

3-Level Security Escalation Planning Guide



TRUE SECURITY INTEGRATION

A  **FIRSTSERVICE** COMPANY



3-LEVEL SECURITY ESCALATION PLANNING GUIDE

Benefits

Three level security escalation plans are prepared by company security directors or property managers to establish, in advance of a crisis or anticipated crisis, comprehensive lists of escalating security measures. Benefits of this process include:

1. The elimination of panic or impulse buying of security goods and services.
2. Ensures that what security goods and services that are purchased are deployed in the most effective and efficient manner possible.
3. Encourages the pre-need purchase and installation of security equipment such as card readers. Even if not required on a daily basis during the normal operation (Level I) stage, the ability to quickly activate this equipment adds flexibility and speed to management's response options.
4. Demonstrates a pro-active management approach to employees.
5. Helps avoid employee panic.

Operating Modes

1. Level I is the normal day-to-day security operating mode.
2. Level II outlines security measures that are to be implemented as a response to a threat or situation that management, in conjunction with the police and Intercon Security professionals, has evaluated as serious, but not immediately dangerous.
3. Level III outlines additional security measures that are to be implemented supplementary to Level II, and as a response to a situation that has been evaluated as very serious and potentially dangerous.
4. Initiation of the Level II or Level III security plan will normally be in response to a threat. They may also be instituted as a result of deteriorating local conditions, or in response to intelligence gathered from the media including local and foreign newspapers, the Internet, the police and other government agencies.

The following charts indicate in general terms, options to be considered by management for each level. As well, it will provide further information on analysis of threats and deciding when to institute Level II or Level III.



3-LEVEL SECURITY ESCALATION PLANNING GUIDE

LEVEL I	
TACTIC	SAMPLE TIMES/PROCEDURES
1. Common Area Open-Up	7:00 a.m.
2. Common Area Lock-Up	6:00 p.m.
3. Building Access Control System (includes elevator controls)	Off at 7:00 a.m. On at 7:00 p.m.*
4. Building Stairwell Open-Up	7:00 a.m.
5. Building Stairwell Lock-Up	6:00 p.m.
6. Stairwells (on all floors except those currently secured)	Open-Up at 7:00 a.m. Secure at 6:00 p.m.
7. Supplementary Card Readers	Off at 7:00 a.m. On at 7:00 p.m. (Note: Supplementary card readers, in some cases, may be completely inactive until a threat is received. A typical use for supplementary card readers is on doors providing access from the office lobby to the office interior).
8. Site Security	Normal Duties and On-Going Intelligence Gathering.
9. Utility Security	Normal Procedures.
10. Site Staff	Adherence to Regular Security Procedures (e.g., visitor sign-in, visitor escorts, etc.).
*This reflects common practice in many buildings. The most appropriate times are 'off' at 8:00 a.m. (or whenever reception starts, and 'on' at 6:00 p.m. (or whenever reception coverage ends).	



3-LEVEL SECURITY ESCALATION PLANNING GUIDE

LEVEL II	
TACTIC	SAMPLE TIMES/PROCEDURES
1. Common Area Open-Up	9:00* a.m., site conditions permitting. (*Or when reception coverage commences – e.g., 8:30 a.m.).
2. Common Area Lock-Up	5:00* p.m., site conditions permitting. (*Or when reception coverage ends).
3. Building Access Control System (includes elevator controls)	Off at 9:00 a.m., site conditions permitting. On at 5:00 p.m., site conditions permitting.
4. Building Stairwell Open-Up	9:00 a.m., site conditions permitting.
5. Building Stairwell Lock-Up	5:00 p.m., site conditions permitting.
6. Stairwells on the Floor Identified in the Threat	Secure 24 Hours.
7. Supplementary Card Readers	Secure 24 Hours.
8. Site Security	Two extra coverage Security Officers during business hours. One stationed in the threatened area. One stationed in the lobby (plus one on general patrol if there is not site coverage). Site Security is advised to be very vigilant and alert. Site Security Officers conduct more intensive patrols of sensitive areas (including parking), and continue active intelligence gathering.
9. Utility Security	All utility, mechanical, and fuel storage areas are secured 24 hours, and patrolled at least once every four hours. Fire and sprinkler systems are checked by Security. All fire and intrusion systems etc., have central station connections tested.



3-LEVEL SECURITY ESCALATION PLANNING GUIDE

LEVEL II cont'd	
TACTIC	SAMPLE TIMES/PROCEDURES
10. Site Staff	Staff advised of threat and requested to: Review all security procedures, report unusual activity, report any missing or unaccounted for keys and passcards.
11. Potential Target	Advised to take suitable security precautions at work, in transit, and at home. Also, advised to maintain close communication with their manager and to advise Security of <u>all</u> untoward/unusual activity at work, in transit, and at home.
12. Assailant	Active intelligence gathering continues. Obtain and circulate photographs. Ensure the police are aware and have the suspect's photograph, date of birth, address, description, etc.



3-LEVEL SECURITY ESCALATION PLANNING GUIDE

LEVEL III	
TACTIC	SAMPLE TIMES/PROCEDURES
1. Common Area Open-Up	Building perimeter remains secure and on access control 24 hours, site conditions permitting. If site conditions do not permit the securing of the perimeter, then elevators should be put on card access, stairwells secured, and visitors escorted from the lobby by tenants/building occupants/employees.
2. Common Area Lock-Up	Building perimeter remains secure and on access control 24 hours, site conditions permitting. If site conditions do not permit the securing of the perimeter, then elevators should be put on card access, stairwells secured, and visitors escorted from the lobby by tenants/building occupants/employees.
3. Building Access Control System (includes elevator controls)	Building perimeter remains secure and on access control 24 hours, site conditions permitting. If site conditions do not permit the securing of the perimeter, then elevators should be put on card access, stairwells secured, and visitors escorted from the lobby by tenants/building occupants/employees.
4. Building Stairwell Open-Up	Secure 24 hours, site conditions permitting.
5. Building Stairwell Lock-Up	Secure 24 hours, site conditions permitting.
6. Stairwells on the Floor Identified in the Threat (and all other stairwells, except cross-over floors and any other stairwells which cannot be secured for operational reasons)	Secure 24 hours, site conditions permitting.
7. Supplementary Card Readers	Secure 24 hours.



3-LEVEL SECURITY ESCALATION PLANNING GUIDE

LEVEL III cont'd	
TACTICS	SAMPLE TIMES/PROCEDURES
8. Site Security	Security Officers advised to review all Officer safety procedures, and to wear protective equipment at all times. Level II extra coverage, and possibly three additional, 24-hour patrols. Security Officers: One interior, one exterior, one parking, one additional lobby S/O (or more depending upon access control requirements), and one additional S/O in shipping/receiving during business hours.
9. Utility Security	All utility, mechanical, and storage areas are to be secured 24 hours, and patrolled once every two hours. Sensitive areas such as fuel storage and gas valves are to be patrolled hourly, resources permitting. All non-occupied and non-essential areas secured 24 hours, and opened on request only.
10. Site Staff	Staff advised of the seriousness of the threat and the requirement for 24-hour access control.
11. Potential Target	Additional security measures are considered, including transfer to a more secure location, time off, residential security coverage, secure transport, etc.
12. Assailant	Consider covert or overt surveillance. Ensure the police are continuously updated.

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.

10912