the professional recording association

STUDIO SECURITY Draft Guidelines - 2004

There are concerns within the recording industry regarding the security of recordings during the production process. The APRS suggests studios could consider their security by reference to the guidelines, in the form of the checklist below, as a response to those concerns.

A studio using this checklist to conduct an audit of their security arrangements can assess how well it ranks by allocating values between 0 and 3 (0 for "no provision", 1 for "some provision", 2 for "adequate provision", 3 for "good provision") in each section below.

Recording studios need to be able to show that they have taken reasonable steps to protect the security of copyright works from unauthorised copying, and to protect finished or unfinished physical recordings - whether made at the studios or brought in for further work - also from loss, damage or theft. However, even a maximum score cannot guarantee the studio freedom from claims.

Clients may in any case request other security measures to be adopted. The APRS hopes that studios will find this checklist useful and that insurers will recognise that a high score along these lines would assist studios in negotiating premiums for cover against these risks.

Pre-release Security - Preliminary Checklist (Version 4 - 27/4/04)

		Score 0, 1, 2, or 3
Security Policy	All commercially trading recording studios should have a security policy. The terms of a studio's security policy should be acknowledged in the contract between the client and the studio.	
Physical Security		
Access Doors	Unlocked, exterior main doors to studio reception areas should be attended at all times during "working" hours by an experienced responsible person. Studio Access doors should be lockable from the inside. Dark access points should be well lit - possibly by infra-red sensitive floodlights. Recordable CCTV is recommended for secluded entrances.	
Deliveries	Systems should be in place which specify where goods, materials and hire equipment are to be received that include provision for retention of signed delivery notes.	
Collections	Records should be kept of all collections of materials (such as tapes, cds and DVDs,) made from studio premises including item, date, time and signature.	
Recording rooms & Control Rooms	Access should be restricted to authorised studio personnel and named individuals listed by client. Ideally, studios and control rooms should be locked whenever the session team leaves them empty or if they are vacant or not in use.	
Client materials	Materials - working multi-tracks, hard drives CD Roms etc - should not be left in control rooms overnight by should be secured in a lockable safe place.	
Tapes/Hard disks Log	Systems should be in place to provide for all materials to be logged in and out of studio buildings so that there is a verifiable "audit trail" for media movements.	
Data Security		
Web and Email Access	Studio internet connections must be fire-walled utilising 'email gateway' software that filters out viruses and large media attachments. Client email/internet access ports should be regularly vetted for rogue software. Notices warning of the illegality of copyright infringement should be displayed prominently. Any computer that connects to the internet either directly or via a shared network must have an up to date virus scanner. Staff should be reminded that production software is also subject to copyright protection.	
Secure File Transfer	External digital file movements should always be via secure transfer network service providers or closed secure 'extranet' systems. The APRS can provide information on recommended suppliers. Internal file transfers should be logged.	
Hired-in DAWs	Hired DAWs should be checked for previous session data and anything found should be deleted. Internal hard disk data should be erased before collection by hire companies.	
Computers	No desktop or lap-top computer should have any P2P sharing programs installed (KaZaa, Bearshare etc). Notices forbidding client use of portable download devices (Laptops, PDAs, mobile phones etc.) should be prominently displayed. Individual computer access should be subject to non-predictable and regularly changed password controls	
WI-FI	If there is access to a wireless network connection, the connection should have been set up to use access control lists and WEP encryption.	

APRS
the professional recording association

STUDIO SECURITY
Draft Guidelines (4)- 2004

Blank Media

Any media created during a session should be identifiable and logged into a tape/disk logging system. This can be a simple paper based system or a software database solution. Consideration should be given to watermarking all blank media at the point of burning/recording (EXCEPT MASTER MEDIA*) to provide an evidential audit trail and a promotable deterrent against careless copying.

New blank media coming into the studio from outside should be logged and marked with indelible marker and, if possible, watermarked at the point of burning, as should any media leaving the studio.

*Watermarking is not recommended for any media that is used for the fixation of master recordings as interference with the purity of the audio signal may compromise the fidelity of the recording.

Transportation

Couriers

The studio should use an approved courier or carriage company for all media deliveries. Courier companies should be fully appraised of the security issues surrounding media transfers and their responsibilities confirmed in a legally binding agreement. Individual couriers, drivers and riders should carry photo ID.

Media Transfers

All media should be logged at the point of leaving the studio so that responsibility for its security and integrity until its acceptance at its destination lies clearly with the carrying company by virtue of the signature of an identified employee of that company.

Media Transfer logs

Verifiable details of the identity of the courier and those of the person designated to receive the media at its destination should be recorded in a delivery note, a copy of which is retained by both the consignee and the recipient.at the receiving end.

Media Packaging

Media should be sealed with anti tamper labels to prevent unauthorised copying while in transit.

Media Integrity

All media, including work in progress, when transported by a cab or courier, should be appropriately packaged,preferably boxed and labelled showing the details of the destination and the name of the recipient. The APRS recommends the use of couriers that offer security transportation services wherever possible but acknowledges that such services may not be available in some geographical areas. An experienced member of studio staff should supervise the loading of the media into the vehicle ensuring that there are no magnetic sources in the vehicle within the proximity of the media being transferred that could damage the material.
(eg: Sub woofers in the boot)

Personnel

Terms of employment

Studios should retain employees under a contract of employment that includes an undertaking by employees to respect the integrity of copyright works including the works of company clients and protected software that may be used as a part of their employment on or off the premises.

Awareness

Studios should ensure that their employees receive thorough training so that they are fully aware of the need for studio security and of the particular systems employed in-house.

Notices

Studios should consider displaying notices prominently that convey to employees, clients and visitors the value of copyright material and the importance of maintaining a secure studio environment.

Artists and Visitors

Clients must be made aware that the behaviour of artists or visitors introduced to the studio premises by them may jeopardise the security of the recording/session and that any subsequent breach of security is entirely the responsibility of the client.

Comments and Scoring Guidelines

These guidelines are only for guidance of, and consultation between, APRS members and APRS cannot accept responsibility for liabilities which studios, whether or not APRS members, may have in any aspect of their own businesses. Particular security policies or measures mentioned in these Guidelines are for consultation only and APRS also cannot accept responsibility for the consequences of any particular studio adopting any measure suggested in these Guidelines: studios and those who run them must make their own best business judgment. Although these Guidelines do not comprise an actual or proposed Code of Conduct, APRS members are invited to contact <info@aprs.co.uk> or Peter Filleul on 020 8699 1245 with comments.

As a rule of thumb, scores between 1-25 should be regarded as disappointing, 26-45 barely adequate, 46 - 66 as optimistic.