Security Policies and Procedures

The great strength of the Internet-the fact that it can connect people all over the world to data stored in remote servers-is also one of its weaknesses; it is difficult to prevent people from accessing data that is intended to be secure and/or private. Concerns about data integrity, authenticity, and security are not unique to image management but are common to the management of all types of networked information resources. A digital image collection should be built within a framework of institutional security policies and procedures that address all aspects of the creation, modification, manipulation, access, and use of data. For instance, the original state of files should be documented to provide benchmark values or checksums that can be inspected to verify that data has not been altered or become corrupted. Such guidelines will protect the investment in the creation of both images and metadata and guarantee the usefulness of the collection as a future resource. (See *Long-Term Management and Preservation.*)

There are several, not mutually exclusive, strategies that can be used to ensure the security and integrity of digital information. The most common security model employed by cultural heritage institutions is for access to archival master files to be limited, and for lower-quality derivative access files, delivered with a clear copyright statement, to be made generally available over the World Wide Web. Watermarks, formed by switching particular bits in a digital image, can "brand" image files and enable an image rights holder to verify the source of a digital image and seek legal recourse if it is misused or if access restrictions are violated. It is also possible to make it difficult for users to download images from the Web by, for instance, requiring users to download **plug-ins** that control printing and downloading options before allowing them to view an image.

It is possible to build systems that are designed to enforce legal restrictions—ones that can, for example, track the frequency of use of each image, make users sign in, or require them to acknowledge restrictions on use. However, such systems may be too onerous for the available level of technical support and perhaps too restrictive where the institutional mission is to provide broad public access to collections. Where it is necessary to restrict access, firewalls, **DMZ**s (demilitarized zones), access control lists (**ACL**s), and **directory** services can stand at the gateway of secure networks and control admission, perhaps allowing access only to those users visiting from certain **domain names** or **IP addresses**. By implementing features such as **passwords**, **digital signatures**, or **digital certificates**, authentication may be used to ensure that potential users are indeed who they claim to be, and specific types of users may be limited to viewing certain images under particular conditions or have their ability to alter or delete information restricted. One scenario might be that staff is granted editorial access to administrative metadata and master images; that internal users are granted read-only access to descriptive metadata and high-resolution derivative images; and that external users, limited by bandwidth and legal considerations, are granted access to the same descriptive metadata but lower-resolution images. Digital rights management (**DRM**) server software may use various techniques to protect and control distribution of commercial content offered over the Web.

Security strategies can complicate the management and preservation of digital image collections and should only be instituted where they are realistically necessary. Be wary of technological "magic bullets" claiming to solve security problems. Advances in security technology may be taken as a challenge by **hackers**, although most digital image collections are probably less at risk from malicious unauthorized access than accidental deletion or manipulation. (Note that a common security mistake is for network administrators to forget to change the default password of security software.) Some security strategies, such as **public-key encryption** and digital certification, merely transfer risk to a third party and can only be as robust as that third party is trustworthy, competent, or prescient.