Annex 1 – govroam technical policy

1. Activation procedure

The govroam identity provider authentication server(s) must be reachable from the BELNET RADIUS proxies for authentication and accounting purposes.

The identity provider must create an govroam test account (govroam username and password credential) that will be made accessible to assist in pre-connection testing, ongoing monitoring, support and fault finding activities. If the test account's password is changed, BELNET must be notified by the home organization in a timely manner.

The govroam resource provider may offer any media; however as a minimum, wireless LAN IEEE 802.11b is required whilst 802.11g is also recommended.

The govroam resource provider must deploy the SSID 'govroam' and IEEE 802.1X Extensible Authentication Protocol (EAP) authentication (excluding EAP-MD5) to promote a consistent service and minimum level of security. The SSID govroam should be broadcast.

The govroam resource provider must as a minimum implement IEEE 802.1X and WPA/TKIP, or better. It is strongly recommended that WPA2/AES is implemented.

The govroam resource provider must as a minimum offer:
- Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) egress; UDP/500 (IKE) egress only
- OpenVPN 2.0: UDP/1194
- IPsec NAT-Traversal UDP/4500
- Cisco IPSec VPN over TCP: TCP/10000 egress only
- PPTP VPN: IP protocol 47 (GRE) ingress and egress; TCP/1723 egress
- SSH: TCP/22 egress only
- HTTP: TCP/80 egress only
- HTTPS: TCP/443 egress only
- IMAP2+4: TCP/143 egress only
- IMAP3: TCP/220 egress only
- IMAPS: TCP/993 egress only
- POP: TCP/110 egress only
- POP3S: TCP/995 egress only
- Passive (S)FTP: TCP/21 egress only
- SMTPS: TCP/465 egress only
- SMTP submit with STARTTLS: TCP/587 egress only
- RDP: TCP/3389 egress only

The govroam resource provider should offer:
- Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) ingress
- IPv6 Tunnel Broker service: IP protocol 41 ingress and egress

The govroam resource provider should implement a visitor virtual local area network (VLAN) for govroam-authenticated users that is not to be shared with other network services.

2. Logging

Govroam identity providers must log all authentication and accounting requests; the following information must be recorded:

1. the date and time the authentication request was received
2. the RADIUS request's identifier
3. the authentication result returned by the authentication database
4. the reason given if the authentication was denied or failed.
5. the value of the request's accounting status type.

The govroam identity provider must keep a log of all authentication and accounting requests for a minimum of twelve months and a maximum of twenty-four months. Cooperation about the content of these logs will be restricted to the govroam registered users and BELNET technical contact to assist in resolving specific security or abuse issues that have been reported to BELNET.

The govroam resource provider must log all DHCP transactions including:

1. the date and time of issue of the client's DHCP lease
2. the MAC address of the client
3. the client's allocated IP address.

The govroam resource provider must keep a log of DHCP transactions for a minimum of twelve months and a maximum of twenty-four months. Cooperation about the content of these logs will be restricted to the govroam registered users and BELNET support services to assist in resolving specific security or abuse issues that have been reported to BELNET.

The govroam resource provider must not log any passwords.

3. Govroam user support and guidance

The identity provider must provide support to their users requesting access at an govroam resource provider.

The govroam resource provider should provide support to users from other govroam identity providers that are requesting govroam services at their govroam identity provider campus.

The govroam resource provider must publish local information about govroam services on dedicated web pages on their organization website containing the following minimum information:

1. a text (including an url link) that confirms adherence to this policy (document published on http://www.govroam.be)

2. a hyperlink to a website to govroam resource providers' acceptable use policy or equivalent
3. a list or map showing govroam access coverage areas
4. details of the broadcast or non-broadcast SSID as govroam
5. details of the authentication process and authorized services offered
6. details about the use of a non-transparent application proxy including user configuration guidelines (if applicable)
7. a hyperlink to the website http://www.govroam.be and posting of the govroam logo and trademark statement
8. where user activity is monitored, the govroam resource provider must clearly announce this fact including how this is monitored so as to meet with national legislation, including how long the information will be held for and who has access to it
9. the contact details of the appropriate technical support that is responsible for govroam services.

4. Glossary of acronyms

In the framework of the implementation and execution of the service, the acronyms used will have the following meaning:

AH:	Authentication Header
AUP:	Acceptable Usage Policy
CERT:	Computer Emergency Response Team
DHCP:	Dynamic Host Configuration Protocol
EAP:	Extensible Authentication Protocol
Govroam:	Government Roaming
ESP:	Encapsulating Security Payload
FTP:	File Transfer Protocol
GRE:	Generic Routing Encapsulation
HTTP:	Hypertext Transfer Protocol
HTTPS:	Secured HTTP
IEEE:	Institute of Electrical and Electronics Engineers
IKE:	Internet Key Exchange
IMAP:	Internet Message Access Protocol
IMAPS:	Secured IMAP
IP:	Internet Protocol
IPSec:	IP Secured
LAN:	Local Area Network
MAC:	Media Access Control
MD5:	Message Digest algorithm (version 5)
NAT:	Network Address Translation
POP3:	Post Office Protocol
PPTP:	Point to Point Tunneling Protocol
RADIUS:	Remote Authentication Dial In User Service

RDP:	Remote Desktop Protocol
RFC:	Request For Comments
SMTP:	Simple Mail Transfer Protocol
SMTPS:	Secured SMTP
SSH:	Secured Shell
SSID:	Service Set Identifier
TCP:	Transmission Control Protocol
TERENA:	Trans European Research and Education Networking Association
TKIP:	Temporal Key Integrity Protocol
TLS:	Transport Layer Security
TTLS:	Tunneled TLS
UDP:	User Datagram Protocol
VLAN:	Virtual LAN
VPN:	Virtual Private Network
WEP:	Wired Equivalent Privacy
Wifi:	Wireless Fidelity
WPA:	Wifi Protected Access