Roamingová politika

(verze 1.0 – 9. 5. 2007)

Čl.1 – **Úvod**

1.1 Sdružení CESNET, z. s. p. o. (dále jen CESNET) a jeho členové, veřejné vysoké školy a Akademie věd ČR (dále jen členové), a ostatní připojené instituce provozují ve svých prostorách lokální počítačové sítě. Jejich společným zájmem je zajistit pro své uživatele roaming mezi těmito lokálními sítěmi.

1.2 Tento dokument vymezuje vztahy mezi jednotlivými členy české ***eduroam*** federace a navazuje tak na evropskou ***eduroam*** konfederační politiku, která definuje pravidla pro spolupráci jednotlivých federací (NREN). Více informací na **www.eduroam.org.**

Čl. 2 – **Definice pojmů**

Pro účely této politiky se užitými termíny rozumí následující:

2.1 ***eduroam*** je akademický roamingový systém poskytující síťovou konektivitu pro své uživatele v připojených organizacích. Přístup je založen na zabezpečené autentizaci v domácí instituci.

2.2 Česká eduroam federace je uskupení organizací zapojených do systému ***eduroam*** v rámci České republiky, a to v jakékoliv roli (viz. Čl. 4). Pro potřeby tohoto dokumentu se dále ***eduroam*** federací myslí česká ***eduroam*** federace.

2.3 Evropská ***eduroam*** konfederace je uskupení jednotlivých národních ***eduroam*** federací v rámci Evropy. Federace jsou zpravidla zastoupeny organizacemi, které provozují sítě národního výzkumu a vzdělávání - NREN (v ČR tuto roli zastává sdružení CESNET).

2.4 Access Policy (Zásady pro přístup do sítě národního výzkumu a vzdělávání, dále jen AP) je soubor pravidel definující kdo a za jakých okolností smí využívat služby sítě národního výzkumu a vzdělávání (NREN). Více informací na **www.cesnet.cz/doc/podminky.html.**

2.5 Poskytovatel identity je subjekt, u kterého má uživatel veden svůj „účet" (např. jméno a heslo – ověřovací údaje potřebné pro přihlášení k síti). Ve většině případů se jedná o domovskou instituci, k níž má uživatel organizačně právní vztah – je zaměstnancem, studentem atp. Poskytovatel identity je oprávněn a povinen rozhodnout o povolení či zamítnutí autentizačního požadavku na přístup uživatele ke zdroji (např. síťová konektivita). Tento požadavek je vygenerován poskytovatelem daného zdroje v souvislosti s potřebami uživatele.

2.6 Poskytovatel zdrojů je subjekt, který uživatelům poskytuje síťové služby (např. konektivitu, přístup na www stránky apod.). Rozhodnutí o tom, zda uživatel má nebo nemá právo požadovaný zdroj využít, se uskuteční na základě autentizačního dotazu vzneseného na poskytovatele identity daného uživatele.

Čl. 3 – **Obecná ustanovení**

3.1 Název a logo eduroam jsou registrovanou ochrannou známkou společnosti TERENA (Trans-European Research and Educational Networking Association). Při každém užití jména nebo loga ***eduroam*** je potřeba tuto skutečnost zmínit. Více informací na **www.terena.org.**

3.2 Ve všech lokalitách poskytujících ***eduroam*** by měla být přítomnost tohoto systému jasně vyznačena (např. umístěním loga), a to z důvodu informování uživatelů o možnosti připojení.

3.3 V systému ***eduroam*** musí být vždy zajištěn bezpečný a důvěryhodný přenos autentizačních dat. Uživatelské autentizační údaje musí být při přenosu mezi klientským zařízením a poskytovatelem identity šifrovány, aby nemohlo dojít k jejich diskreditaci.

Čl. 4 – **Vymezení rolí a povinností subjektů zapojených do *eduroam* federace**

4.1 Správce *eduroam* federace

4.1.1 Roli správce ***eduroam*** federace (dále jen správce) vykonává v rámci České republiky sdružení CESNET.

4.1.2 Správce koordinuje dění ve federaci a je vykonavatelem roamingové politiky na národní úrovni, přičemž postupuje v souladu s evropskou konfederační politikou.

4.1.3 Správce provozuje národní autentizační servery v souladu s technickými pravidly definovanými v evropské konfederační politice (především s ohledem na požadovanou vysokou míru zabezpečení). Tyto servery zajišťují napojení národní ***eduroam*** federace k evropským „top-level" autentizačním serverům a zajišťují tak technické připojení do konfederace. Národní autentizační servery musí být dostupné a reagovat na autentizační dotazy od připojených autentizačních serverů.

4.1.4 Správce zaznamenává do logů informace o autentizačním provozu jdoucím přes jeho servery. Tyto údaje je povinen uchovávat po dobu 6 měsíců.

4.1.5 Odpovídající části logů je správce oprávněn použít v souvislosti s identifikací zneužívání sítě anebo služeb sítě. Na vyžádání a je-li to nezbytné je v těchto případech oprávněn poskytnout uložené informace i třetím stranám (poskytovatelům identit, poskytovatelům zdrojů a orgánům činným v trestním řízení).

4.1.6 Je-li to nezbytně nutné (např. z bezpečnostních nebo provozních důvodů), je správce oprávněn na národních autentizačních serverech omezit nebo zcela odepřít přístup pro jednotlivé uživatele nebo celé organizace.

4.1.7 Správce zajišťuje technickou podporu organizacím zapojeným do federace, a to v souvislosti s jejich napojením na národní autentizační servery a řešením případných bezpečnostních incidentů.

4.1.8 Veškerá komunikace se správcem federace probíhá prostřednictvím kontaktů uvedených na informačním portálu **www.eduroam.cz.**

4.2 Poskytovatelé identity

4.2.1 Úkolem poskytovatele identity je především odpovídat na autentizační dotazy přicházející od poskytovatelů zdrojů ohledně možnosti připojení uživatelů, kteří jsou u daného poskytovatele identity definováni. Poskytovatelem identity je většinou domácí organizace uživatele (např. univerzita), kde jsou uchovány všechny informace nutné pro jeho ověření. Poskytovatel identity je odpovědný za autoritativní rozhodnutí, zda má či nemá uživatel právo přístupu k danému zdroji (vyjma případů definovaných v bodě 8.8).

4.2.2 Poskytovatel identity musí vůči svým uživatelům vystupovat ohledně systému ***eduroam*** jako autoritativní orgán. Musí prosazovat dodržování této federační politiky, eventuálně vytvořit vlastní podmínky používání roamingových služeb pro své uživatele (tyto musí být v souladu s federační politikou). S těmito pravidly musí své uživatele seznámit.

4.2.3 Poskytovatel identity musí od svých uživatelů důsledně vyžadovat dodržování AP sítě CESNET a vyšetřovat porušování těchto pravidel. Musí přijímat oznámení o bezpečnostních incidentech, nedodržování AP a federační politiky svými uživateli. Do vyřešení problému je povinen odepřít těmto uživatelům přístup ke zdrojům a v případě potřeby spolupracovat na řešení těchto incidentů s třetími stranami (správce ***eduroam*** federace, poskytovatelé zdrojů, bezpečnostní týmy atd.).

4.2.4 Poskytovatel identity musí svým uživatelům zajistit technickou podporu, základní informace o roamingovém systému ***eduroam*** a platné legislativě. Zejména se jedná o pomoc při konfiguraci klientských stanic a řešení případných problémů s funkčností technických prostředků na straně klienta.

4.2.5 Poskytovatel identity provozuje autentizační servery organizace v souladu s technickými požadavky, které jsou zveřejněné na informačním portálu **www.eduroam.cz**. Tyto servery jsou napojeny na národní autentizační servery a zajišťují tak technické připojení dané organizace k ***eduroam*** federaci. Autentizační servery poskytovatele identity musí být dostupné a reagovat na autentizační dotazy od poskytovatelů zdrojů. Zvláštní důraz je třeba klást na zabezpečení, a to jednak v souvislosti s konfigurací serverů a jednak v souvislosti s použitými autentizačními metodami.

4.2.6 Pro testovací účely musí poskytovatel identity vytvořit správci ***eduroam*** federace testovací účet. Tento účet slouží pouze pro testování autentizačního serveru daného poskytovatele identity a ověření funkčnosti celé autentizační infrastruktury. Nesmí být použit pro přístup k reálným zdrojům. Na autentizační žádosti při použití tohoto účtu musí server poskytovatele identity vždy vracet kladné odpovědi. Testovací účet udržuje správce ***eduroam*** federace i poskytovatel identity v tajnosti (tj. nepředává ho třetím stranám). Při jeho diskreditaci se postupuje standardním způsobem.

4.2.7 Poskytovatel identity zaznamenává do logů informace o autentizačních požadavcích, které jeho servery zpracovávají (zejména uživatelskou identitu, výsledek autentizace, přesný čas atd.). Tyto údaje je povinen uchovávat po dobu 6 měsíců.

4.2.8 Odpovídající části logů je poskytovatel identity oprávněn použít v souvislosti s identifikací zneužívání sítě anebo služeb sítě. Na vyžádání a je-li to nezbytné je v těchto případech oprávněn poskytnout uložené informace i třetím stranám (správci ***eduroam*** federace, poskytovatelům zdrojů a orgánům činným v trestním řízení).

4.2.9 Poskytovatel identity musí určit alespoň jednu osobu jako technický kontakt (z důvodů zástupnosti je samozřejmě preferováno mít technických kontaktů více). Technický kontakt je zodpovědný za komunikaci mezi poskytovatelem identity a správcem ***eduroam*** federace, v odpovídajícím čase řeší technické záležitosti a bezpečnostní incidenty. Pokud dojde ke změně v technickém kontaktu, musí poskytovatel identity tuto skutečnost neprodleně oznámit správci ***eduroam*** federace a udržovat aktuální informace v systému CESNET CAAS (databáze kontaktních údajů).

4.2.10 Poskytovatel identity by měl pro své uživatele vytvořit informační www stránky, které by měly obsahovat zejména kontakty na technickou podporu, popis funkce systému ***eduroam***, popis nastavení klientských zařízení, informace o platné legislativě (pravidla pro použití roamingu definované daným poskytovatelem identity, federační politika), odkazy na národní a evropský ***eduroam*** informační portál atd. Tyto stránky by měly být v českém i anglickém jazyce.

4.3 Poskytovatelé zdrojů

4.3.1 Poskytovatelem zdrojů je každý subjekt, který nabízí své síťové služby (např. konektivitu) uživatelům roamingového systému ***eduroam***, a to pouze za předpokladu platné autentizace u poskytovatele identity daného uživatele na základě jeho autentizačních údajů. Pokud z jakéhokoliv důvodu k ověření uživatele u jeho poskytovatele identity nedojde, nesmí mu být umožněn přístup k síťovým zdrojům. Veškeré zdroje, které poskytovatel uživatelům nabízí v souvislosti se systémem ***eduroam***, musí být dostupné pouze po úspěšné autentizaci.

4.3.2 Poskytovatel zdrojů musí dodržovat zásady AP sítě CESNET a této roamingové politiky. Musí rovněž vyžadovat (a v rámci možností také kontrolovat) dodržování AP a této politiky uživateli, kteří využívají jeho zdroje. V případě potřeby by měl poskytovatel zdrojů definovat vlastní pravidla používání svých síťových prostředků (musí být v souladu s touto federační politikou) a tyto zveřejnit a svém informačním portálu (viz. bod 4.3.13).

4.3.3 Poskytovatel zdrojů musí přijímat oznámení o bezpečnostních incidentech, nedodržování AP a federační politiky uživateli, kteří využívají jeho zařízení, a tyto incidenty také důsledně prošetřovat. Uživatelům podezřelým z činnosti, která se neslučuje s definovanými pravidly, musí do vyřešení problému odepřít přístup ke zdrojům a podle potřeby spolupracovat na řešení těchto incidentů i s dalšími subjekty (správce ***eduroam*** federace, poskytovatelé identity, bezpečnostní týmy atd.) – postupuje přitom podle článku 7 „Postup při řešení bezpečnostních incidentů“.

4.3.4 Poskytovatel zdrojů, nabízející konektivitu k síti, může k tomuto účelu použít různé síťové technologie. Při použití bezdrátové technologie WiFi (802.11 a/b/g) je povinen implementovat bezpečnostní metody 802.1x a WPA/TKIP (nebo lepší), které zajišťují bezpečný přenos dat po radiové síti a minimalizují tak bezpečnostní rizika. Bezdrátová síť musí mít nastavené SSID (identifikátor bezdrátové sítě) „eduroam“ a toto SSID by mělo být anoncováno. V případě rádiového překryvu více sítí (patřících různým poskytovatelům zdrojů, s různými IP subnety atd.) se stejným SSID, se toto SSID nastaví ve formátu „eduroam-[inst]“, kde [inst] je dobře srozumitelná zkratka reprezentující jméno organizace. V tomto případě musí být SSID anoncováno.

4.3.5 Je doporučeno, aby k adresaci sítě, zapojené do systému ***eduroam***, poskytovatel zdrojů použil veřejně routovatelné IP adresy přidělované DHCP serverem. Tato síť by měla být

z bezpečnostních důvodů oddělena od ostatních sítí organizace a IP provoz mezi touto sítí a Internetem by neměl být nijak omezen (např. pomocí firewallu, IP filtrů atd.).

4.3.6 Za přístup k síti na základě roamingu nesmí poskytovatel zdrojů účtovat žádné poplatky. Služba je založena na recipročním principu (viz. bod 4.5.1).

4.3.7 Poskytovatel zdrojů je povinen v nezbytně nutné míře spolupracovat při technické podpoře uživatelů s jejich poskytovatelem identity.

4.3.8 Poskytovatel zdrojů provozuje autentizační servery v souladu s technickými požadavky, které jsou zveřejněné na informačním portálu **www.eduroam.cz**. Tyto servery jsou napojeny na národní autentizační servery a zajišťují tak technické připojení dané organizace k ***eduroam*** federaci. Autentizační servery poskytovatele zdrojů musí být dostupné a generovat autentizační dotazy směrem k poskytovatelům identity v závislosti na požadavcích uživatelů, kteří přistupují ke zdrojům. Požadovaná síťová služba může být uživateli zpřístupněna pouze za předpokladu, že autentizační server obdržel kladnou odpověď na autentizační žádost od poskytovatele identity daného uživatele. Zvláštní důraz je třeba klást na zabezpečení, a to především v souvislosti s konfigurací serverů.

4.3.9 Poskytovatel zdrojů zaznamenává do logů informace o autentizačních požadavcích, které jeho servery zpracovávají (zejména výsledek autentizace, uživatelskou identitu požadavku, identifikátor požadavku, identifikátor poskytovatele identity, přesný čas atd.) a DHCP transakcích (zejména přiřazení IP adresy k MAC adrese, přesný čas atd.). Tyto údaje je povinen uchovávat po dobu 6 měsíců.

4.3.10 Odpovídající části logů je poskytovatel zdrojů oprávněn použít v souvislosti s identifikací zneužívání sítě anebo služeb sítě. Na vyžádání a je-li to nezbytné je v těchto případech oprávněn poskytnout uložené informace i třetím stranám (správci ***eduroam*** federace, poskytovatelům identity a orgánům činným v trestním řízení).

4.3.11 Pokud poskytovatel zdrojů provádí monitoring aktivity uživatelů v rozsahu větším, než odpovídá bodu 4.3.9, je povinen s touto skutečností seznámit uživatele (zejména poskytnout informace jak a v jakém rozsahu monitoring probíhá, jak jsou získané údaje uchovávány a kdo k nim má přístup) a postupovat v souladu s platnou legislativou.

4.3.12 Poskytovatel zdrojů musí určit alespoň jednu osobu jako technický kontakt (z důvodů zástupnosti je samozřejmě preferováno mít technických kontaktů více). Technický kontakt je zodpovědný za komunikaci mezi poskytovatelem zdrojů a správcem ***eduroam*** federace, v odpovídajícím čase řeší technické záležitosti a bezpečnostní incidenty. Pokud dojde ke změně v technickém kontaktu, musí poskytovatel zdrojů tuto skutečnost neprodleně oznámit správci ***eduroam*** federace a udržovat aktuální informace v systému CESNET CAAS (databáze kontaktních údajů).

4.3.13 Poskytovatel zdrojů musí vytvořit informační www stránky, které musí obsahovat minimálně:

- kontakty na technickou podporu
- informace o platné legislativě (pravidla pro použití roamingu definované daným poskytovatelem zdrojů, federační politika)
- odkazy na národní a evropský ***eduroam*** informační portál
- popis nebo plánek prostoru pokrytého signálem sítě ***eduroam*** (eventuálně umístění přístupových bodů)
- informace o použitých SSID rádiové sítě a o jejich anoncování

- informace o použitých šifrovacích a autentizačních algoritmech (WPA, WPA2, 802.1x, EAP metody atd.)
- popis použitého IP adresového prostoru a informace o případném omezení provozu (IP filtrace)
- detaily o použitých netransparentních aplikačních proxy serverech včetně popisu jejich funkce a nastavení
- logo ***eduroam*** a klauzuli o tom, že je ***eduroam*** registrovanou ochrannou známkou společnosti TERENA
- informace o prováděném monitoringu ve smyslu bodu 4.3.11

Měly by obsahovat také popis funkce systému ***eduroam***, popis nastavení klientských zařízení atd. Tyto stránky musí být v anglickém a měly by být také v českém jazyce.

4.4 Uživatelé

4.4.1 Uživatelem roamingu se může stát každý, kdo má právní vztah (zaměstnanec, student atd.) k organizaci, která je členem ***eduroam*** federace a působí v roli poskytovatele identity.

4.4.2 Uživatel je povinen řídit se pravidly pro přístup k síti definovanými svým poskytovatelem identity (domácí organizace) a poskytovatelem zdrojů (navštívená organizace). Pokud se tato pravidla liší, platí restriktivnější varianta.

4.4.3 Uživatel je plně odpovědný za svoje přihlašovací údaje i za jejich zneužití. Musí postupovat tak, aby jejich zneužití v maximální možné míře předešel. V případě jejich diskreditace je povinen tuto skutečnost neprodleně oznámit svému poskytovateli identity.

4.4.4 Uživatel je povinen okamžitě reagovat na výzvy a pokyny svého poskytovatele identity, poskytovatele zdrojů a správce ***eduroam*** federace.

4.5 Společná ustanovení

Organizace poskytující identitu (ve smyslu bodu 4.2) musí být současně poskytovatelem zdrojů (ve smyslu bodu 4.3). Z tohoto pravidla může být udělena speciální výjimka, která musí být schválena správcem ***eduroam*** federace a oznámena všem členům federace.

Čl. 5 – **Zapojení organizace do *eduroam* federace**

5.1 Do systému ***eduroam*** se v rámci české ***eduroam*** federace může připojit každá organizace, která je připojena na síť národního výzkumu a vzdělávání CESNET2. Musí přitom splňovat technické podmínky AP a dodržovat tuto roamingovou politiku. Konečné rozhodnutí, zda bude nebo nebude organizace přijata do ***eduroam*** federace, náleží správci federace.

5.2 Organizace svým přistoupením k systému ***eduroam*** souhlasí s touto roamingovou politikou v plném rozsahu a zavazuje se ji dodržovat. Aktem „přistoupení“ se pro potřeby této politiky rozumí technické napojení autentizačních serverů organizace k národním autentizačním serverům, a to v souladu s technickými podmínkami.

5.3 Systém ***eduroam*** je postaven na recipročním principu. Pokud chce organizace využívat služeb systému ***eduroam,*** musí sama také nějaké nabízet (většinou jde o přístup k síti pomocí bezdrátové technologie WiFi).

5.4 Členství v ***eduroam*** federaci je pro organizaci bezúplatné.

5.5 Organizace nesmí za služby poskytnuté v rámci systému ***eduroam*** účtovat žádné poplatky.

5.6 Organizace musí vybudovat technickou strukturu, která odpovídá zásadám zveřejněným na informačním portálu **www.eduroam.cz.** Technické parametry musejí být rovněž v souladu s požadavky, které jsou definované v evropské konfederační politice (European ***eduroam*** confederation service level agreement).

5.7 Organizace musí spolupracovat se správcem federace a v odpovídajícím čase reagovat.

Čl. 6 – **Opuštění *eduroam* federace**

6.1 Rozhodne-li se organizace (ať už v roli poskytovatele identity nebo poskytovatele zdrojů) o své vůli opustit ***eduroam*** federaci a dále nespolupracovat v rámci roamingového systému ***eduroam,*** musí tento záměr ohlásit správci federace s předstihem alespoň 1 měsíc. Během této doby se připraví správce federace na provedení technického odpojení a oznámí tuto skutečnost na informačním portálu **www.eduroam.cz.** Především je potřeba uvést, jaká organizace se bude odpojovat, jméno jejího realmu (jednoznačný identifikátor poskytovatele identity) a přesné datum odpojení.

6.2 Pokud musí dojít k odpojení organizace z důvodů porušení pravidel (např. této roamingové politiky, AP atd.), zablokuje správce federace okamžitě veškerý autentizační provoz dané organizace, čímž se tato fakticky izoluje od zbytku ***eduroam*** federace. Po dobu 1 měsíce se organizace uvede do stavu „izolace“, což znamená, že je na technické úrovni zablokovaná, ale pokud v této lhůtě odstraní nedostatky, izolace bude zrušena a organizace bude dále vystupovat jako plnohodnotný člen federace. Veškeré skutečnosti o uvalení izolace na organizaci (zejména důvody, termíny, případné zrušení izolace atd.) oznamuje správce federace neprodleně na portálu **www.eduroam.cz.** Během izolace je organizace stále vedená v seznamu připojených, pouze s poznámkou o blokování provozu. Pokud během izolace (lhůta 1 měsíc) organizace neodstraní problém, dojde k úplnému odpojení od federace.

6.3 Po odpojení organizace od ***eduroam*** federace musí tato neprodleně odstranit veškeré odkazy na systém ***eduroam.*** Jde zejména o informace na webových stránkách, loga, anoncované SSID na rádiových sítích atd.

Čl. 7 – **Postup při řešení bezpečnostních incidentů**

7.1 V případě, že poskytovatel zdrojů identifikuje uživatele, který provádí činnost neslučitelnou s pravidly roamingového systému ***eduroam*** (např. porušuje roamingovou

politiku, AP atd.), je povinen mu v tom neprodleně a všemi dostupnými prostředky zabránit. Poskytovatel zdrojů zjistí identifikační údaje uživatele (jeho uživatelské jméno, IP a MAC adresu atd.) a okamžitě znemožní tomuto uživateli přístup k prostředkům sítě na technické úrovni. Neprodleně o problému informuje správce identity, ke kterému daný uživatel přísluší, oznámí mu činnost, kterou uživatel prováděl a zažádá o zablokování tohoto uživatele. Jakmile poskytovatel zdrojů obdrží od poskytovatele identity potvrzení o zablokování podezřelého uživatele, odstraní jeho blokaci na lokálním autentizačním serveru. Dokud se celá záležitost nevyřeší, dotyčný uživatel nesmí využívat služeb systému ***eduroam.*** O veškerých bezpečnostních incidentech musí být neodkladně informován správce federace. Poskytovatel zdrojů, poskytovatel identity a správce federace musejí při řešení problémů vzájemně spolupracovat. Pokud poskytovatel identity v odpovídajícím čase nezablokuje účet podezřelého uživatele a nespolupracuje na řešení incidentu, je správce federace oprávněn zablokovat autentizaci celého realmu, a to až do vyřešení problému. Pokud není poskytovatel identity členem české ***eduroam*** federace (jde o organizaci z cizího státu) a vyžadují-li to okolnosti, informuje správce federace o situaci i evropský „***eduroam*** operational team".

7.2 Organizace může požádat o vyřešení bezpečnostního incidentu svůj bezpečnostní tým (CSIRT, CERT, abuse team atd.). Ten při řešení postupuje v souladu s touto roamingovou politikou (zejména podle bodu 7.1) a za využití všech prostředků a postupů, které má definované ve své bezpečnostní politice.

7.3 Při zjištění bezpečnostního incidentu (eventuálně porušování roamingové politiky, AP atd.) musí veškeré dotčené subjekty zapojené do ***eduroam*** federace vyvinout maximální úsilí k odstranění problému, a to podle okolností v nejkratším možném čase. Porušení této zásady bude považováno zaporušení roamingové politiky ze strany těchto subjektů. O všech bezpečnostních incidentech v rámci ***eduroam*** federace musí být neprodleně informován správce federace.

Čl. 8 – **Pravomoce, dodržování politiky a sankce**

8.1 Vykonavatelem této roamingové politiky je správce ***eduroam*** federace, tedy sdružení CESNET.

8.2 Na členství organizace v ***eduroam*** federaci, a to v jakékoliv roli (podle čl. 4.2 a 4.3), není právní nárok.

8.3 Na využívání služeb systému ***eduroam*** v roli „uživatel" (ve smyslu čl. 4.4) není právní nárok. Vytvoření pravidel pro přístup uživatelů ke službě ***eduroam*** je plně v kompetenci příslušného poskytovatele identity.

8.4 Napojením autentizačních serverů organizace k národním autentizačním serverům (podle technických pravidel připojení) prokazuje organizace svůj plný souhlas s touto roamingovou politikou a zavazuje se ji dodržovat.

8.5 Veškeré změny v této roamingové politice budou oznámeny minimálně 3 měsíce před jejich účinností a budou v rámci možností konzultovány se všemi organizacemi zapojenými do české ***eduroam*** federace. Pokud bude pro organizaci nová verze politiky nepřijatelná, musí se od federace nejpozději do data nabytí účinnosti změn odpojit (podle článku 6 tohoto dokumentu). Pokud zůstane nadále technicky připojená, deklaruje tím svůj plný souhlas s novým zněním federační politiky.

8.6 Autoritativní a konečné rozhodnutí přísluší vždy správci federace, a to zejména v případech, kdy se jedná o přijetí organizace do ***eduroam*** federace, jejím vyčlenění z federace nebo v případech uplatňování sankcí. Rovněž pro záležitosti ohledně roamingové politiky je autoritativním orgánem správce federace.

8.7 V případě hrubého nedodržení této roamingové politiky, porušování technických zásad ***eduroam*** federace, způsobení závažného bezpečnostního incidentu a v dalších případech, kdy dojde k hrubému porušení pravidel roamingového systému ***eduroam***, přistoupí správce ***eduroam*** federace k vyčlenění a technickému odpojení organizace z ***eduroam*** federace. Tento krok správce federace dotčené organizaci oznámí a bude o této skutečnosti informovat na veřejném portálu **www.eduroam.cz**.

8.8 V případě bezpečnostních incidentů nebo nedodržování této roamingové politiky, AP, případně dalších pravidel pro roamingový systém ***eduroam*** má správce ***eduroam*** federace nebo poskytovatel zdrojů právo omezit nebo zcela zablokovat autentizaci jednotlivých uživatelů nebo celých realmů (veškerý autentizační provoz od daného poskytovatele identity). Tyto restrikce musí být provedeny jen v nezbytně nutné míře s cílem zabránit dalšímu zneužívání sítě nebo služeb sítě. O tomto kroku musí neprodleně informovat poskytovatele identity, jehož se toto omezení týká a pokud tuto restrikci provádí poskytovatel zdrojů, musí též informovat správce federace.

8.9 V případě bezpečnostních incidentů nebo nedodržování této roamingové politiky, AP, případně dalších pravidel pro roamingový systému ***eduroam,*** má poskytovatel identity právo omezit nebo zcela zablokovat autentizaci svých uživatelů. Postupuje přitom podle interních pravidel pro používání roamingových služeb.

Čl. 9 - **Odpovědnost**

Česká ***eduroam*** federace a sdružení CESNET jako správce této federace neposkytuje žádné garance týkající se dostupnosti a funkčnosti systému ***eduroam*** v rámci federace. Systém je provozován jako „best effort“ a jeho služby jsou poskytovány bez záruky.

Čl. 10 – **Přechodná ustanovení**

Z důvodu snadného přechodu od již nainstalovaných systémů s webovým ověřováním k technologii splňující kritéria této roamingové politiky se definuje tzv. „přechodné období“. Po jeho skončení již nebude přípustné používat webovou autentizaci, která je z principu nedostatečně zabezpečená proti zneužití.
Tato přechodná fáze končí 1. října 2007.
Dále již nebude přípustné jakkoli spojovat webově autentizované sítě se systémem ***eduroam*** (např. použitím loga, SSID eduroam atp.).

Čl. 11 – **Závěrečná ustanovení**

11.1 Tento dokument nabývá platnosti a účinnosti **1. září 2007** a je platný v rámci české ***eduroam*** federace.

11.2 V rámci české ***eduroam*** federace je tento dokument nadřazen evropské konfederační politice. Nastane-li nesrovnalost mezi těmito dvěma dokumenty, postupuje se v rámci ČR podle ustanovení uvedených v této federační politice.

V Praze dne 4.6.2007

Ing. Jan Gruntorád, CSc., v. r.
Ředitel sdružení CESNET