

The Top 10 Office Security Tips

TRUE SECURITY INTEGRATION

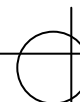


A  **FIRSTSERVICE** COMPANY



THE TOP 10 OFFICE SECURITY TIPS

1. Have a designated person (or persons) open-up and lock-up your premises at the start and end of the business day. It is best not to operate on the basis of 'first employee(s) in unlocks the office, and last employee(s) out lock-up the office. Avoid leaving entrance doors unlocked and unattended. Ideally, entrance doors should only be unlocked when reception coverage commences, and re-locked when the receptionist goes off duty. Where building conditions permit, the access control system should remain 'on control' until reception coverage begins. The system should then be put back 'on control' as soon as possible after reception coverage terminates for the evening. Part of the lock-up procedure should include checking areas such as closets and internal washrooms where persons, wishing to 'break out' after hours, could hide. To accommodate employees arriving and departing before or after reception coverage, install electronic card access on one (or more) access doors.
2. Where electronic access control is in place, issue access cards on the basis of **'least access to perform a specific job function'**. Twenty-four hour, 7-day-a-week access should only be assigned to employees who really require it as part of their job function. Delete missing, lost, or stolen cards immediately. At least annually, request employees to produce their assigned access card. Review access records regularly and follow-up on cards that are not used on a frequent basis. If cards cannot be accounted for, they should be deleted. All visitors should sign 'in' and 'out' in a register. Unknown visitors should be escorted for their first two or three visits. While on-site, guests should be advised to prominently wear their visitor access badges at all times. Visitor access badges should only work during business hours, and they should be audited on a daily basis.
3. Request employees to wear their access cards as a method of making strangers stand out. To discourage 'piggybacking', erect closed-circuit television (CCTV) cameras at entrances. Employees should be advised that if a person who is unknown to them appears to be waiting outside an entry point, they should avoid letting them in. Tactical options include using another entry point, calling security or a manager, offering assistance such as "can I call someone for you?" In the event that the subject person obtains entry, follow him/her, and using a pre-determined 'code word', notify a co-worker. Said co-worker should discreetly contact security and/or management and/or the police. Employees, who are expected to challenge strangers, should be trained on how to do it safely. This training should include the use of intuition, interpreting aggressive body language, the stages of anger, etc.
4. To help prevent theft of proprietary information, a 'clean desk' policy should be instituted. To ensure on-going compliance, inspections should be conducted every two to four weeks during program implementation, and at least quarterly thereafter. As well, the use of a self-inspection checklist can encourage employees to keep their desks clean, and secure sensitive data when they leave their work area unattended.





THE TOP 10 OFFICE SECURITY TIPS

5. Losses due to theft can be reduced by adhering to the following:
 - a. Encourage employees to only bring items to work that are replaceable and have no emotional value.
 - b. Purses left in unlocked, lower right hand drawers, and wallets left in unattended suit/coat pockets, are easy targets for 'sneak' thieves.
 - c. Wallets and purses should be kept in a locked metal drawer when unattended.
 - d. Lock-up the postage meter, cheque writer, and company cheque books when they are going to be left unattended.
 - e. If petty cash on hand is over \$500.00, use a money safe. Otherwise, use a metal cash box and lock it in a metal filing cabinet in the inner office at night.
 - f. When a cash box or combination lock holder leaves the company, change the location of the cash box. This is to prevent theft by current employees who believe that the departing staff member will likely be 'blamed' for the theft.
6. Laptops and PC's, especially those considered to be 'state-of-the-art', are prime choices for thieves. Preventing computer theft begins with an effective reception security program to keep 'opportunistic' thieves and pre-attack 'probers' out. There should be no entrances to the inner office that are not controlled by 'in' card readers and/or the receptionist. Where the use of a full-time receptionist cannot be fiscally justified, a restricted-use telephone, internal telephone directory, and appropriate signage should be located outside a suitable access door. To aid employees when they are challenging strangers, phone directories, which can be accessed by thieves, should not list job titles or departments. Criminals will often use the names of senior company officials to justify what they are doing. Avoid situations such as "Sir, where are you going with six of our laptops?" "It is OK, I am putting in a software 'fix' for Barb Smith, VP of IT". PC's in areas accessible to the general public, such as the mailroom, reception, shipping/receiving etc., should be secured with cable locks or plate locks (preferable). Hopefully, this will give thieves the impression that all computers in the office are protected. Installing secure docking stations, on roller shelves that can be rolled into lockable furniture when the employee is leaving his/her work area, best protects laptops. If employees spend most of their time in the office, issuing them a PC instead of the highly-portable, easily-concealed, laptop can mitigate the risk of laptop theft. Outside of the office, employees should be encouraged to carry laptops in a sports bag or briefcase and not in the manufacturer's bag.



THE TOP 10 OFFICE SECURITY TIPS

7. Keys should be stamped with a number and signed for when issued. At least annually, employees should be asked to produce the key(s) that they were originally issued/signed for. Issuances of 'master' keys should be kept to a minimum. Keys being issued to contractors and cleaners should be signed 'in' and 'out' on a daily basis. Where this is not practical, consider purchasing an automated key control cabinet such as those produced by Key Systems Inc. and sold by Intercon.
8. When issuing access cards to contractors, they should be programmed to provide the 'least access necessary to perform a specific job function'. For example, evening cleaners should typically receive cards that only work between 5:00 p.m. and 11:30 p.m., Monday through Friday. Also, their cards should only work in a designated area or certain floors. When contractors' cards are not restricted, they become a major exposure if they become lost, missing, or stolen. Contractor cards that are being signed 'in' and 'out' should be audited daily.
9. Secure stairwells either by locking same, or installing suitable electronic locking devices and card readers. Where cross-over floors cannot be 'maglocked', consider renovating the floor so that they are located outside of the protected area.
10. Install apartment-style, optical viewers on solid doors used by staff for after hours shipping/receiving, who leave work late, or who must use washrooms located outside of the protected area. Consider installing cypher locks or spring-loaded deadbolts on washrooms located outside of the protected area. To eliminate 'real' or 'perceived' ambush hazards, install overhead-mount, convex mirrors in hallways used by staff after hours. The foregoing will also improve the comfort level of employees who work late.

For more information on these topics, please see the following Intercon Security documents:

- Reception Security Guide
- Bi-Annual Security Self-Inspection Checklist
- Electronic Access Control Bulletin
- Cleaners Security Bulletin
- Key Control Bulletin

This document is intended for the sole use of Intercon Security and its clients. No one is permitted to reproduce this document in any form, in whole or in part, without the permission of Intercon Security.