

## Summary of site setup recommendations

In this section we list security-related issues to consider when deploying an H.323 service, in particular when joining the JANET H.323 service, using a studio system on the local campus.

### Using Janet Videoconferencing

In the context of Janet Videoconferencing, that service will be responsible for:

- MCU set-up at the JANET C-PoPs;
- gatekeeper set-up at the JANET C-PoPs;
- monitoring and security checks of the publicly accessible C-PoP H.323 devices;
- informing users of the booking system of the importance of the privacy of any booking information the users see (having logged into the booking system);
- resilience to DoS attacks on the C-PoP-hosted H.323 components.

Responsibilities for sites connecting to the service include:

- set-up, configuration and security checks of any site gatekeeper used;
- set-up, configuration and security checks of any site proxy and/or firewall;
- security of the site H.323 videoconferencing studio;
- deployment of switched Ethernet paths to the studio and for network management;
- physical security of the H.323 terminal;
- lockdown of configuration options for the H.323 terminal;
- ensuring any site gatekeeper is manually configured, not using multicast discovery;
- liaising with the Regional Networks for QoS provision where required.

Further site-specific issues are described in [Appendix A](#) <sup>[1]</sup>.

The JANET Videoconferencing Management Centre is responsible for performing site (studio) tests for quality assurance.

### Risk assessment

The following table shows some recommendations and suggested risk assessment considerations. This is not an exhaustive list; sites should perform their own assessment exercises.

Threat	Likelihood	Impact	Countermeasures
--------	------------	--------	-----------------

Theft of system	Low	High	Physical security CCTV.
Unauthorised use of system.	Low	Low	Security code dedicated passwords
Unauthorised monitoring of an H.323 session.	Low	Variable, depending on nature of conference.	Use of encryption e.g. H.235,  Use of switch  Do not publish sessions.
Unauthorised joining of an H.323 session.	Low	Variable, depending on nature of conference.	Controls at gatekeeper  Do not publish sessions.
Network adapter/cable problems causing poor performance.	High	High	Test physical  Check duplex settings.
Gatekeeper ceases to function through hardware or failure.	Low	High	Offer redundant devices to of failure point
User at client terminal is an impostor.	Very Low	Variable.	Unlikely to the person recognisable threat is very

*Figure 7: H.323 risk assessment threats*

**Source URL:** <https://community-stg.jisc.ac.uk/library/janet-services-documentation/summary-site-setup-recommendations>

#### Links

[1] <http://community.ja.net/library/janet-services-documentation/appendix-deployment-security-checklist>