Code of Practice

This Code of Practice is a MoSCoW prioritised list of considerations that together constitute a best practice guide for deploying govroam infrastructure. Jisc has developed this code in partnership with an independent third party security specialist to ensure that it offers the very best objective advice to the govroam membership.

Regional Federation Operators (RFOs) are required to complete and return this checklist as part of their boarding process, and are expected to comply with (or at least be working towards) all of the mandatory requirements (MUST/MUST NOT) listed below, and hopefully many of the SHOULD/SHOULD NOT's too.

The quality and consistency of the RADIUS deployment at all participating organisations is a vital part of the overall security model of the govroam service, as a misconfigured server may generate service-disrupting traffic or serve as an attack route against the service or your users. RFOs are strongly recommended to use this document as part of their own process in bringing member organisations into the RADIUS trust fabric of their own regional federations.

Customers must indicate their status at each point, specifying if it's in place, planned, an alternative solution has been implemented or if it is not planned at all. If it is planned, please give an indication of timescales. If an alternative solution is in place, please give details on the alternative solution.

No.	Subject	Control	Detail	In place, planned, other alternative solution, not planned
1	**Network Security**			
1.1	Firewall Placement	A layer 4 firewall which separates the Internet facing Radius server from the Internet and internal network **MUST** be in place.	Network access between external, internal and DMZ assets must all be controlled and monitored to ensure only necessary traffic is permitted.	
1.2	Server and network device administration	Administration **MUST** be performed over a private, internal network.	This prevents external attacks against the administration interfaces.	
1.3	DMZ Connectivity	Connectivity to servers using known risky protocols **MUST** be risk assessed.	Protocols such as SMB and RDP may present security risks and must be heavily locked down or blocked.	
1.4	Radius Network Port Access	The open ports on public interfaces **MUST** be restricted to only those ports required for authentication.	For most instances these will be UDP port 1812, status-server port 18121, and/or TCP port 2083 if RadSec is in use. Radius servers **MUST NOT** be configured to listen on UDP/1645.	
1.5	Radius Network Port Access	The open ports on internal interfaces **MUST** be restricted to	Ideally this will be locked down to RDP (TCP port 3389) or SSH (TCP	

		only ports required for administration functions**.**	port 22). Only permit administration services that are essential.
1.6	RadSec (RADIUS over TCP/TLS)	If Radsec is used, X.509 certificates **MUST** be used to identify RADIUS servers.	More information in "Govroam Technical Specification" Section 2.1.1
1.7	ICMP from govroam	Firewalls **MUST** permit ICMP requests inbound from NRPS and govroam Portal to ORPS, and subsequent replies.	Govroam must be able to ping the organisation's RADIUS servers.
1.8	User Segmentation	Network segmentation **SHOULD** be considered, so that roaming users, once connected, are placed into the correct segment with appropriate access to internal and external resources.	Visiting users should not be automatically attached to the same network as local organisation users; instead they should be connected to a special segment. Connections back to the guest's home network should be handled by their own systems (most likely through a VPN).
1.9	VLAN spoofing	The visitor network fabric **SHOULD** prevent devices from maliciously placing themselves onto unauthorised VLANs	Devices should be prevented from manipulating DHCP or VLAN assignments such that they could move onto unauthorised networks.
1.10	Internet Facing Vulnerability Assessment	Customers **SHOULD** perform a technical vulnerability assessment of Internet-facing estate.	It is important to test what vulnerabilities may be present when exposing the RADIUS server to the Internet.
1.11	Internal DMZ Vulnerability Assessment	Customers **SHOULD** perform a technical vulnerability assessment from inside the DMZ to the internal network if a DMZ is used.	It is important to test what vulnerabilities may be present when exposing the Radius and CA server to the internal network.
1.12	Visitor Traffic Interception	Participants **MUST NOT** deploy interception technology that would provide monitoring of visitor traffic.	Transport Layer Security (TLS) / Secure Sockets Layer (SSL) interception proxies MUST NOT be used against govroam visitors.
1.13	Guest Wi-Fi	In addition to offering a govroam service for roaming visitors, an organisation may also offer a facility for non-govroam 'guest' users. Customers **SHOULD** separate govroam/internal users from such guest users.	Guest Wi-Fi users should be provisioned onto a separate network with appropriate monitoring, control and authentication. Consideration should be given for preventing users operating on the guest network from circumventing organisational security controls.

1.14	Audit trail	Customers **MUST** ensure that they retain the records required in the govroam service definition to ensure that there is a complete audit trail for authentications and associated devices.	Ensuring an audit trail will help to identify any users misusing the network. Such identification may require reconciling logs between Jisc, the home organisation and the visited organisation.
1.15	Credentials	Credentials **SHOULD NOT** be shared between users (or between devices where device authentication is used).	Credentials limited to a per user or device prevents access using stolen credentials. A single user credential may be used across multiple devices that the user controls, or in BYOD scenarios.
2	**Physical Security**		
2.1	Wi-Fi Access Points and Cabling	Wi-Fi Access points and network cabling **SHOULD** be secured as much as possible.	Securing hardware will prevent physical attacks such as the introduction of network taps.
2.2	Servers	All hosts and network equipment **MUST** be located in a secure environment.	Physical access to servers is almost guaranteed to result in compromise and so they must be secured at all times. A locked server cabinet in a locked room, with administrator-only access is ideal.
3	**Server Deployment**		
3.1	Redundant RADIUS Servers	Govroam RADIUS servers **SHOULD** be deployed in a redundant, diverse configuration to minimize the risk of loss of availability.	If a user is not able to connect to their home RADIUS server due to it being offline they will not be able to authenticate and so not be allowed network access. RFOs are required to meet SLAs with Jisc for server availability.
3.2	Dedicated Server	The physical or virtual server used to host the govroam RADIUS function **SHOULD** be dedicated to the task.	Limited functionality on the server reduces the attack surface.
3.3	Server Hardening	All servers used within the govroam architecture **MUST** be hardened to appropriate standards before being deployed.	Either NIST or CIS standards are recommended: **https://nvd.nist.gov/ncp/repository** **https://www.cisecurity.org/** This requirement includes any secondary or backup servers whether they are active online or kept offline until required.
3.4	Patch Management	All server operating systems and applications **MUST** be kept fully	This includes any secondary or backup servers whether they are

		patched and up-to-date.	active online or kept offline until required.
3.5	NTP (Network Time Protocol)	All servers **MUST** be configured with the same time-synched NTP server.	Time synchronisation prevents issues with system compatibility, redundancy and logging.
3.6	Backups	All servers and configuration files **MUST** be regularly backed up.	Backups must be performed as a minimum after every configuration change.
4	**Server Monitoring and logging**		
4.1	Monitoring	Monitoring and alerting **MUST** be enabled to detect attacks such as password brute forcing.	Servers must be configured to detect and log rogue behaviour in both the operating system and the applications. Some automated defence may also be possible (e.g. increasing back-off times between multiple failed password attempts)
4.2	Alerting	Alerts **MUST** be sent to appropriate staff to be acted on. Regular tests should be carried out to ensure alerts are being delivered as expected.	Servers must be configured to send logs and alerts to system administrators in order to detect incidents and attacks in real time.
4.3	Authentication Logging	Logging of all authentication attempts **MUST** be enabled	More information is available in the "Govroam Technical Specification", section 18. Note that authentication logs may contain personally identifiable data, and that storage and processing of this must be handled in a GDPR-compliant fashion.
4.4	Authentication Log Times	All authentication logs **MUST** be time-stamped in UTC (see 3.5).	Govroam requires consistent log formats within the UK time zone.
4.5	Authentication Log Retention	All authentication logs **MUST** be kept for a minimum of 3 months	Govroam requires logs be kept for a minimum of 3 months for auditing purposes. Wider regulatory compliance such as GDPR must be adhered to.
5	**User Education**		
5.1	User education	Users **SHOULD** be trained how a legitimate govroam access point behaves. If they see deviation from that they should know not to connect and who to contact.	If users can be tricked into connecting to fake services then they may reveal sensitive information. Any training which will help prevent this is encouraged. Instructional posters are a useful aid.

5.2	Govroam User Expectations	Organisations **MUST** educate their users to know how the govroam service should behave.	A govroam user should be prepared e.g. not to click ignore when warned of certificate mismatches, not to enter their govroam credentials into web forms etc.
5.3	Govroam Visitor Expectations	Organisations **MUST** minimize any possibility of confusion between the govroam service and any other guest facility they offer.	Visited organisations must ensure that is not possible for a non-govroam service to be mistaken by visitors for the participant's govroam service.
5.4	Govroam Service Information	Participants **MUST** publish a govroam service information website.	Such websites must be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily on site. More information available in "Govroam Tech Spec" document.
5.5	Security contact	Users **MUST** have an obvious point of contact at their home organization in case of account compromise or loss/theft of devices.	The point of contact must be able to disable accounts and/or to revoke client-side certificates if applicable.
5.6	Support contact	Organisations **MUST** ensure there's an advertised support infrastructure both for their own users when roaming, and for second line support requests originating from visited organisations or Jisc.	The point of contact must be able reset/disable accounts and assist Jisc/other organisations to identify and fix issues arising.
6	**Certificate Authority (CA)**		
6.1	Public vs Private Certificates	Organisations **MUST** undertake a risk based selection of Private vs Public Certificate Authorities. Private is usually preferable and most commonly used.	Pros and cons exist with the use of both private and public certificate authorities. Private CAs carry less chance of security issues. Only consider public CAs if every client will always be auto-configured by the CAT. Make a risk based decision to choose which is best for your organisation.
6.2	CA Server Location	CA server **MUST** be on a dedicated, locked down server with minimal user access	Compromise of a certificate authority would give an attacker the ability to set up a fake server to trap users. Revocation of the CA and issuing of new certificates is

			also likely to be a hard and expensive operation.
6.3	Certificate Server Name	The server name **SHOULD** be a fully qualified domain name (FQDN).	Some end-user device operating systems might (incorrectly) require the name to be parseable as a hostname; so it is a good idea to use a server name which parses as a fully-qualified domain name - the corresponding record does not have to exist in DNS though. The server name should then be both in certificate's Subject field (Common Name component) and be a subjectAltName:DNS as well.
7	**RADIUS Server Configuration**		
7.1	Shared Secret	The shared secret between clients and the RADIUS server **MUST** have sufficient entropy.	A password of at least 16 characters is required, including upper and lower alpha characters and numbers.
7.2	Do Not Reuse Secrets	Each Access Point <-> RADIUS server relationship **MUST** have a unique secret.	This limits the scope in case of compromise.
7.3	Disable PAP	Password Authentication Protocol (PAP) between Access Points and the RADIUS server **MUST NOT** be used.	If there are any proxies between the Access Point and the end server, each proxy must decrypt the PAP password and then reencrypt it with the key for the next hop. This leaves the system vulnerable to password sniffing if a proxy is compromised.
7.4	Disable SPAP	Customers **MUST** disable the Shiva Password Authentication Protocol.	SPAP passwords are sent in a reversibly encrypted format making the protocol weak and open to interception. **https://technet.microsoft.com/en-us/library/dd197599(v=ws.10).aspx**
7.5	Disable MS-CHAP	Customers **MUST** disable Challenge Handshake Authentication Protocol (CHAP).	MS-CHAP (version 1) is considered a weak protocol and must not be used.
7.6	Enable the Message-Authenticator attribute	The Message-Authenticator attribute **MUST** be enabled (where supported).	The Message Authenticator helps to prevent fake message injection through IP spoofing. **http://www.networksorcery.com/enp/rfc/rfc3579.txt**

			https://technet.microsoft.com/en-us/library/cc753271(v=ws.10).aspx
7.7	Encrypt Communications	Customers **SHOULD** use a VPN to protect communications between Access Points and the RADIUS server.	For more information see: **https://technet.microsoft.com/en-us/library/cc725908(v=ws.10).aspx**
7.8	EAP Types	Customers **SHOULD** use at least one of the following EAP types: • TLS • TTLS • EAP-FAST • PEAP	Information about EAP types: **https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol**
7.9	Anonymous Outer Identities	Where supported by the EAP type and supplicants, anonymous outer identities **SHOULD** be enabled.	As not all supplicants support this it cannot be mandated however to add anonymity to the connection this is highly recommended. **https://wiki.geant.org/display/H2eduroam/eap-types**
7.10	Enable Chargeable User Identity	Chargeable User Identity (CUI) **SHOULD** be implemented to ensure users can be traced through the system for accountability purposes.	Enabling this from the outset will greatly enhance accountability which may help with adoption and troubleshooting, especially during early stages of the roll out. CUI use is highly recommended.
7.11	RADIUS Accounting	Radius accounting messages **MUST NOT** be forwarded to the govroam National RADIUS Proxy Servers (NRPS).	The govroam National RADIUS Proxy Servers (NRPS) do not require visibility of the potentially sensitive information stored within RADIUS accounting messages.
7.12	VLAN Attributes	Dynamic VLAN attributes **SHOULD NOT** be sent in Access-Accept replies to NRPS	Where an authentication request is received from the NRPS, as opposed to being received from an internal RADIUS client or NAS, a Home organisation's Access-Accept reply should not contain dynamic VLAN assignment attributes, unless a mutual agreement is in place with the Visited organization concerned. This may be achieved by the Home organisation filtering out dynamic VLAN assignment attributes if present in Access-Accept packets sent to the NRPS.

7.13	Specify the Operator-Name	Organisations **SHOULD** configure their ORPS to insert the Operator-Name attribute, accurately composed for their realm, into all Access-Request packets forwarded to a RRPS or NRPS.	Configuring an ORPS to add Operator-Name, with a value set to the domain of the local site, means that all proxies in the chain can easily identify the source of the request. This could be invaluable for audit and security.
8	**Device Configuration**		
8.1	Automated Configuration	Wherever possible, the govroam "Configuration Assistant Tool" (CAT) **SHOULD** be used to assist with client deployments.	See **https://cat.govroam.uk/** The CAT tool eliminates the risk of accidental misconfiguration and ensures consistent set up across your userbase.
8.2	Manual (non-CAT) configuration	When CAT is not used, the deployment of configuration details to the users **SHOULD** be done in a prescribed and secure way.	Deployment should be performed by an administrator (not the end user) using a trusted management network. Non-CAT deployments are not recommended.
8.3	Certificate revocation	If an EAP type which uses client side certificates is used (e.g. EAP-TLS), a revocation process **SHOULD** be put in place.	This will cover devices which are lost, stolen or compromised.
8.4	Deployment Speed	Govroam clients **SHOULD** be deployed within a short window of time.	When deploying govroam to a user base, e.g. with govroam CAT, any unenrolled users may attempt to self-enroll through manual configuration. Self-enrolment is not advisable. A quick roll out of govroam to all users should prevent users trying to self enroll.
9	**WI-FI Access Points**		
9.1	WPA2-CCMP (AES)	Govroam Visited Wi-Fi services **MUST** implement WPA2 Enterprise with the use of the CCMP (AES) algorithm.	More information in "Govroam Technical Specification" Section 4.10
9.2	WPA-TKIP	The WPA specification **MUST NOT** be supported and the TKIP algorithm **MUST NOT** be employed in govroam services.	More information in "Govroam Technical Specification" Section 4.10
9.3	Rogue AP detection	Customers **SHOULD** monitor for rogue access points.	A rogue wireless access point is an unauthorised access point that has been installed on the network. Attackers will use rogue access points to trick users into exposing their data and credentials. Tools

			and processes should be implemented to actively monitor the Wi-Fi network for rogue devices to ensure these are removed.
9.4	Wireless IPS	Customers **SHOULD** implement Wi-Fi Intrusion Prevention Systems	Wi-Fi Intrusion Prevention Systems can detect more advanced attack techniques such as AP spoofing, malicious broadcasts, and packet floods.
9.5	Use of "govroam" SSID	Customer **MUST** only use the "govroam" SSID for compliant networks	Other Wi-Fi networks that do not utilise govroam or comply with its standards must not be named "govroam" or by a name that could potentially be confused or associated with govroam.
9.6	Dedicated use of "govroam" SSID	The "govroam" SSID network **MUST NOT** be shared with any other network	The "govroam" SSID network must be exclusive to providing govroam services.
9.7	Wi-Fi services on non-IEEE 802.11 protocols.	Wi-Fi services **MUST** only be provided on IEEE 802.11	Other wireless technologies such as Bluetooth are not permitted.
10	**Ports and Protocols**		
10.1	Default deny policy	Providers **SHOULD** operate all firewalls and access control lists against a default deny policy, only allowing specific traffic types that are required to pass.	It is better to consciously grant access to useful traffic than to reactively attempt to block traffic that you find is causing a problem.
10.2	Govroam network access control	Providers **MUST** allow roaming govroam users access to the minimum standard ports and protocols specified in the govroam tech spec.	User need to be able to predict what services (email, web, VPN) will work over govroam when they arrive at a new venue.