

Sample Building Access Policies and Procedures

How to use this document

All of us want our buildings to convey the message that we are welcoming institutions. At the same time, our stakeholders want to feel secure.

Developing a sound access control policy helps to achieve a difficult balance. By developing clear access policies and procedures both your staff and stakeholders know what is expected of them. Incorporating simple and inexpensive measures will protect your organization, your people, your reputation and your assets.

This document suggests sample policies and procedures for a multiuse building. No template is perfect for every situation. Each building has a wide variety of operations and layouts as well as their own specific hazards. Use this document as a base for your organization's discussions about security policies and procedures, customizing it as needed to your organization and facility. Recognize that not all elements suggested here will be appropriate for your facility.

Consider professional security consultation to develop complete and effective access control, security and emergency plans.

Because your Access Policy and Procedures are so important they should be approved by your Board of Directors. The discussion and "sign-off" help to build consensus and send a significant signal to your employees and stakeholders that the organization will take the implementation seriously.

INTRODUCTION

<NAME OF ORGANIZATION> strives to achieve a difficult balance-both as a warm, friendly, and welcoming environment and, at the same time, one that is safe and secure for all who use our building. This document will detail the policies and procedures that will be used to protect our organization, facility, people, and assets by controlling what enters and leaves the building.

Comment: When developing policies and procedures it's important to know what your goals are. Security policies are only effective when they are supported by your leadership. The security-related mission of your organization should be discussed and approved by your Board of Directors.

© 2009 Jewish Community Relations Council of New York

This publication is not in the public domain. These materials are licensed for the exclusive informational use by New York nonprofits and are expressly not for commercial use by consultants or vendors. Licensees shall not modify, publish, transmit, transfer, sell, create derivative works from, display or in any way exploit any of the contents, in whole or in part, except as otherwise expressly permitted.

This publication is not intended to provide comprehensive, institution-specific advice on any aspect of security or emergency planning nor is it meant to replace the advice of a professional in the appropriate field (e.g., emergency planning, law, building safety). Some of the topics discussed in this publication are subject to federal, state/provincial and/or local codes and regulations. This publication does not provide a universal guide for regulatory compliance. The material is being provided for educational and informational purposes only, without representation, guarantee or warranty of any kind, and it should not be construed as professional advice. Neither the authors nor JCRC-NY are responsible for any injury, loss or damages to persons or property arising from the use or misuse of this information.

Comments, questions and suggestions are welcome. Send them to info@jrcny.org.

For your policy to be completely effective, you must also involve everyone within your organization to promote adherence and assistance.

Threat-based policies

The policies established in this document are consistent with what has been determined to be realistic and possible threats that pose a risk for our organization. However, while certain activities such as thefts, property damage, or unauthorized entry are always possible, we must be aware for times when we need to raise our security levels. Increased levels of neighborhood crime or terrorist activity will make it necessary to make changes in the policies that will be addressed in this document. <DESIGNATED PERSON> will monitor news sources and communications from <TRUSTED SOURCES> regarding when to implement increased vigilance and heightened security operations.

Comment: Develop, at the minimum, two different levels of security: normal and high. The normal level will represent your regular security procedures.

The high level will detail how increased vigilance and heightened security operations will be implemented. Some suggestions for a higher level of security can include an immediate and continuing inspection of the premises and grounds, specifically of all access and egress points, bag and body searches, increased premises surveillance, increased attention to mail and packages or other steps as necessary.

BUILDING ACCESS

<DESIGNATED ENTRANCE/S> will be the only point/s to enter and exit the building during normal operations. A front desk/screening area, staffed by <DESIGNATED SCREENER>, is positioned to provide an unimpeded view of the front entrance and all building entrants must pass by this area. The screener will have the responsibility for screening and granting access to all building entrants. Anyone entering the building should immediately feel that this staff is both welcoming and professional. The buildings bathrooms, service spaces, stairwells, or other amenities will not be accessible without passing this front desk/screening area.

All other doors will only be used for emergency exits and are alarmed at all times. Routine inspections by <APPOINTEE> will ensure that the alarms are functioning, that the routes to the emergency exits are clearly marked and unblocked, and that exterior doors are not propped open for any reason which may allow outsiders access into the building.

Comment: If a door is not under physical or electronic surveillance it should be locked (even if some people have to walk around to another door in the building). Consider alarming lower level windows and adding extra protection such as security bars and/or camera surveillance. Make sure building design and landscape elements do not support easy access to windows, loading docks, air intakes, or any other access points of the building (e.g. a tree that enables someone to climb into a window). Air intakes should be relocated to a higher level or fitted with appropriate designs that would make them harder to be breached. Make sure rooftops are secure and consider alarming and monitoring rooftops.

Authorized Individuals

Official staff and clients (regular and well known customers, congregants, and constituents) shall be admitted to the building without additional screening. All employees must undergo a background check before employment.

Comment: Your plans should address what establishes someone as an "official" client. Based on your facility's needs and usage, consider more secure measures such as using ID cards and/or other electronic access control methods for anyone entering the building or grounds.

Guest Policy

Any building occupant expecting a guest must notify the front desk and provide the guest's information before the guest's arrival via an "Expected Visitor Form." The screener should be trained to greet visitors and to ask appropriate questions about the visitor's destination in a courteous and professional manner. The screener will contact the staff person being visited to verify that the guest is welcome and expected before permitting the guest access to the premises. In some instances, such as <SPECIFY>, the staff person expecting the guest must come to escort the guest into and out of the premises. Before being permitted access to the premises all guests must present a valid ID and must sign-in into the log book. The log book requires the person's name written by the screener, the time of arrival, who they are visiting, and the guest's signature. The guest must sign out with the front desk when leaving.

Comments: Based on your needs you may want to add more elements to your log book, such as recording the guest's license number or contact information. Having the guest sign out enables you to know who is still in the building if this information is needed. You may also want to consider additional security measures such as a buzzer and camera system that the guest must use before proceeding to the front desk/sign-in area. A buzzer and camera system will immensely improve the security capabilities of your facility by not allowing any questionable visitor to gain access to the building without being first recognized and/or screened before entering.

Random Searches

During holidays, special events, times of expected increase in guest traffic, or during times of heightened security levels, the front desk staff/ screeners will be provided with a "clicker" to select every "nth" visitor for a bag search. A wand search may be carried out when applicable.

Vendors and Service Personnel

All vendor or service companies must provide verification that their employees undergo background checks. Front desk staff/screeners must have a list of all contracted vendors and service personnel on hand and will require proper business-specific identification from the visiting personnel. The front desk staff should be made aware of expected vendor or service visits via the "Expected Visitor Form." Any service personnel who must be permitted access to the premises must sign in and out with the visitor log book.

Master Key Control System

<APPOINTEE> is responsible for monitoring the distribution of keys and duplicates. Only authorized employees will have keys that offer access to specified areas of the building. Accordingly, staff will only obtain keys that are relevant to their position (e.g. teachers do not need keys for mechanical rooms). All keys are made with non-duplicative features. Anyone receiving keys will sign out the key/s upon receipt. When someone completes their employment with the company, they must return the key/s.

The distribution of master keys should be as limited as possible. Master keys must be readily available for emergency personnel.

EMPLOYEE AWARENESS & TRAINING

For our policies to provide effective security, all building occupants must recognize the importance of following and adhering to the developed security procedures. All staff will be informed of policies through <SPECIFY MEANS SUCH AS TRAINING, ORIENTATION, ETC> and will be trained to recognize strangers and report suspicious activity.

OTHER POSSIBLE ADDITIONS TO YOUR POLICY

Synagogues

<YOUR ORGANIZATION> is, first and foremost, a house of Jewish prayer. People coming to attend services should be able to do so without being greatly inconvenienced for security measures. The <SECURITY/FRONT DESK STAFF> should be familiar with most of the regular worshippers, whether at daily, Shabbat, or Holiday services. Unknowns should be stopped and screened, including through carrying out bag inspections and/or metal detector screenings, as deemed necessary and appropriate. A recent membership and donor list will be available for the security staff to aid in the screening. The security policy for funeral services and member simchas should be the same as for other services.

High Holidays

The potential of threat increases during the High Holidays. Those receiving tickets for services should be pre-screened by the office staff. There is an obvious hierarchy to those attending High Holiday Services: long-term members, long-term casuals (who regularly attend only on the holidays) and new casuals. New casual attendees require the greatest scrutiny. When a new casual attendee calls to purchase tickets their identity should be confirmed (e.g. phone book listing, valid driver's license, references, or similar methods). Special scrutiny should be made of anyone who insists on paying in cash. Provisions should be made to secure the tickets to maintain its legitimacy, i.e., not easily duplicated by using a scanner or color printer. The <PERSONS RESPONSIBLE FOR SECURITY> should check tickets and inspect bags of those entering the synagogue. Those without tickets must receive increased scrutiny.

Schools

Students are to be provided access in the same manner as authorized staff and employees are provided access. Parents and caregivers wishing to enter the building will be treated the same as a regular visitor. All parents who employ caregivers or who have someone other than the regular arrangement picking up their child must notify <PERSON TO NOTIFY>. The child will not be allowed to leave without appropriate arrangements made with the school. Inform custodial parents that it is their responsibility to specify authorized people for pickups and for notifying the school of any changes in authorization status.

Special attention must be made for situations where children are outside the building, e.g. on the playground or a trip, since individuals from the outside can approach the children easily. On duty staff must be alert for such occurrences.

OTHER THINGS TO CONSIDER

This document is not all inclusive. There are many other functions and services that your organization may provide that demand specific security provisions. Parking facilities, open spaces, and other physical elements require you to secure them appropriately. If your organization rents out space, has a soup kitchen or bingo night, provides summer camps, or provides any other services outside of your regular operations, you must plan accordingly. This document is only to help you understand the needs and responsibilities of security provisions and access control policies. It should not take the place of professional security consultation.