INTRODUCTION

From my observations and experience with well over 1000 facilities spread over more than 30 countries worldwide, there are two (2) issues regarding Security Policy documents that ***I cannot over emphasize*** to readers:

- A good Security Policy is THE most essential element in maintaining EFFECTIVE physical security, and
- Security Policy documentation is THE most commonly deficient element found in any security program.

Developing and writing a good security policy document is both a skill and a bit of an art. It has a lot in common with the task of writing *laws, legislation, contracts* and other legal documents, and with "technical writing" such as *user's guides* and *instruction manuals*. Like these two examples, ANYONE can write them … but very few can write them so that they have the INTENDED overall effect. "Precision" writing is different than conversational or typical writing.

This white paper is less about "*what should BE INCLUDED in your security policy*" and more about HOW to structure, develop and write such a document. The strategy, wording and style are the more difficult aspects for most people undertaking such an endeavor. The objective is to REQUIRE specific behavior with clarity, without unintentionally REQUIRING MORE and without PERMITTING LESS. Often, this may seem simple to the writer who knows exactly what he or she "means", but is NOT in a way that is reasonably understandable to all the READERS that have to live with it. The most common error is to describe things in a manner that is much too "subjective" and open to interpretation.

UNDERSTANDING THE PARTS

The term "Security Policy" is often used loosely to describe all manner of organizational mandates. To accomplish the objective, it may be best to define some of the types or parts of security documents so that they can be utilized appropriately.

- *POLICY* should be considered as the broad and general mandate or position formally established by an organization, company or enterprise. These set out objective oriented goals that reflect the philosophy, culture and ideals of the group. Normally there are numerous such mandates within each document that addresses a particular subject – like "Security" – and they might also be referred to as "Policies" in plural. POLICIES are almost never effective if NOT fully and officially supported by the very highest levels of management (CEO and/or Board of Directors). The wording is usually broad and general, with the focus being on the desired end result.

- *STANDARDS* are more specific than policies, but are an essential feature for the "implementation" of policy. To the fullest extent practical, standards should be written in terms that are "MEASURABLE and/or OBSERVABLE". Examples include characteristics such as "time", "distance" and "speed". These are important in "objectively" determining compliance, non-compliance and levels and quality of performance for auditing.

- *PROCEDURES* are the most detailed of the documents and may be highly SPECIFIC to an individual building or facility. These describe "steps" to be taken in order, "tasks" to be accomplished and similar ACTIONABLE information that a reader can use to correctly comply with Policy. Elements such as WHO, WHAT, WHEN, WHERE and HOW should be considered when writing a procedure. In the security realm, "Post Orders" and "General Orders" for guards would be in the category of Procedures.

- *GUIDELINES* are items that are NOT "Mandatory", but might include examples, suggestions, recommendations and other language that HELPS a reader better understand mandates contained within Policies, Standards and Procedures. The language can be less precise than employed in policy and standards writing. Describing the OBJECTIVE of a policy, standard or procedure can often assist in clarity by conveying to the reader WHY the provision exists.

All together, these will be referred to as "security documents" herein.

CHALLENGES FOR THE GLOBAL ENTERPRISE

For any large organization having numerous physical locations spread over great distances, writing security documents for application to the entire enterprise can be particularly challenging. Because all physical security planning should be based upon the specific THREATS and RISKS at the protected premises (Design Basis Threat – DBT), *there is no "one size fits all" solution*… but there is a very effective and proven workable solution! Organizations with far flung international operations have additional issues including laws and culture. Risks for threats such as crime and terrorism can be different even for multiple locations within a single city, state, country or continent. Likewise when the combination of facilities varies in nature such as some *office buildings*, some *retail outlets*, some *production plants*, some *warehousing*, etc. the challenge is further compounded.

"WORD-SMITHING"

When developing the security documents for a global enterprise, the "wording" is CRITICAL when conveying "*applicability*" of each statement or provision. Generally, ONLY those included in the wording need to comply. If they don't fit the criteria, they are excluded from that provision. Some examples should further explain this concept;

- *All facilities …*
- *All facilities employing more than 50 persons shall….*
- *All facilities designated at "MEDIUM" or "HIGH" for CRIME risks shall…*
- *All facilities designated at "HIGH" for TERRORISM risks shall…*
- *All facilities or portions thereof having access by the general public shall…*
- *All employees…*
- *All visitors…*
- *All vendors…*
- *All contractors…*

Provisions can be described as either MANDATORY or VOLUNTARY using words such as;

- Shall or Will (mandatory)
- May or Can (voluntary)
- Should (recommended or suggested, but not mandatory)

ACCOMODATING VARIATIONS IN THREATS and RISKS

An effective strategy for addressing the variations in the specific security needs of each of numerous facilities is to develop a graphic MATRIX for this purpose. An example using 4 levels for CRIME and 4 Levels for TERRORISM is shown here;

SECURITY RISK DESIGNATION MATRIX *(SRDM)*				
TERRORISM > / v CRIME	1 = EXTREME	2 = HIGH	3 = MEDIUM	4 = LOW
A = EXTREME	A1	A2	A3	A4
B = HIGH	B1	B2	B3	B4
C = MEDIUM	C1	C2	C3	C4
D = LOW	D1	D2	D3	D4

We delineate between CRIME and TERRORISM because some of the security measure employed against the threat of most crimes might not be suitable against the threat of terrorism. For example, a location may require dynamic vehicle barriers and deep search processing for terrorism, but is not necessarily in need of them for most criminal activities.

Using the example matrix, every facility will be assigned one of the 16 designations at the time of implementation of this concept. It will also be reviewed periodically and – if warranted – changed to a higher or lower designation as appropriate. The actually number of levels for your matrix can have less or more distinctions if desired, but 3 and 3 would usually be the minimum.

While a good researcher / analyst might be able to determine the appropriate designations for each facility initially, the author's experience has been that the use of one of the specialty firms is likely the best source for obtaining and monitoring global threat risks. For CRIME data in areas they cover, CAPINDEX has been frequently used. For TERRORISM data, there are several including iJET, Control Risk and others. Some of these will have data with category designation that can be used directly as a matrix.

DOCUMENT STRUCTURE & FORMAT

There are MANY variations in the layout of policy related documents. Some organizations use a form having blocks with fields for information such as title, subject, dates of revisions, signatures, etc. In these cases, the intent is usually that – in printed form – the document could be in a binder and sections would be replaced at each revision. Alternatively, a single document is used that contains all provisions can be written. Most often, it is appropriate to use the format and structure that already exists for the organization as the "standard" way for all such documents, "security" and non-security.

Regardless of the structure, it is important to have the parts, sections, chapters, paragraphs, provisions and similar elements ALPHA and/or NUMERICALLY annotated. When writing correspondence, reports, messages or other communications, the highest inclusive level annotation can be mentioned, rather than duplicating the content or repeating the content as a quote. This is commonly known as a "Citation". Other than in a Table-of-Contents (TOC) or Index, "page numbers" should not have much significance as these will change often due to revisions.

One example of how this might look is as follows (example for global hospitality chain);

1. PhYSICAL SECURITY MEASURES

1.1 PARKING AND TRAFFIC CONTROL

A. Policy

The Security Department shall have authority over all traffic, parking and vehicles on Hotel property to the extent necess ary to maintain security.

B. Standards

1. Subject to applicable law, the Security Department shall cause the immediate removal (without the need for providi ng prior notice or obtaining the owner□s consent) of any vehicle parked in an area designated "No Parking" in acco rdance with Local Security Procedures. Signage designating "No Parking" areas and indicating that vehicles parke d in "No Parking" areas will be towed at the vehicle owner□s expense shall be posted in all such "No Parking" area s. Subject to applicable law, vehicles that have been parked in violation of posted restrictions shall be towed from t he Hotel premises at the vehicle owner□s expense.

2. Subject to applicable law, the Security Manager may cause any vehicle to be towed from Hotel property (without th e need for providing prior notice or obtaining owner□s consent) where probable cause exists to believe that such v ehicle may pose a threat to people or assets or that is otherwise obstructing Hotel operations.

3. Where Hotel employees are permitted to park on Hotel premises, the Security Manager (after informing the Gener al Manager and Director of Human Resources) may revoke the parking privileges of any employee found to have v iolated this Security Policy or Local Security Procedures with respect to parking his or her vehicle.

All Category (A) High Terrorism Locations shall designate a "Stand Off Zone" surrounding the Hotel and a ny other structure on Hotel premises that is considered an integral part of the Hotel operations for the pur pose of minimizing the potential effects of an explosion in accordance with following considerations:

a. Each Stand Off Zone shall be clearly identified in the Local Security Procedures.

b. No Stand Off Zone shall extend to property that is outside of the security control of the Hotel, and the l ine delineating a Stand Off Zone may be at various distances from the building at different points on it s perimeter as a result.

c. Where it is practical, a minimum distance of 150 feet (45 meters) should be used as the Stand Off Zone for vehicles and 50 feet (15 meters) for persons and small packages. Where these distances are not r easonably possible, the maximum practical distance available under the conditions and circumstance s should be utilized.

d. The perimeter of a Stand Off Zone shall be resistant to penetration by vehicles, using natural terrain, a rchitectural features, fixed barriers or dynamic barriers. Traffic control arms, gates and other measure s that are not resistant to forcible penetration by vehicles shall not be considered as compliant with th is requirement.

e. Prior to entry into the Stand Off Zone all vehicles, individuals and items shall be screened in accordan ce with the requirements of Section 7.6 of this Security Policy.

C. Guidelines

It is not the intent of this section to require that complete responsibility for all parking operations be vested with the Secu rity Department. It is the intent that the Security Manager have sufficient authority over some parking related matters so as to insure compliance with this Security Policy.

The text in RED (any chosen COLOR) is just one method of calling attention to requirements that apply to facilities with an elevated level of risk for CRIME and/or TERRORISM (those locations other than LOW/LOW). In the example, this applies to HIGH TERRORISM designations. Color coding the text to correspond with the matrix is one way of assisting readers in finding "exceptions" to the norm that might apply to the facility for which they are responsible (such as always looking for "blue" text, or "green" text, etc.).

These provisions for elevated threat risk locations can be referred to as "**ENHANCED STANDARDS**" collectively.

PROCEDURES

To address issues that are best DETAILED based upon specific conditions and each location, the ENTERPRISE level security document will have provisions requiring the development of LOCAL PROCEDURES where appropriate, thereby creating an auditable document for that premises. At inception, these should be reviewed and approved by security staff at a higher level, such as cluster, area, region or headquarters to assure compliance with the global policy. This would specifically include – but not be limited too - "Post Orders" and "General Orders" for guards.

CONCLUSION

It has been said that there are ONLY 3 REASONS for failures in physical security;

1. There is NO POLICY covering the issue; or
2. The POLICY does exist, but was not FOLLOWED; or
3. The POLICY was followed, but it was INADEQUATE for the situation.

#2 is likely related to "training" or may be a "disciplinary" matter. #1 and #3 can ONLY rest with the responsible security MANAGEMENT staff.

ABOUT THE AUTHOR: Michael Minieri CPP, CSC is the Principal Security Consultant for Minieri Associates Worldwide which offers Security Document Development among its core services. He can be contacted at MMinieri@MinieriAssociates.com