Regulamin eduroam

Preambuła

eduroam jest zadaniem realizowanym przez Konsorcjum PIONIER w ramach umowy Lidera Konsorcjum z Ministrem Nauki i Szkolnictwa Wyższego, umowy nr POIG.02.03.00-00-028/08-00 o dofinansowanie projektu pn. Platforma Obsługi Nauki PLATON - Etap I: Kontener usług wspólnych realizowanego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 (Priorytet 2 Infrastruktura sfery B + R, Działanie 2.3 Inwestycje związane z rozwojem infrastruktury informatycznej nauki, Poddziałanie 2.3.1 Projekty w zakresie rozwoju infrastruktury informatycznej nauki oraz 2.3.3 Projekty w zakresie rozwoju zaawansowanych aplikacji i usług teleinformatycznych).

I. Wprowadzenie

§1

Niniejszy regulamin (zwany dalej „Regulaminem") określa zasady i warunki realizacji eduroam w sieci PIONIER w ramach projektu PLATON.

§2

Definicje pojęć:

a. Lider – Instytut Chemii Bioorganicznej PAN – Poznańskie Centrum Superkomputerowo-Sieciowe;
b. Partner/rzy Realizujący eduroam – jedna lub kilka z wymienionych poniżej instytucji, w których realizowany jest eduroam. Partnerami tymi są:
   - Akademia Górniczo-Hutnicza - Akademickie Centrum Komputerowe Cyfronet AGH w Krakowie,
   - Instytut Chemii Bioorganicznej PAN – Poznańskie Centrum Superkomputerowo-Sieciowe,
   - Instytut Uprawy, Nawożenia i Gleboznawstwa - Państwowy Instytut Badawczy,
   - Naukowa i Akademicka Sieć Komputerowa – instytut badawczy,
   - Politechnika Białostocka,
   - Politechnika Częstochowska
   - Politechnika Gdańska – Centrum Informatyczne TASK,
   - Politechnika Koszalińska,
   - Politechnika Łódzka,
   - Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu,
   - Politechnika Rzeszowska,
   - Politechnika Śląska Centrum Komputerowe,
   - Politechnika Wrocławska Wrocławskie Centrum Sieciowo–Superkomputerowe,
   - Uniwersytet Marii Curie-Skłodowskiej LubMAN UMCS,
   - Uniwersytet Mikołaja Kopernika w Toruniu,
   - Uniwersytet Opolski,

- Uniwersytet Technologiczno-Przyrodniczy im. Jana i Jędrzeja Śniadeckich,
- Uniwersytet Warmińsko-Mazurski,
- Uniwersytet Warszawski,
- Uniwersytet Zielonogórski,
- Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Akademickie Centrum Informatyki.

c. Świadczący – członek Konsorcjum PIONIER udostępniający eduroam;
d. Sieć MAN (ang. *Metropolitan Area Network*) – szerokopasmowa sieć miejska lub regionalna zarządzana przez członka Konsorcjum PIONIER;
e. Sieć PIONIER - ogólnopolska szerokopasmowa sieć optyczna stanowiąca bazę dla badań naukowych i prac rozwojowych w obszarze informatyki i telekomunikacji, nauk obliczeniowych, aplikacji oraz usług dla społeczeństwa informacyjnego. Obecnie łączy 21 ośrodków Miejskich Sieci Komputerowych (sieci MAN) i 5 Centrów Komputerów Dużej Mocy za pomocą własnych łączy światłowodowych;
f. Konsorcjum PIONIER – formalne porozumienie zawarte przez 21 Miejskich Sieci Komputerowych MAN i 5 Centrów Komputerów Dużej Mocy (KDM);
g. Jednostka – jednostka prowadząca działalność naukową lub edukacyjną, do której stosują się przepisy ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki (dz. U. Z 2010 r. Nr 96, poz. 615, Art. 2, lit. 9 lub instytucja edukacyjna, oświatowa, jednostka administracji rządowej lub samorządowej, instytucja kulturalna, biblioteka, jednostka służby zdrowia, instytucja wyższej użyteczności i pożytku publicznego, mająca zawartą umowę na realizację usług telekomunikacyjnych w sieci MAN, tj. będąca abonentem sieci MAN;
h. Korzystający – Jednostka, która zaakceptowała niniejszy Regulamin i podpisała deklarację chęci korzystania z eduroam;
i. Użytkownik – pracownik, student, doktorant Korzystającego lub Świadczącego bądź osoba realizująca prace zlecone lub zamówione dzieło na rzecz Korzystającego lub Świadczącego;
j. Przedstawiciel Korzystającego – osoba uprawniona przez Korzystającego do kontaktów ze Świadczącym;
k. eduroam - zastrzeżony znak towarowy zarejestrowany przez organizację TERENA na potrzeby ogólnoświatowej inicjatywy „*educational roaming*”. Pojęcie eduroam obejmuje zarówno projekt pilotowy o zasięgu ogólnoświatowym, jak również dostęp eduroam w sieci GEANT;
l. Operator eduroam w Polsce (w znaczeniu określonym przez Europejską Politykę eduroam - National Roaming Operator) - Lider;
m. Krajowy koordynator eduroam w Polsce - Uniwersytet Mikołaja Kopernika, Uczelniane Centrum Informatyczne (UCI UMK) pełniący tę funkcję na mocy porozumienia z Liderem;
n. Polska Federacja eduroam (w znaczeniu używanym w Europejskiej Polityce eduroam) - Konsorcjum PIONIER oraz Korzystający;
o. Europejska konfederacja eduroam – porozumienie mające na celu międzynarodową współpracę w zakresie upowszechnienia dostępu do Internetu użytkownikom krajowych naukowych sieci informatycznych regulowane dokumentami:
   - European eduroam Confederation Policy Declaration i eduroam Policy Service Definition,
   - Deklaracja przystąpienia do Europejskiej Konfederacji eduroam podpisana przez Operatora eduroam w Polsce.
p. Specyfikacja techniczna – część „Specyfikacja techniczna eduroam w Polsce” niniejszego Regulaminu;

q. Zasób eduroam - punkt gościnnego dostępu do sieci (bezprzewodowy lub przewodowy), łącznie z mechanizmami uwierzytelniania użytkowników podłączony do struktury eduroam;

§3

Zastrzeżenia:

a. Znak oraz nazwa eduroam mogą być używane tylko w odniesieniu do inicjatywy eduroam i zasobów z nią związanych. Dodatkowe informacje i dokumenty na temat formalnych aspektów eduroam są dostępne pod adresem www.eduroam.org;
b. Zasoby eduroam udostępniane użytkownikom powinny być oznakowane logo eduroam, przy czym dopuszczalne jest oznakowanie całych budynków, bądź obszarów w tych budynkach, gdzie sieć jest dostępna. Użycie logo eduroam musi być zgodne z zasadami opublikowanymi na www.eduroam.org;
c. Informacja o lokalizacji zasobów eduroam musi być wprowadzana do bazy lokalizacji w ramach portalu administracyjnego eduroam.

II. Dostęp do eduroam

§4

1. Korzystający korzysta z eduroam na podstawie złożonej Deklaracji chęci korzystania z eduroam, zawierającej m.in. akceptację niniejszego Regulaminu.
2. Korzystający musi wyrazić zgodę na uruchomienie w swojej sieci gościnnego dostępu do Internetu. Korzystający jest zatem **Instytucją udostępniającą zasoby eduroam**. Dostęp gościnny powinien być zagwarantowany na możliwie najszerszym obszarze sieci Korzystającego.
3. Każdy Korzystający może występować w roli **Instytucji uwierzytelniającej** i tym samym zapewniać swoim Użytkownikom dostęp do Internetu na terenie wszystkich instytucji współpracujących z eduroam.
4. Wyrażenie chęci korzystania z eduroam jest dokonywane poprzez podpisanie deklaracji przez osobę upoważnioną do reprezentowania Instytucji (załącznik nr 1).
5. Deklaracje chęci korzystania z eduroam przyjmuje właściwy Świadczący.

§5

1. eduroam polega na dostarczeniu mechanizmów pozwalających na uwierzytelnianie Użytkowników w sieci komputerowej, z wykorzystaniem standardu 802.1x i serwera uwierzytelniającego Korzystającego.
2. eduroam umożliwia zainteresowanym Korzystającym uruchomienie uwierzytelnianego gościnnego dostępu na swoim terenie.
3. Użytkownicy eduroam uzyskują możliwość korzystania z gościnnego dostępu we wszystkich sieciach eduroam na świecie.

§6

Ogólnoświatowa inicjatywa eduroam jest tworzona w postaci federacyjnej struktury zaufania, której podmiotami są:

a. krajowe federacje eduroam;
b. operatorzy krajowych, akademickich sieci komputerowych reprezentujący krajowe federacje eduroam;
c. Europejska Konfederacja eduroam, jako stowarzyszenie europejskich federacji krajowych;

d. konfederacje eduroam w innych regionach świata.

III Zobowiązania w ramach eduroam

§7

eduroam jest świadczony w trybie 24h/365 zgodnie z następującymi zasadami:

a. serwery eduroam działają bez przerw, a w przypadku awarii są automatycznie zastępowane przez serwery zapasowe;
b. serwis informacyjny eduroam działa bez przerw;
c. administratorzy Świadczących oraz krajowy Koordynator są dostępni w dni robocze w godzinach 8.00 do 15:30;
d. zgłoszenia za pomocą e-mail mogą być zgłaszane w dowolnym momencie, odpowiedź zostanie udzielona bieżącego dnia, o ile zgłoszenie wpłynęło do godziny 14:00 w dniu roboczym, lub nie później niż w kolejnym dniu roboczym, o ile zgłoszenie wpłynęło po godzinie 14 lub w dniu wolnym od pracy.

§8

Zadania jednostek zarządzających eduroam:

a. zadania Operatora polegają na:
   - reprezentowaniu Konsorcjum PIONIER w Europejskiej Konfederacji eduroam,
   - nadzorowaniu przestrzegania Europejskiej Polityki eduroam,
   - nadzorowaniu wdrażania i przestrzegania niniejszego Regulaminu,
   - przyjmowaniu deklaracji chęci korzystania z eduroam od członków Konsorcjum PIONIER oraz bezpośrednich abonentów sieci PIONIER,
   - prowadzenia zapasowego krajowego serwera pośredniczącego eduroam i utrzymywaniu logów przechodzących przez niego transakcji uwierzytelnienia.
b. zadania krajowego Koordynatora eduroam polegają na:
   - nadzorowaniu i koordynowaniu rozwoju eduroam w Polsce,
   - udziale w ciałach koordynujących międzynarodowy rozwój eduroam,
   - prowadzeniu głównego krajowego serwera pośredniczącego eduroam i utrzymywaniu logów przechodzących przez niego transakcji uwierzytelnienia oraz nadzorowaniu działania zapasowego serwera krajowego eduroam,
   - monitorowaniu sprawności serwerów uwierzytelniających Korzystających z eduroam,
   - koordynowaniu obsługi zdarzeń niepożądanych (nadużyć prawa, etykiety itp.) związanych z działaniem eduroam,
   - utrzymywaniu serwisu www.eduroam.pl,
   - utrzymywaniu serwisu administratorów eduroam (bazy Korzystających i lokalizacji, list mailowych, wiki),
   - utrzymywaniu centralnego serwisu zbierania statystyk korzystania z eduroam,
   - zatwierdzaniu wystąpień Korzystających o przydział certyfikatów na potrzeby połączeń w protokole RADIUS-TLS (Internet Draft).
c. zadania Świadczących polegają na:
   - udzielaniu wsparcia jednostkom zlokalizowanym w obsługiwanym regionie, korzystającym lub pragnącym korzystać z eduroam,
   - prowadzeniu dwóch regionalnych serwerów pośredniczących eduroam,

utrzymywania logów operacji uwierzytelnienia przesyłanych poprzez regionalne serwery pośredniczące,
- prowadzeniu rejestru Korzystających z eduroam,
- przyjmowaniu deklaracji chęci korzystania z eduroam od użytkowników sieci MAN,
- współpracy z krajowym Koordynatorem eduroam,
- współpracy z krajowym Operatorem eduroam w Polsce.

§9

Obowiązki Korzystającego z eduroam:

a. Jako instytucja udzielająca gościnnego dostępu do Internetu Korzystający zobowiązuje się do:
   - zapewnienia dostępu do swojej sieci wszystkim osobom, które zostały poprawnie uwierzytelnione przez inne instytucje stowarzyszone w eduroam, na warunkach określonych w Specyfikacji technicznej,
   - wprowadzania i aktualizowania informacji o własnych zasobach eduroam w portalu administracyjnym eduroam,
   - prowadzenia serwisu WWW pod adresem http://eduroam.(nazwa_domenowa_instytucji), w którym muszą być zawarte podstawowe informacje dla gości w językach polskim i angielskim zgodnie ze Specyfikacją techniczną.
b. Jako instytucja uwierzytelniająca Korzystający z eduroam zobowiązuje się do:
   - poinformowania swoich Użytkowników o niniejszym Regulaminie i zobowiązania ich do jego przestrzegania,
   - potwierdzania tożsamości wyłącznie uprawnionych, zarejestrowanych osób za pomocą serwera uwierzytelniającego,
   - utrzymywania zapisów wszystkich operacji uwierzytelnienia, zgodnie z wymaganiami opisanymi w Specyfikacji technicznej,
   - współpracy z krajowym Koordynatorem eduroam w Polsce w wypadkach naruszenia bezpieczeństwa, etykiety sieciowej, prawa itp.,
   - udzielania wsparcia technicznego zarejestrowanym przez nią osobom pragnącym skorzystać z zasobów eduroam udostępnianych lokalnie i w innych instytucjach biorących udział w eduroam.

§10

Obowiązki Użytkowników:

a. Użytkownik jest odpowiedzialny za wszelkie działania sieciowe dokonane po uwierzytelnieniu przy pomocy jego danych uwierzytelniających. W przypadku podejrzenia, że dane uwierzytelniające mogły się dostać w ręce osób trzecich, Użytkownik jest zobowiązany do niezwłocznego zawiadomienia o tym fakcie administratora w swojej instytucji macierzystej, w przypadku niewykonania powyższego obowiązku Użytkownik ponosi pełną odpowiedzialność za szkody wywołane działaniem lub zaniechaniem osób trzecich korzystających z jego danych uwierzytelniających. Dane kontaktowe administratora są podawane w odpowiednim serwisie internetowym instytucji macierzystej;
b. Użytkownik powinien dołożyć starań, aby przed wysłaniem danych uwierzytelniających upewnić się, że korzysta z autentycznego zasobu eduroam (zgodnie z zaleceniami swojej instytucji macierzystej);
c. Użytkownik powinien być świadomy, że fakt gościnnego korzystania z sieci jest

odnotowywany w logach systemowych zarówno instytucji udostępniającej zasoby, jak i jego macierzystej instytucji uwierzytelniającej;
   d. Użytkownik musi działać zgodnie z lokalnym prawem i regulaminem sieci komputerowej, z której korzysta;
   e. Użytkownik eduroam może korzystać z gościnnego dostępu wyłącznie na swój własny użytek.

IV Specyfikacja techniczna korzystania z eduroam w sieci PIONIER

§11

Używane w tekście słowa kluczowe „MUSI", „MOŻE", „POWINIEN", „NIE WOLNO" i ich odmiana, pisane wielkimi literami są używane zgodnie z definicją ich angielskich odpowiedników określonych w RFC 2119, w szczególności słowo „POWINEN" należy rozumieć w taki sposób, że niespełnienie warunku opatrzonego tą klauzulą jest dopuszczalne tylko w szczególnie uzasadnionych przypadkach.

§12

1. Struktura serwerów Radius eduroam w Polsce składa się z:
   a. serwerów udostępniających zasoby;
   b. serwerów uwierzytelniających (często pełniących również rolę serwera udostępniającego zasoby);
   c. regionalnych serwerów pośredniczących;
   d. krajowych serwerów pośredniczących.
2. Rolą serwerów pośredniczących jest przekazywanie zleceń uwierzytelnienia, dotyczących gościnnego dostępu do sieci eduroam. Serwer pośredniczący MUSI być zdublowany.
3. Dodatkową rolą serwera pośredniczącego jest monitorowanie ruchu i zapewnienie dodatkowego poziomu bezpieczeństwa w strukturze zaufania.
4. Wszelkie dane archiwalne dotyczące procesu uwierzytelniania MUSZĄ być odpowiednio chronione.
5. Serwery pośredniczące MUSZĄ monitorować występowanie atrybutów Tunnel-Type, Tunnel-Medium-Type i Tunnel-Private-Group-ID, ponieważ pojawianie się ich zazwyczaj jest spowodowane błędem w konfiguracji serwerów lokalnych i może doprowadzać do zakłóceń działania eduroam. W przypadku wykrycia występowania takich atrybutów, administrator serwera pośredniczącego zgłasza ten fakt administratorowi serwera, który generuje pakiety zawierające te atrybuty.
6. Serwery pośredniczące MUSZĄ reagować na otrzymane pakiety Accounting-Request odsyłając pakiet Accounting-Response i nie przesyłając dalej pakietu Accounting-Request. Wyjątkiem od tej zasady może być umowa między konkretnymi Korzystającymi i właściwymi Świadczącymi dotycząca przesyłania ruchu Accounting pomiędzy konkretnymi instytucjami.
7. Serwery pośredniczące MUSZĄ na bieżąco przesyłać informacje do centralnego serwisu zbierania statystyk prowadzonego przez krajowego Koordynatora eduroam. Zasady przesyłania tych informacji określa krajowy Koordynator eduroam.

§13

Rola instytucji udostępniającej zasoby:

   a. Sieć bezprzewodowa udostępniana, jako zasób eduroam podlega następującym zasadom:
      - z wyjątkiem sytuacji szczególnych opisanych w §13 lit. b, nazwa sieci (SSID)

MUSI mieć wartość „eduroam” i ta nazwa MUSI być rozgłaszana,
- sieć MUSI wspierać szyfrowanie WPA2-AES i MOŻE dodatkowo wspierać WPA-TKIP w połączeniu z 802.1x (tzw. WPA2-Enterprise lub WPA-Enterprise),
- przy dostępie do sieci NIE WOLNO stosować portali WWW wymagających wprowadzenia danych uwierzytelniających użytkownika.

b. W przypadkach, kiedy występuje nakładanie się zasięgów sieci dwóch Korzystających z eduroam prowadzące do zakłóceń w dostępie użytkowników do sieci, Korzystający powinni dołożyć starań, by poprzez odpowiednią konfigurację i ustawienie swoich urządzeń zminimalizować zakłócenia;
c. Sieć przewodowa udostępniana, jako zasób eduroam MUSI stosować uwierzytelnianie 802.1x;
d. Sieci udostępniane, jako zasób eduroam MUSZĄ w sposób przezroczysty traktować protokół EAP;
e. Pakiety uwierzytelniające z nazwą użytkownika zawierającą realm nie należący do polskiej instytucji MUSZĄ być kierowane przez strukturę eduroam do krajowych serwerów pośredniczących, z wyjątkiem sytuacji opisanej w §13 lit. g.;
f. Pakiety uwierzytelniające z nazwą użytkownika zawierającą realm, który nie odpowiada domenie zarejestrowanej przez daną instytucję udostępniającą zasoby, POWINNY być kierowane do serwera eduroam stojącego w hierarchii bezpośrednio powyżej serwera danego Korzystającego, z wyjątkiem sytuacji opisanej w §13 lit. g. Odstępstwa od tej reguły MUSZĄ być uzgadniane z administratorami regionalnych serwerów pośredniczących lub krajowym Koordynatorem eduroam w Polsce;
g. Od momentu ogłoszenia dokumentu **Zasady bezpieczeństwa obowiązujące przy bezpośrednich połączeniach serwerów eduroam**, pakiety uwierzytelniające nazwą użytkownika zawierającą realm, który nie odpowiada domenie zarejestrowanej przez daną instytucję udostępniającą zasoby, MOGĄ być kierowane bezpośrednio do serwera wskazanego przez system DNS, z zachowaniem warunków opisanych w tym dokumencie;
h. Serwer udostępniający zasoby NIE MOŻE wysyłać pakietów Accounting-Request z wyjątkiem sytuacji opisanych §12 ust. 6;
i. Informacje o uwierzytelnieniach użytkowników korzystających z gościnnego dostępu na terenie Instytucji POWINNY być przesyłane do centralnego serwisu zbierania statystyk prowadzonego przez krajowego Koordynatora eduroam;
j. Serwer Instytucji POWINIEN dołączać do zapytań uwierzytelniających atrybut Operator-Name (RFC-5580) o wartości odpowiadającej głównej nazwie domenowej instytucji;
k. Serwer Instytucji MOŻE dołączać do zapytań uwierzytelniających zapytanie Chargeable-User-Identity (RFC-4372);
l. Gościnny dostęp do Internetu, udostępniany, jako zasób eduroam, POWINIEN być otwarty. Wprowadzanie blokad może utrudnić lub uniemożliwić korzystanie z ważnych zasobów naukowych, jak np. PL-GRID;
m. W ramach gościnnego dostępu do Internetu, udostępnianego, jako zasób eduroam, MUSI być zagwarantowany dostęp do następujących zasobów:
    - Standard IPSec VPN: IP protokoły 50 (ESP) and 51 (AH) (oba wejście i wyjście); UDP/500 (IKE) (tylko wyjście);
    - OpenVPN 2.0: UDP/1194;
    - IPv6 Tunnel Broker service: IP protokół 41;
    - IPsec NAT-Traversal UDP/4500;
    - Cisco IPSec VPN over TCP: TCP/10000 (tylko wyjście);
    - PPTP VPN: IP protokół 47 (GRE) (wejście i wyjście); TCP/1723 (tylko wyjście);

- SSH: TCP/22 (tylko wyjście);
- HTTP/HTTPS: TCP/80, TCP/443, TCP/3128, TCP/8080 (wszystkie tylko wyjście);
- IMAP2+4: TCP/143 (tylko wyjście);
- IMAP3: TCP/220 (tylko wyjście);
- IMAPS: TCP/993 (tylko wyjście);
- POP: TCP/110 (tylko wyjście);
- POP3S: TCP/995 (tylko wyjście);
- NTP: UDP/123 (tylko wyjście);
- Passive (S)FTP: TCP/21 (tylko wyjście)+ inne wysokie porty wykorzystywane zgodnie z protokołem Passive (S)FTP (wyjście);
- SMTPS: TCP/465 (tylko wyjście);
- SMTP submit z STARTTLS: TCP/587 (tylko wyjście);
- RDP: TCP/3389 (tylko wyjście);
- XMPP – TCP/5222 (tylko wyjście);
- H.323 – TCP/1719, TCP/1720 (tylko wyjście);
- SIP: TCP/UDP/5060-5061 (tylko wyjście).+inne wysokie porty wykorzystywane zgodnie z protokołem SIP;
- FRING: TCP/18182(wychodzący) TCP/UDP 52000-53800(wychodzące).

n. Instytucja udostępniająca zasoby MOŻE stosować przezroczyste proxy zabezpieczające przed wysyłaniem spamu i propagacją wirusów;

o. Instytucja udostępniająca zasoby, we własnym interesie, POWINNA stosować środki techniczne umożliwiające identyfikację użytkowników działających w sieci. Brak odpowiednich środków i logów uniemożliwi przeniesienie odpowiedzialności za naruszenia prawa dokonane z sieci gościnnej. W szczególności:
   - wskazane jest, aby gościnny dostęp do Internetu był realizowany w wydzielonym VLAN-ie,
   - w ramach gościnnego dostępu do Internetu NIE POWINNNO się stosować adresów prywatnych i NAT,
   - stosowane środki techniczne POWINNY pozwalać na powiązanie działań użytkownika eduroam z konkretną sesją uwierzytelnienia, w szczególności niemożliwa powinna być zmiana adresu IP na inny niż nadany użytkownikowi w czasie logowania do sieci.

p. Instytucja udostępniająca zasoby MUSI przechowywać logi sesji uwierzytelnienie i POWINNA przechowywać logi wiążące adresy IP z sesjami uwierzytelniania. Czas przechowywania logów NIE POWINIEN być krótszy niż 6 miesięcy. Logi MUSZĄ być znakowane czasem synchronizowanym za pomocą protokołu NTP i MUSZĄ zawierać:
   - czas uwierzytelnienia i przydzielenia adresu IP,
   - identyfikator (EAP outer identity) osoby uwierzytelnionej,
   - adres MAC klienta,
   - adres IP klienta,
   - identyfikator Chargeable-User-Identity (o ile został odebrany).

q. Instytucja MUSI prowadzić po polsku i angielsku informacyjny serwis WWW przeznaczony dla gości i zawierający przynajmniej:
   - logo eduroam wraz z odsyłaczem do strony www.eduroam.pl,
   - tekst zawierający informację o dostępności zasobów eduroam na terenie Instytucji i akceptację niniejszego Regulaminu (łącznie z odsyłaczem do

dokumentu umieszczonego w ogólnopolskim serwisie eduroam),
- informacje o obszarze, na którym jest udostępniane są zasoby eduroam,
- informacje techniczne o udostępnianych zasobach eduroam, a więc: rodzaju protokołu bezprzewodowego (802.11b, 802,11g, 802.11a, 802.11n), rozgłaszaniu lub nierozgłaszaniu SSID eduroam, rodzaju szyfrowania (WPA2/AES, WPA/TKIP, itp.),
- informacje o stosowanych ogranicznikach dostępu (stosowanych filtrach) oraz o zakresie zbieranej informacji o połączeniach,
- informacje (lub odsyłacz) o lokalnych zasad korzystania z sieci.

§14

Rola instytucji uwierzytelniającej:

a. Serwer uwierzytelniający instytucji uwierzytelniającej MUSI stosować bezpieczne metody EAP. EAP-MD5 jest uważany za niedostatecznie bezpieczny i w związku z tym NIE MOŻE być stosowany;
b. Instytucja uwierzytelniająca MUSI dołożyć starań, aby oprogramowanie 802.1x, z którego korzystają uwierzytelniane przez nią osoby, było skonfigurowane w sposób uniemożliwiający przesłanie danych uwierzytelniających do niepowołanego serwera;
c. Instytucja uwierzytelniająca MUSI dołożyć starań, aby osoby przez nią uwierzytelniane znały podstawowe zasady bezpieczeństwa przy korzystaniu z sieci bezprzewodowych;
d. Instytucja uwierzytelniająca MUSI prowadzić serwis internetowy zawierający kontakt do administratora serwera uwierzytelniającego;
e. Instytucja uwierzytelniająca MUSI przechowywać logi systemowe dotyczące uwierzytelnień eduroam dokonanych spoza jej własnej sieci. Czas przechowywania logów NIE MOŻE być krótszy niż 6 miesięcy. Logi MUSZĄ być znakowane czasem synchronizowanym za pomocą protokołu NTP i MUSZĄ zawierać:
   - czas otrzymania zlecenie uwierzytelnienia,
   - wartość atrybutu Calling-Station-Id zawartą w pakiecie uwierzytelniającym,
   - wartość atrybutu Chargeable-User-Identity (o ile została wysłana),
   - dane pozwalające na zidentyfikowanie użytkownika, którego uwierzytelniono.
f. Serwer uwierzytelniający Instytucji POWINIEN odpowiadać na żądania Chargeable-User-Identity (zgodnie z RFC-4372) pod warunkiem, że żądania zawierają atrybut Operator-Name (zgodnie z RFC-5580). Wartość atrybutu przekazywana w odpowiedzi CUI MUSI mieć niezmienną wartość dla jednego użytkownika i jednej wartości Operator-Name. Wartość atrybutu CUI MUSI być skonstruowana w sposób, który gwarantuje, że odczytanie na jej podstawie rzeczywistego identyfikatora użytkownika jest możliwe wyłącznie w instytucji macierzystej;
g. Instytucja MUSI udostępnić krajowemu Koordynatorowi eduroam konto testowe służące do monitorowania poprawności pracy serwera uwierzytelniającego tej instytucji;
h. Instytucja MUSI wyznaczyć administratorów odpowiedzialnych za kontakty ze Świadczącym eduroam.

V Incydenty sieciowe

§15

Pod pojęciem incydentów sieciowych rozumiane będą naruszenia prawa, naruszenia etykiety

internetowej oraz naruszenia lokalnych regulacji instytucji udostępniających zasoby przez użytkowników eduroam korzystających z gościnnego dostępu do Internetu.

§16

Naruszenia prawa:

a. W przypadkach, kiedy z Korzystającym skontaktują się, w trybie zgodnym z aktualnie obowiązującym prawem dla danego przypadku, właściwe organy ścigania w celu pozyskania informacji na temat konkretnego incydentu z udziałem adresu IP przydzielonego w efekcie poprawnego uwierzytelnienia eduroam, Korzystający MUSI:
   - zlokalizować fragmenty logów odpowiadających danemu incydentowi i przekazać je uprawnionym organom ścigania, razem z informacją, że zlokalizowanie konkretnej osoby będzie możliwe we współpracy z pozostałymi elementami struktury eduroam,
   - poinformować krajowego Koordynatora eduroam o wystąpieniu incydentu i przekazać mu dane na temat czasu sesji uwierzytelniania i odnotowanego identyfikatora użytkownika.
b. Krajowy Koordynator eduroam (przy pomocy administratora regionalnego serwera pośredniczącego lub administratora głównego serwera eduroam) ustala dane instytucji uwierzytelniającej odpowiedzialnej za użytkownika i przekazuje te dane organom ścigania;
c. Tylko macierzysta instytucja uwierzytelniająca może przekazać dane osobowe użytkownika i czyniąc to MUSI stosować się do ograniczeń stawianych przez ustawę o ochronie danych osobowych.

§17

Naruszenia etykiety sieciowej i lokalnych regulacji:

a. W przypadkach, kiedy incydenty nie naruszają prawa, ale są działaniami niepożądanymi z punktu widzenia instytucji udostępniającej zasoby, administrator eduroam w tej instytucji zawiadamia o incydencie krajowego Koordynatora eduroam;
b. Krajowy Koordynator eduroam przejmuje sprawę, w celu zawiadomienia instytucji macierzystej użytkownika o problemie i spowodowania, by incydent nie mógł się powtórzyć;
c. Instytucja udostępniająca zasoby ma prawo zablokować uwierzytelnianie wszystkich użytkowników związanych z instytucją, której użytkownik spowodował incydent. Możliwość uwierzytelniana powinna zostać przywrócona po wyjaśnieniu sprawy;
d. Incydenty międzynarodowe są rozwiązywane z udziałem PIONIER CERT – http://cert.pionier.gov.pl.

VI Ustalenia końcowe

§18

1. Lider czuwa nad wdrażaniem niniejszego Regulaminu.
2. Wszelkie zmiany niniejszego Regulaminu będą dokonywane w drodze konsultacji z krajowym koordynatorem eduroam oraz partnerami realizującymi eduroam w Polsce.
3. Instytucje partycypujące obecnie w pilotowym projekcie eduroam będą musiały złożyć pisemną deklarację o przyjęciu niniejszego Regulaminu w terminie 6 miesięcy od jego ogłoszenia. W przypadku odmowy przyjęcia niniejszego Regulaminu, Korzystający zostanie odłączony od struktury uwierzytelniającej eduroam.

4. Instytucje korzystające z eduroam nie będą występować względem siebie z roszczeniami cywilno-prawnymi z tytułu ewentualnych incydentów sieciowych.
5. Rezygnacja z korzystania z eduroam powinna być poprzedzona 3-miesięcznym okresem wypowiedzenia i złożona na piśmie pod rygorem nieważności.
6. Regulamin obowiązuje od dnia 18.10.2013r.
7. W sprawach nieuregulowanych niniejszym Regulaminem, mają zastosowanie przepisy Kodeksu cywilnego oraz inne powszechnie obowiązujące przepisy prawa polskiego.
8. Wszelkie spory wynikające z niniejszego Regulaminu, rozstrzygane będą przez sąd powszechny, właściwy dla siedziby Świadczącego, zaś w przypadku Użytkowników - według właściwości przemiennej sądu właściwego dla siedziby Świadczącego albo sądu właściwego dla Użytkownika.

VII Dane kontaktowe

§19

1. Pytania, uwagi, zgłoszenia usterek należy kierować do administratorów eduroam we właściwej siedzibie Świadczącego.
2. Informacje na temat eduroam znajdują się na portalu www.eduroam.pl
3. Dane kontaktowe Świadczących eduroam:

   a. Instytut Chemii Bioorganicznej PAN – Poznańskie Centrum Superkomputerowo-Sieciowe
      ul. Noskowskiego 12/14, 61-704 Poznań
   b. Uniwersytet Technologiczno-Przyrodniczy
      ul. Ks. Kordeckiego 20, 85-225 Bydgoszcz
   c. Akademia Górniczo-Hutnicza - Akademickie Centrum Komputerowe Cyfronet
      ul. Nawojki 11, 30-950 Kraków
   d. Instytut Uprawy, Nawożenia i Gleboznawstwa - Państwowy Instytut Badawczy
      ul. Czartoryskich 8, 24-100 Puławy
   e. Uniwersytet Marii Curie-Skłodowskiej w Lublinie
      Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin
   f. Politechnika Białostocka
      ul. Wiejska 45a, 15-351 Białystok
   g. Politechnika Częstochowska
      ul. Dąbrowskiego 69, 42-200 Częstochowa
   h. Politechnika Gdańska – Centrum Informatyczne TASK
      ul. Narutowicza 11/12, 80-233 Gdańsk
   i. Politechnika Koszalińska
      ul. Śniadeckich 2, 75-453 Koszalin
   j. Politechnika Łódzka
      ul. Wólczańska 175, 90-924 Łódź
   k. Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu
      ul. Malczewskiego 29, 26-600 Radom
   l. Politechnika Rzeszowska – Centrum Zarządzania Rzeszowską Miejską Siecią Komputerową
      ul. M. Skłodowskiej-Curie 8/2, 35-959 Rzeszów
   m. Zachodniopomorski Uniwersytet Technologiczny - Akademickie Centrum Informatyki
      Al. Piastów 17, 70-310 Szczecin

n. Politechnika Śląska – Centrum Komputerowe
   ul. Akademicka 16, 44-100 Gliwice
o. Politechnika Świętokrzyska
   Al. Tysiąclecia Państwa Polskiego 7, 25-314 Kielce
p. Politechnika Wrocławska - Wrocławskie Centrum Sieciowo–Superkomputerowe
   ul. Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
q. Uniwersytet Mikołaja Kopernika - Uczelniane Centrum Informatyczne
   ul. Gagarina 11 , 87-100 Toruń
r. Uniwersytet Opolski
   pl. Kopernika 11a, 45-040 Opole
s. Uniwersytet Warmińsko-Mazurski - Ośrodek Eksploatacji i Zarządzania Miejską Siecią Komputerową OLMAN
   ul. Heweliusza 8, 10-726 Olsztyn
t. Uniwersytet Warszawski - Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego
   ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa
u. Uniwersytet Zielonogórski - Centrum Komputerowe
   ul. Licealna 9, 65-417 Zielona Góra
v. Naukowa i Akademicka Sieć Komputerowa w Warszawie
   ul. Wąwozowa 18, 02-796 Warszawa