

# Security

## Overview

At PIX, keeping your material safe is our first priority. Our methods for protecting your media far exceed those of current filmmaking practices. There are no DVDs or VHS tapes, no FTP sites, and no Emails. Access can be restricted to specific computers, media can be watermarked, administrators can monitor all viewing and movement of material, and errant users can be locked out of the system at any time.

In 2005, PIX underwent a security review by Paramount Pictures, which included analysis by Paramount's parent company, Viacom. Viacom's CTO and his staff were satisfied with the security system and procedures and approved the use of PIX at Paramount. In addition to regular internal audits, PIX employs Neohapsis, a respected security organization, to audit its security infrastructure.

To date, the PIX security system has protected films for Paramount, Warner Bros., Universal, DreamWorks, Disney, New Line, Spyglass, and MGM.

## PIX System's Security Features Include:

- All connections to and from the PIX System data center are secured using 128-bit Secured Sockets Layer (SSL) encryption, the de-facto security standard in use today. If supported on the client-side, we automatically use 256-bit SSL.
- Each file/clip is individually encrypted with AES-128 encryption. No keys are stored and PIX personnel do not need access to any file keys. With our upload application, files are fully encrypted on the client-side before leaving the user's computer.
- All images and video clips viewed from PIX can be marked with both a project watermark (e.g. "Property of Paramount Pictures") and a user-specific watermark specifying who accessed the image and when (e.g. "J. Doe 01\_18\_07"). Different real-time watermark settings can be specified per user or group.
- Clients may restrict project access for an individual to a specific IP address.
- All file downloads and transfers are logged. Both PIX and the client are able to monitor usage and activity logs, bringing human oversight to the security process.
- PIX uses a multi-tiered intrusion detection and prevention system. All connections are logged and monitored.
- Strong, secure user authentication controls access to every element of the system (per each request).
- PIX personnel do not have access to and do not store user passwords or security codes.
- PIX provides a true cross-platform media solution (Mac/Windows). We also offer a complete integrated DRM solution, developed in-house, and based on peer-reviewed, industry standard encryption algorithms. Our DRM solution is available via a simple QuickTime plug-in, encrypts media at the sample level, and is transparent to properly authorized users.
- PIX uses encrypted remote servers to enhance streamed delivery. These remote servers have been deployed internationally as well as at Paramount and several LA facilities with great success.
- The main PIX application cluster and storage servers are located in a highly secured tier-1 data facility. Entry and movement within this facility are fully controlled and monitored, including two levels of access verification and 24/7/365 security monitoring.
- PIX can immediately disable a user's access to the service, or the entire Project, if authorized by the client. Users are automatically locked out if an incorrect username/password combination is entered multiple times.