LYRASIS

Preservation Services Leaflet

1438 West Peachtree Street, Suite 200/Atlanta, GA 30309
Phone: 404-892-0943/Fax: 404-892-7879
Website: <www.lyrasis.org>

Security Audit

The security audit on the following five pages is designed to identify and assess an institution's vulnerabilities in relation to security. Through periodic audits, staff can reduce security risks and better protect people, property, and collections. Information can be gathered in regular tours of your building(s) and through conversations with others in the organization.

The information can be used in two ways. First, the audit may reveal areas of vulnerability that can be remedied through changes to current policies and procedures. Second, staff may identify liabilities related to the physical space and structure of the building(s). Some of these problems might be corrected easily; others may require long-term planning to reduce the area of vulnerability. As you fill out the security audit, answer yes/no where appropriate. Add notes indicating the specific problem areas and potential solutions to reduce the risk. Update the audit when actions are completed that address problems.

In actual use, an institution may create its own audit checklist based on the frequency with which each item needs to be checked. Some areas will need attention only once or every few years (e.g., identifying potential blind spots). Others may merit more frequent auditing, such as examining frequency of security controls or currency of virus protection software. Although the areas listed may fall under the responsibility of different personnel, one individual should maintain the audit and track progress in improving security (such as an administrator responsible for the building's security or the chair of a security committee).

Building Name _____
Date of Audit _____

Part 1. The Building	Yes/No	Notes/Action Required
Does building design create blind spots inside the building?		
Outside the building?		
Is indoor lighting adequate during open hours?		
During closed hours?		
Is outdoor lighting adequate during open hours?		
During closed hours?		

(Continued) Part 1.	Yes/No	Notes/Action Required
Is access adequately controlled? (Explain how in notes section)		
Do staff patrol open stacks? How often?		
Is access to storage areas limited? Who has access?		
Is access to Special Collections stacks limited? To whom?		
Are security features (security cameras, mirrors, etc.) employed?		
Are other theft detection systems used? If so, describe type of system.		
Are there operational difficulties with the theft detection system?		
Are opening and closing procedures written down?		
Does staff always follow such closing procedures?		
Are all areas checked to ensure no one is left in the building?		
Is there a fire suppression system?		
Is there a water detection system?		
Are alarms connected to outside system?		

Part 2.
The Collections

Are all materials marked? How?		
Are marks visible?		
Are inventories regularly conducted?		
For circulating collections?		
For non-circulating collections?		

(Continued) Part 2.	Yes/No	Notes/Action Required
Are all materials tagged with anti-theft devices (tattletape, RFID tags, etc.)?		
Are items secure in transit (e.g. between branch/main libraries, materials on loan)?		
Are exhibit areas guarded?		
Are there locks/alarms on exhibit cases?		
Are non-circulating collections loaned?		
Under what conditions?		
Is there a procedure in place to determine damage after loans?		
Are staff assigned to Special Collections reading room at all times?		
Are bags allowed in Special Collections reading rooms?		
Do people have to log into computers?		
Are networks and servers located in staff only areas? How is access controlled?		
Is electronic equipment surge protected?		
Is data backed up? How? How often?		
Is virus-protection software current?		

Part 3.
The People

Is identification required to enter building?		
Is identification required to use materials?		
Is there a policy for excluding individuals?		
If so, it is enforced?		
Is patron privacy protected? How?		
Are users and their bags inspected when leaving Special Collections areas?		

(Continued) Part 3.	Yes/No	Notes/Action Required
Are staff references checked? How closely?		
Is staff given security training?		
Is security training adequate?		
Does institution have security staff?		
Does staff have identification visible to users? Do they use it?		
Is staff and/or their bags searched when they leave the building?		
Is institution insured against theft from staff and others?		
Does institution compile crime statistics?		
Are crimes (theft, assault, etc.) reported internally?		
Are crimes reported externally?		
Are theft prevention policies and procedures in place?		
Have specific theft prevention procedures been implemented? What types? (RFID, security cameras, visual inspection by library/security staff, etc.)		
Does institution publicize penalties for theft?		

Part 4.
Other Security Issues

Is the cash in vending machines secure? How?		
Is the cash in copy machines secure? How?		
Are cash drawers secured? How?		
Do you have a safe in the building? Who has access?		

(Continued) Part 4.	Yes/No	Notes/Action Required
Does institution have a disaster plan?		
Is disaster plan up-to-date?		
Does institution have disaster insurance?		
Does it cover all types of disasters?		
Does staff know how to contact appropriate authorities?		
Have past security issues been addressed?		
Does institution have other security concerns that need to be addressed? What are they?		