EDUROAM

National policy for Armenia

version 1.0

01 May 2012

TABLE OF CONTENTS

1. Background to this document

1.1 This document sets out guidelines that cover the control of the supply and receipt of Internet access for educational and scientific purposes that is primarily (but not exclusively) offered to visitors of Participating Organizations within Armenia.

1.2 eduroam[1] is a TERENA[2] registered trademark and is an abbreviation for "educational roaming" that originated from a European National Education and Research Networks (NRENs) project to deliver a user-friendly, secure and scalable Internet access solution for visitors. The European eduroam confederation provides the legal framework for the organization of the European eduroam service. The use of eduroam is restricted to the closed community served by NRENs according to their national policies.

1.3 More information about eduroam is available at the relevant eduroam Service Provider (ESP) website[3].

2. Roles and Responsibilities

2.1 ASNET-AM

2.1.1 This policy and any future changes requires ratification by Academic Scientific Network of Armenia (ASNET-AM)[4].

2.2 eduroam Service Provider (ESP)

2.2.1 The ESP will coordinate the management and support delivery of eduroam services in accordance with the current eduroam Service Definition and Implementation Plan detailed in Schedule 1 of this document.

2.2.2 The ESP role is two fold, (1) to coordinate and support the eduroam service to nominated technical contacts of participating organizations only, and (2) to maintain

---

[1] eduroam, http://www.eduroam.org
[2] Trans-European Research and Education Networking Association, http://www.terena.org
[3] Eduroam in Armenia, http://www.eduroam.am
[4] ASNET-AM, http://www.asnet.am

links with the global eduroam community and their respective authentication servers, and contribute to the further development of the eduroam concept.

2.2.3 The ESP is responsible for maintaining and developing a national authentication server network that connects to participating organizations on a best efforts basis. The ESP assumes no liability for any impact as a result of a loss or disruption of service.

2.2.4 The ESP is responsible for managing a second line technical support function covering pre-connection and ongoing technical support and maintenance of a dedicated website containing technical, service, policy and process information[5], and mailing lists.

2.2.5 The ESP is responsible for coordinating communications between participating organizations so that policies and procedures contained herein are adhered to in a timely manner and as a matter of last resort has
the right to impose technical sanctions.

2.2.6 The ESP will work with the nominated eduroam technical contact of a participating organization to test one or more of the following aspects (1) initial connectivity, (2) authentication and authorization processes and (3) the authorized services offered, and review of the logging activities and the relevant authentication server configuration for compliance with the policy.

2.3 Participating organizations: Home Organization

2.3.1 The role of the home organization is to act as the credential provider for registered staff and students who must be over the age of 18 years of age or have parental consent to use this service.

2.3.2 The role of the home organization is to act as the first line technical and service support function for its users who want to access eduroam services at other participating organizations. Only nominated technical contacts can escalate technical support, service support or security issues on behalf of their users to the ESP.

2.3.3 The home organization must abide by this policy and follow ESP service processes and guidelines listed herein and at the relevant ESP website listed in Schedule 1 of this document.

---

[5] Handling security incidents, abuse of use, service faults, eduroam service blocking or shutdown/restart for operational or security reasons, including notifications thereof.

2.3.4 The home organization is responsible for the behavior of the users they authenticate and must take appropriate action in accordance with their local acceptable use policies (AUP) or equivalent where incidents of abuse are reported by visited organizations.

2.3.5 The home organization must notify to their own users that participating organizations may log user activity.

2.3.6 There is an expectation that the home organization will cooperate with the ESP.

2.3.7 Where the ESP issues a "security advisory" on the ESP website and mailing list, the home organization must comply (and confirm by email to the ESP of compliance) with recommended actions in a timely manner so as not to compromise the security or integrity of the eduroam service.

2.4 Participating organizations: Visited organizations

2.4.1 The role of the visited organization is to supply network access to visitors via eduroam (based on trusting that the visitor's home organization authentication check and response is valid). The visited organization has control over the authorization of services.

2.4.2 The visited organization is not obliged to act as a home organization.

2.4.3 The visited organization can connect to other physical sites to extend eduroam service coverage, however the visited organization would be responsible for maintaining policy compliance and service delivery for itself and other sites connected to it and as such treated as a single virtual organization entity.

2.4.4 Where user activity is monitored, the visited organization must clearly announce this fact including how this is monitored, stored and accessed so as to comply with state or national legislation[6].

2.4.5 The visited organization must abide by this policy and follow ESP service processes and guidelines listed herein and at the relevant ESP website in Schedule 1.

2.4.6 There is an expectation that the visited organization will cooperate with the ESP.

2.5 User

[6] For example, to comply with the new NSW guidelines on workplace surveillance

2.5.1 A user's role is in most cases as a visitor who wants internet access at another participating organization. The user must abide by their home organization AUP or equivalent and respect the visited organization's AUP or equivalent. Where regulations differ and the user has been notified or instructed to do so, the more restrictive applies. For the avoidance of doubt, all users must as a minimum abide by relevant national law.

2.5.2 The user is responsible for taking reasonable steps to ensure that they are connected to a genuine eduroam service including adequate security checks (as directed by their home organization) prior to entering their login credentials.

2.5.3 The user is responsible for their credentials and must not allow them or authorized internet access to be shared or used independently by other users.

2.5.4 If credentials may have been lost or compromised, the user must immediately report back to their home organization.

2.5.5 The user is responsible for informing the visited organization (where possible) and home organization of any faults with the eduroam service.

2.5.6 The user is responsible for keeping their systems patched and uninfected with viruses, otherwise access may be restricted by the visited organization.

3. Base service

3.1 Participating organizations must deploy an authentication server in accordance with eduroam technical and policy guidelines available at the relevant ESP website. A secondary authentication server is recommended for resilience purposes.

3.2 The home organization authentication server(s) must be reachable from the ESP authentication servers for authentication and accounting purposes.

3.3 The home organization must create an eduroam test account (eduroam username and password credential, where the "username" should contain the word "test" to enable filters to be applied for eduroam measurement data collection) that will be made accessible to the ESP to assist in pre-connection testing, ongoing monitoring, support and fault finding activities. If the test account password is changed, the ESP must be notified by the home organization in a timely manner. Ideally, no authorized services should be accorded to the test account.

3.4 The visited organization may offer any media; however as a minimum, wireless

LAN IEEE 802.11b is required whilst 802.11g is also recommended.

3.5 The visited organization must use "eduroam" as the SSID where there are NO instances of an overlap with other participant eduroam wireless hotspots. If the "eduroam" SSID cannot be broadcasted due to technical limitations on the wireless access point, "eduroam" must be made available as a non-broadcasted SSID instead.

3.5.1 Where there are instances of an overlap with other participant eduroam wireless hotspots, affected participating organizations must use a modified SSID name that must be no greater than 31 characters in length and must follow the "eduroam-institution name" where the institution name is a shortened abbreviation of the full name. It must also be a broadcasted SSID. This only applies to overlapping wireless hotspots operated by more than one participating organization that results in users reporting an impact on access to authorized services. In these cases, all relevant participants must also inform the ESP responsible for the maintenance of the eduroam website so that service information to end-users can remain up to date.

3.6 The visited organization must as a minimum implement IEEE 802.1X Extensible Authentication Protocol (EAP) authentication (excluding EAP-MD5) with WPA/TKIP, with a strong recommendation to move to WPA2 as soon as practically possible to promote a consistent service and reasonable level of security.

3.7 The recommended access offered by the visited organization is vpn, http, https, and ssh on both on net and off net however visited organizations may vary this access to meet with their requirements on the proviso that the services offered are publicized on both the visited organization's eduroam web pages and on the relevant ESP website.

3.8 Where the visited organization chooses to offer network access that includes commodity Internet access (e.g. off.net) to authenticated users, the cost of access is charged to the visited organization.

3.9 The visited organization should implement a visitor VLAN for eduroam-authenticated users that is not to be shared with other network services. The VLAN must use of publicly routable IPv4/IPv6 addresses using DHCP and should not use NAT for IPv4 addresses[7].

---

[7] NAT is discouraged because it could impact on current VPN services and future application services that may become available on eduroam.

3.10 The visited organization is recommended to use Quarantine Virtual LANs that check the user device has up to date operating system and antivirus patches and no known viruses, prior to allowing authorized Internet access.
3.11 The visited organization must not charge for eduroam access. This service is based on a shared access model where participating organizations supply and receive Internet access for their users.
3.12 Where the ESP issues a "security advisory" on the ESP website and mailing list, the visited organization must comply (and confirm by email to the ESP of compliance) with recommended actions in a timely manner so as to not compromise the security or integrity of the eduroam service.

4. Logging

4.1 Participating organizations must log all authentication and accounting requests; the following information must be recorded:

- The date and time the authentication request was received;
- The RADIUS request's identifier;
- The authentication result returned by the authentication database;
- The reason given if the authentication was denied or failed;
- The value of the request's accounting status type.

4.2 The visited organization must log all DHCP transactions, including

- The date and time of issue of the client's DHCP lease;
- The MAC address of the client;
- The client's allocated IP address.

4.3 The visited organization must keep a log of DHCP transactions for a minimum of three months. Access to these logs should be restricted to the eduroam technical contacts and ESP technical contact, or relevant staff responsible for maintaining and supporting these logs as per the visited organisation policy, to assist in resolving specific security or abuse issues that have been reported to ESP, and for operational support of the service.

5. Support

5.1 The home organization must provide support to their users requesting access at a visited organization campus.
5.2 The home organization should provide support to users from other participating organizations that are requesting eduroam services at their home organization campus.
5.3 The visited organization must publish local information about eduroam services on dedicated web pages on their organization website containing the following minimum information:

- Text that confirms adherence (including a url link) to this policy document must be published at the relevant ESP website.
- A url link to visited organization acceptable use policy or equivalent;
- A list or map showing eduroam access coverage areas;
- Details of the broadcasted or non-broadcasted SSID as eduroam (or equivalent eduroam-inst-name where eduroam overlap occurs);
- A statement that eduroam is only available to users over 18 years of age or those users who have acquired parental consent to use the “non-filtered” Internet access;
- Details of the authentication process and authorized services offered;
- Details about the use of a non-transparent application proxy including user configuration guidelines (if applicable);
- A url link to the relevant ESP website and posting of the eduroam logo and trademark statement;
- Where user activity is monitored, the visited organization must clearly announce this fact including how this is monitored so as to meet with state or national legislation, including how long the information will be held for and who has access to it.
- The contact details of the appropriate technical support that is responsible for eduroam services.

6. Communications

6.1 The home organization must provide the ESP with contact details of two nominated technical contacts. Any changes to contact details must be notified to ESP

in a timely manner.

6.2 The home organization must designate a contact and their contact details to respond to security issues; this may be the same person designated as the nominated technical contact.

6.3 Each participating organization must have at least one nominated contact subscribed to the ESP mailing lists

To enable access to eduroam service availability updates in real time for the eduroam monitoring service, institutions must create a generic email address "eduroam_ops_contact@inst.domain" so that any service availability alerts can be sent to appropriate contacts under the local control of the participating institution.

6.4 Participating organizations must notify the ESP in a timely manner of the following incidents; (1) security breaches; (2) misuse or abuse; (3) service faults; (4) changes to access controls (e.g. permit or deny of a user or realm) by emailing to the ESP support email address.

7. Authority, Compliance & Sanctions

7.1 The authority for this policy is the ESP who will implement this policy.

7.2 Any changes to this policy will be made in consultation with participating organizations via ASNET-AM.

7.3 Connecting to the ESP authentication servers will be deemed as acceptance of this policy and relevant policies of the ESP. Any organization that is currently connected will be given a period of one month's grace from the official ratification date of this policy by ASNET-AM, to either continue to connect as a statement of acceptance of this policy or the removal of their authentication server connection(s) to indicate an inability to accept this policy at the present time.

7.4 In cases where immediate action is required to protect the integrity and security of the eduroam service, the ESP has the right to suspend the eduroam service or restrict eduroam access to only those participating organizations that can comply with the required changes. To do so, the ESP will notify participating organizations of such incidents, outages and remedial action to be taken on the relevant ESP mailing list.

7.5 The ESP will notify by email to the nominated technical and/or security contact of

the participating organization of any technical or policy breach or incident that requires resolution. Where such notifications are not acted upon in a timely manner, or where the breach or incident may impact on the security and integrity of eduroam, the ESP has the right to block eduroam access to that organization.

7.6 Visited organizations may prevent use of their networks by all users from a particular home organization by configuring their authentication server(s) to reject that realm; in some cases a visited organization may also be able to block a single visiting user.

7.7 Home organizations may withdraw an individual user's ability to use eduroam by configuring their own authentication server or removing that user from their authentication database.

7.8 Home organizations must also ensure that their computing regulations enable users who breach this policy to be subject to an appropriate internal disciplinary process irrespective of their location at the time.

Schedule 1

"ASNET-AM" is the eduroam Service Provider for Armenia.

"ASNET-AM" currently manages the ESP website at www.eduroam.am.

"ASNET-AM" supplies an ESP Support email address at support@eduroam.am.

"ASNET-AM" currently manages the following additional mailing lists

- Eduroam participants list - users@eduroam.am;
- Eduroam technical (e.g. technical contact) and security list - admin@eduroam.am;
- Eduroam official contact – info@eduroam.am

Where eduroam services access the ASNET-AM network infrastructure they will do so in accordance with the ASNET-AM Policy: http://www.asnet.am/aup/