair time pro havárie**	Doba obnovení provozu při havárii A	hod	4
Metriky	**Rychlost odezvy na servisní požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	2
Metriky	**Rychlost odezvy na změnové požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	NBD
Metriky	**Poznámky**			
Kvalitativní ukazatelé	**Rychlost**		Mbit/s	1-1000
Kvalitativní ukazatelé	**Zálohování trasy**		ANO/NE	
Kvalitativní ukazatelé	**QoS třída**	Definice priority provozu v rámci sítě 21Net	DSCP	BE
Servisní činnosti	**Pravidelné činnosti**	záloha konfigurací aktivních prvků	-	-
Servisní činnosti	**Reaktviní činnosti**	diagnostika závad, zajištění nápravy, upgrade, údržba,likvidace, dálková správa,	-	-
Servisní činnosti	**Druhy požadavků**	V rámci služby rozlišujeme řešení servisních požadavků (chyb) a změnových požadavků (aktualizace, konzultace, rozvoj) s rozdílným SLA pro tyto služby	-	-

02-Připojení subjektu ke službám CMS

Karta služby				
Oblast	**Položka**	**Popis / počet**	**Jednotka**	**Hodnota**
Základní informace	**Název**	02-Připojení subjektu ke službám CMS		
Základní informace	**Platí od**	1.1.2013		
Základní informace	**Platí do**			
Základní informace	**Odpovídá - service level manažer**	xyz		
Základní informace	**Vykonává**	servisní organizace XYZ		
Základní informace	**Konzultován**	Správce KIZK, Česká pošta		
Základní informace	**Schvaluje**			
Základní informace	**Informován**			
Základní informace	**Umístění dokumentů**	http://www.21net.cz/		
Základní informace	**Hlášení požadavků**	http://www.21net.cz/helpdesk		
Základní informace	**Základní dostupnost služby**	24x7		
Základní informace	**Poznámky a výjimky**			
Základní informace	**Výklad pojmů a související dokumenty**	Provozní řád sítě 21Net http://www21net.cz		
Metriky - garance	**Dostupnost**	Plánovaná měsíční dostupnost lokality	%	99,5
Metriky - garance	**Garantovaný repair time pro havárie**	Doba obnovení provozu při havárii A	hod	4
Metriky	**Rychlost odezvy na servisní požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	2
Metriky	**Rychlost odezvy na změnové požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	NBD
Metriky	**Poznámky**			
Kvalitativní ukazatelé	**Rychlost**		Mbit/s	1-1000
Kvalitativní ukazatelé	**Zálohování trasy**		ANO/NE	
Kvalitativní ukazatelé	**QoS třída**	Definice priority provozu v rámci sítě 21Net	DSCP	
Servisní činnosti	**Pravidelné činnosti**	záloha konfigurací aktivních prvků	-	-
Servisní činnosti	**Reaktviní činnosti**	diagnostika závad, zajištění nápravy, upgrade, údržba,likvidace, dálková správa,	-	-
Servisní činnosti	**Druhy požadavků**	V rámci služby rozlišujeme řešení servisních požadavků (chyb) a změnových požadavků (aktualizace, konzultace, rozvoj) s rozdílným SLA pro tyto služby	-	-

03-Připojení subjektu ke službám IVVS

Karta služby				
Oblast	**Položka**	**Popis / počet**	**Jednotka**	**Hodnota**
Základní informace	**Název**	03-Připojení subjektu ke službám IVVS		
Základní informace	**Platí od**	1.1.2013		
Základní informace	**Platí do**			
Základní informace	**Odpovídá - service level manažer**			
Základní informace	**Vykonává**			
Základní informace	**Konzultován**			
Základní informace	**Schvaluje**			
Základní informace	**Informován**			
Základní informace	**Umístění dokumentů**	http://www.21net.cz/		
Základní informace	**Hlášení požadavků**	http://www.21net.cz/helpdesk		
Základní informace	**Základní dostupnost služby**	24x7		
Základní informace	**Poznámky a výjimky**			
Základní informace	**Výklad pojmů a související dokumenty**	Provozní řád sítě 21Net http://www21net.cz		
Metriky - garance	**Dostupnost**	Plánovaná měsíční dostupnost lokality	%	99,5
Metriky - garance	**Garantovaný repair time pro havárie**	Doba obnovení provozu při havárii A	hod	4
Metriky	**Rychlost odezvy na servisní požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	2
Metriky	**Rychlost odezvy na změnové požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	NBD
Metriky	**Poznámky**			
Kvalitativní ukazatelé	**Rychlost**		Mbit/s	1-1000
Kvalitativní ukazatelé	**Zálohování trasy**		ANO/NE	
Kvalitativní ukazatelé	**QoS třída**	Definice priority provozu v rámci sítě 21Net	DSCP	BE
Servisní činnosti	**Pravidelné činnosti**	záloha konfigurací aktivních prvků	-	-
Servisní činnosti	**Reaktviní činnosti**	diagnostika závad, zajištění nápravy, upgrade, údržba,likvidace, dálková správa,	-	-
Servisní činnosti	**Druhy požadavků**	V rámci služby rozlišujeme řešení servisních požadavků (chyb) a změnových požadavků (aktualizace, konzultace, rozvoj) s rozdílným SLA pro tyto služby	-	-

04-Připojení subjektu ke službám PACS

Karta služby				
Oblast	**Položka**	**Popis / počet**	**Jednotka**	**Hodnota**
Základní informace	**Název**	04-Připojení subjektu ke službám PACS		
Základní informace	**Platí od**	1.1.2013		
Základní informace	**Platí do**			
Základní informace	**Odpovídá - service level manažer**			
Základní informace	**Vykonává**			
Základní informace	**Konzultován**			
Základní informace	**Schvaluje**			
Základní informace	**Informován**			
Základní informace	**Umístění dokumentů**	http://www.21net.cz/		
Základní informace	**Hlášení požadavků**	http://www.21net.cz/helpdesk		
Základní informace	**Základní dostupnost služby**	24x7		
Základní informace	**Poznámky a výjimky**			
Základní informace	**Výklad pojmů a související dokumenty**	Provozní řád sítě 21Net http://www21net.cz		
Metriky - garance	**Dostupnost**	Plánovaná měsíční dostupnost lokality	%	99,5
Metriky - garance	**Garantovaný repair time pro havárie**	Doba obnovení provozu při havárii A	hod	4
Metriky	**Rychlost odezvy na servisní požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	2
Metriky	**Rychlost odezvy na změnové požadavky**	Doba od nahlášení incidentu do začátku řešení	hod	NBD
Metriky	**Poznámky**			
Kvalitativní ukazatelé	**Rychlost**		Mbit/s	1-1000
Kvalitativní ukazatelé	**Zálohování trasy**		ANO/NE	
Kvalitativní ukazatelé	**QoS třída**	Definice priority provozu v rámci sítě 21Net	DSCP	BE
Servisní činnosti	**Pravidelné činnosti**	záloha konfigurací aktivních prvků	-	-
Servisní činnosti	**Reaktviní činnosti**	diagnostika závad, zajištění nápravy, upgrade, údržba,likvidace, dálková správa,	-	-
Servisní činnosti	**Druhy požadavků**	V rámci služby rozlišujeme řešení servisních požadavků (chyb) a změnových požadavků (aktualizace, konzultace, rozvoj) s rozdílným SLA pro tyto služby	-	-

Provozní řád uzlového bodu - *šablona*

Identifikační údaje

Připojovaný subjekt	
Se sídlem	
Adresa přípojného bodu	
Pověřený zástupce	Starosta
Technický garant	IT správce

Kontaktní osoby

Níže uvedené osoby jsou oprávněny kontaktovat helpdesk sítě 21Net dle podmínek provozního řádu 21Net.:

1. jméno, email, tel, interní funkce, role vůči síti 21Net (lokální správce/proškolený uživatel)
2. jméno, email, tel, interní funkce, role vůči síti 21Net (lokální správce/proškolený uživatel)
3. jméno, email, tel, interní funkce, role vůči síti 21Net (lokální správce/proškolený uživatel)

Popis způsobu připojení

HW vybavení

L2 topologie

IP adresace

Popis prostředí uzlového bodu (UB)

V níže uvedené tabulce jsou uvedeny detaily uzlového bodu, šedě vyznačené řádky jsou povinné, ostatní řádky jsou volitelné.

Druh informace	Popis	Nápověda
Identifikace uzlového bodu (UB)		interní označení (např. UH56_ORP)
Adresa umístění UB		kompletní adresa
Druh budovy UB		např. sídlo městského úřadu, škola,…
Identifikace provozovatele UB		jméno, IČ, sídlo, statutární zástupce, kontakt
Standardní provozní doba UB		
Informace o jiných dotčených subjektech		pokud existují. Například majitelé pozemků na kterých UB stojí apod.
Bližší specifikace umístění UB		např. 2 patro, č. dveří 205
Podrobný popis přístupu k UB		např. po vstupu do hlavního vchodu je nutno projít přes turniket ve vrátnici a prokázat se OP,

		dále pak po schodech na levé straně do druhého patra, kde na konci chodby po pravé straně jsou dveře s označením 205, kterými se po otevření pomocí čipové karty vejde do serverovny
Popis umístění UB v rámci serverovny		např. třetí RACK po levé straně místnosti
Kontaktní informace na správce budovy		
Kontaktní informace na správce serverovny		pokud existuje
Kontaktní informace na bezpečnostního technika		
Stavební materiál budovy		panel, cihla,…
Půdorysný plán budovy		
Půdorysný plán serverovny		+ vyznačení kde je umístěn rack a plánovaný přívod konektivity/elektriky do racku
Fotodokumentace		objektu z venku, vstupních dveří do objektu, vstupu do serverovny, serverovny, umístění racku, detail racku i zařízení, všechny možné vstupy (dveře, okna, větrací šachty,…)
Je objekt v zátopové zóně		
Hrozí u objektu vyšší nebezpečí živlů?		např, kolem teče řeka, sousedí s továrnou na výrobu výbušných látek,…
Existují nějaké jiné fyzické či enviromentální hrozby?		např. objekt je poddolován, kolem objektu jsou vysoké stromy, objekt nemá hromosvod, dveře do serverovny se nezamykají, po objektu se pohybují externí lidé bez evidence na vrátnici, zdi serverovny jsou ze sádrokartonu a do vedlejší místnosti je volný přístup,…
Přibližný dojezdový čas či vzdálenost HZS		
Přibližný dojezdový čas či vzdálenost ostrahy		Bezpečnostní agentura, PČR, najmutý strážný,…
Kdo a v jakém režimu objekt střeží v pracovní době		Informace o bezpečnostní agentuře, PČR apod. včetně kontaktních informací, případně o vrátném a spojení na něj
Kdo a v jakém režimu objekt střeží mimo pracovní dobu		Informace o bezpečnostní agentuře, PČR apod. včetně kontaktních informací, případně o vrátném a spojení na něj
Za jakých podmínek		kam telefonovat, co je kontrolováno (OP, osobní

se dá do objektu dostat		průkazka), příp. evidováno (zápis do knihy návštěv, elektronická čtečka OP,…)
Kdo má přístup do objektu, kdo přístupy schvaluje		jak v pracovní době tak mimo ní
Jaké je pasivní zabezpečení vstupu do serverovny		pasivní prvky (dveře, zámky, mříže, okna)
Jaké je aktivní zabezpečení vstupu do serverovny		aktivní prvky (PCO, EZS, EPS, CCTV) + typy a u CCTV jakým způsobem se zaznamenává (kontinuelně, motion detection,…). Jou technologie připojeny na UPS?
Druh přístupu		bezpečnostní klíč, čipová karta, snímač zornice, atp. (jak pro vstup do serverovny, tak do racku)
Je rack vyhrazen výhradně pro UB		je/není (jaké cizí technologie jsou v něm obsaženy)
Jak je zabezpečen provoz technologií		např. klimatizace, UPS, dieselagregát, přívod el. proudu z více zdrojů, zhášecí systém + jejich typy (jsou tyto technologie vlastníka budovy a nebo součástí UB)
Popis serverovny (technologické místnosti)		jaké jsou zde cizí technologie, počet racků a hrubý popis vybavení (servery, diskové pole, UPS, tel. ústředna apod.)
Je (příp. jaká) dostupná stávající dokumentace k fyzické bezpečnosti		popis fyzického/objektového zabezpečení, tj. správa budovy/místnosti, fyzický přístup, přístup třetích stran, servis, úklid, revize, EZS, EPS, ostraha apod.
Je (příp. jaká) dostupná stávající dokumentace k organizační bezpečnosti		popis organizačního zajištění, tj. jaká je hierarchie řízení UB, zaměstnanci, příp. externí pracovníci, dodavatelé služeb, kompetence, pravomoci a odpovědnosti
Je (příp. jaká) dostupná stávající dokumentace k technické bezpečnosti		popis ICT bezpečnosti, tj. technické/technologické bezpečnostní prvky systému
Je (příp. jaká) dostupná stávající dokumentace k personální bezpečnosti		popis personálního zabezpečení, tj. řízení lidských zdrojů, nábor, změna, zrušení prac. poměru zaměstnanců-obsluhy, školení, kdo definuje a jaké požadavky na kvalifikaci, odbornost
Kdo je kompetentní osobou pro řešení havárií?		Bezpečnostní manažer, správce objektu, ...
Jsou nějaké exaktní požadavky na použití norem/standardů pro havarijní plánování?		Např. je vyžadováno havarijní plánování v souladu s normou ČSN BS 25999, BS 25777...?
Existuje nějaká		např. strategické materiály z krizového řízení?

strategie pro havarijní plánování?		
Jaké jsou požadavky na zajištění provozu?		Např. legislativní podmínky, smluvní závazky, lhůty, SLA, ...?

pozn.: šedé pole je povinná položka

Seznam výjimek proti provoznímu řádu sítě 21Net

Provozní řád přípojného bodu

Identifikační údaje

Připojovaný subjekt	
Se sídlem	
Adresa přípojného bodu	
Pověřený zástupce	Starosta
Technický garant	IT správce / šéf IT

Kontaktní osoby

Níže uvedené osoby jsou oprávněny kontaktovat helpdesk sítě 21Net dle podmínek provozního řádu sítě 21Net

1. jméno, email, tel, interní funkce, role vůči síti 21Net (lokální správce/proškolený uživatel)
2. jméno, email, tel, interní funkce, role vůči 21Net (lokální správce/proškolený uživatel)
3. jméno, email, tel, interní funkce, role vůči 21Net (lokální správce/proškolený uživatel)

Popis způsobu připojení

HW vybavení

L2 topologie

IP adresace

Popis prostředí přípojného bodu (PB)

V níže uvedené tabulce jsou uvedeny detaily přípojného bodu, šedě vyznačené řádky jsou povinné, ostatní řádky jsou volitelné.

Druh informace	Popis	Nápověda
Identifikace přípojného bodu (PB)		interní označení (např. UH56_ORP)
Adresa umístění PB		kompletní adresa
Druh budovy PB		např. sídlo městského úřadu, škola,…
Identifikace provozovatele PB		jméno, IČ, sídlo, statutární zástupce, kontakt
Standardní provozní doba PB		
Bližší specifikace umístění PB		např. 2 patro, č. dveří 205
Podrobný popis přístupu k PB		např. po vstupu do hlavního vchodu je nutno projít přes turniket ve vrátnici a prokázat se OP, dále pak po schodech na levé straně do druhého patra, kde na konci chodby po pravé straně jsou dveře s označením 205, kterými se po otevření pomocí čipové karty vejde do serverovny

Kontaktní informace na správce budovy		
Kontaktní informace na správce serverovny		pokud existuje
Kontaktní informace na bezpečnostního technika		
Stavební materiál budovy		panel, cihla,…
Půdorysný plán budovy		
Půdorysný plán serverovny		+ vyznačení kde je umístěn rack a plánovaný přívod konektivity/elektriky do racku
Fotodokumentace		objektu z venku, vstupních dveří do objektu, vstupu do serverovny, serverovny, umístění racku, detail racku i zařízení, všechny možné vstupy (dveře, okna, větrací šachty,…)
Je objekt v zátopové zóně		
Hrozí u objektu vyšší nebezpečí živlů?		např, kolem teče řeka, sousedí s továrnou na výrobu výbušných látek,…
Existují nějaké jiné fyzické či enviromentální hrozby?		např. objekt je poddolován, kolem objektu jsou vysoké stromy, objekt nemá hromosvod, dveře do serverovny se nezamykají, po objektu se pohybují externí lidé bez evidence na vrátnici, zdi serverovny jsou ze sádrokartonu a do vedlejší místnosti je volný přístup,...
Přibližný dojezdový čas či vzdálenost HZS		
Přibližný dojezdový čas či vzdálenost ostrahy		Bezpečnostní agentura, PČR, najmutý strážný,…
Kdo a v jakém režimu objekt střeží v pracovní době		Informace o bezpečnostní agentuře, PČR apod. včetně kontaktních informací, případně o vrátném a spojení na něj
Kdo a v jakém režimu objekt střeží mimo pracovní dobu		Informace o bezpečnostní agentuře, PČR apod. včetně kontaktních informací, případně o vrátném a spojení na něj
Za jakých podmínek se dá do objektu dostat		kam telefonovat, co je kontrolováno (OP, osobní průkazka), příp. evidováno (zápis do knihy návštěv, elektronická čtečka OP,…)
Kdo má přístup do objektu, kdo přístupy schvaluje		jak v pracovní době tak mimo ní
Jaké je pasivní zabezpečení vstupu do serverovny		pasivní prvky (dveře, zámky, mříže, okna)
Jaké je aktivní zabezpečení vstupu		aktivní prvky (PCO, EZS, EPS, CCTV) + typy a u CCTV jakým způsobem se zaznamenává

do serverovny		(kontinuelně, motion detection,…). Jou technologie připojeny na UPS?
Druh přístupu		bezpečnostní klíč, čipová karta, snímač zornice, atp. (jak pro vstup do serverovny, tak do racku)
Je rack vyhrazen výhradně pro PB		je/není (jaké cizí technologie jsou v něm obsaženy)
Jak je zabezpečen provoz technologií		např. klimatizace, UPS, dieselagregát, přívod el. proudu z více zdrojů, zhášecí systém + jejich typy (jsou tyto technologie vlastníka budovy a nebo součástí PB)
Popis serverovny (technologické místnosti)		jaké jsou zde cizí technologie, počet racků a hrubý popis vybavení (servery, diskové pole, UPS, tel. ústředna apod.)
Je (příp. jaká) dostupná stávající dokumentace k fyzické bezpečnosti		popis fyzického/objektového zabezpečení, tj. správa budovy/místnosti, fyzický přístup, přístup třetích stran, servis, úklid, revize, EZS, EPS, ostraha apod.
Je (příp. jaká) dostupná stávající dokumentace k organizační bezpečnosti		popis organizačního zajištění, tj. jaká je hierarchie řízení PB, zaměstnanci, příp. externí pracovníci, dodavatelé služeb, kompetence, pravomoci a odpovědnosti
Je (příp. jaká) dostupná stávající dokumentace k technické bezpečnosti		popis ICT bezpečnosti, tj. technické/technologické bezpečnostní prvky systému
Je (příp. jaká) dostupná stávající dokumentace k personální bezpečnosti		popis personálního zabezpečení, tj. řízení lidských zdrojů, nábor, změna, zrušení prac. poměru zaměstnanců-obsluhy, školení, kdo definuje a jaké požadavky na kvalifikaci, odbornost
Kdo je kompetentní osobou pro řešení havárií?		Bezpečnostní manažer, správce objektu, ...
Jsou nějaké exaktní požadavky na použití norem/standardů pro havarijní plánování?		Např. je vyžadováno havarijní plánování v souladu s normou ČSN BS 25999, BS 25777...?
Existuje nějaká strategie pro havarijní plánování?		např. strategické materiály z krizového řízení?
Jaké jsou požadavky na zajištění provozu?		Např. legislativní podmínky, smluvní závazky, lhůty, SLA, ...?

pozn.: šedé pole je povinná položka

Seznam výjimek proti provoznímu řádu sítě 21Net