

# INDUSTRIAL SECURITY & ASSET PROTECTION

## Part 2



For Additional Info ..... <http://www.elitecanada.com/tips.php>

## **Identification of importance of product, process, information, etc.**

- A. Importance of specific product, process, or service, and current security efforts applied to protect same**
  
- B. Levels of classification and authorization for access to specific product, tooling, equipment, DOCUMENTS etc.**
  
- C. Determination of how critical a security breach would be to company operations. What happens if someone steals your client info.**
  
- D. Identification of critical office and work areas involving the use of the product, process, information, or service**
  - I. How vulnerable are these areas at the present time?**
  
  - II. How frequent is an evaluation made of critical areas?**
  
  - III. How effective is pre-employment screening for persons in high risk or critical areas?**
  
  - IV. What are the levels of authorization?**
  
  - V. What levels of accountability are in force?**
  
  - VI. Have security classifications been assigned?**
  
  - VII. Has an assessment been made of the value, critical nature, and related impact on the company if a loss occurs?**
  
  - VIII. What special advantages might be lost?**
  
  - IX. Have effective countermeasures been implemented?**

## **External planning and assessment factors: security environments**

### **Assessment of the business or facility in relation to the surrounding neighborhood, business district, industrial park, and other related setting**

- I. Is good surveillance of the property possible?**
- II. Are effective access controls in place?**
- III. Is the structure located in a high crime area?**
- IV. What has been the history of crime and/or security breaches?**
- V. Is the facility isolated and located in a remote area? (VELCO)**
- VI. If so, what has been done to protect/safeguard approaches to the facility? (Identification of visitors, vendors, etc.)**
- VII. Are all possible access points monitored and protected?**
  
- VIII. What would be the probable response time by police or security staff, if a security breach occurs?**

## **Assessment of factors pertaining to freedom of access and factors related to layout and design considerations**

**I. Are external areas designed and developed in conjunction with security needs?**

**II. Who is allowed access to the facility and during what times of the day? Levels of authorization?**

**III. Have high risk areas, such as those containing trade secrets, confidential information, computer files, sensitive records, and documents been given special attention for security and protective needs?**

**IV. What factors are specific to this particular operation?**

**V. Are there any aspects of the facility in need of upgrade with regard to security?**

**VI. How effective are the current security aspects of the following areas?**

1.
  - a. Barrier controls, fencing, building design, etc.
  - b. Lighting conditions for security illumination
  - c. Obstructions to security patrols and surveillance visibility
  - d. Exterior doors, access points, entrances, etc.
  - e. Exterior windows and other openings
  - f. Possible points of concealment and climbing aids
  - g. Trash collection areas and disposal of documents, papers,
  - h. Alarm systems and related security devices
  - i. Personnel, visitors, and others: control of movement, etc.

## **Assessment of the potential of unauthorized entry to high risk or sensitive areas**

- I. Do neighboring facilities, structures, buildings, etc. present or create any observable security hazards? Could access control be compromised by an intruder gaining access from another building or facility?**
- II. Could locking mechanisms be compromised?**
- III. Do other openings create security problems?**
- IV. Is there an effective program of lock maintenance and **key control** management?**
- V. Has everyone been identified who has keys or other forms of access to high risk areas? Is the list up-to-date? Are there restrictions combined with levels of authorization?**
- VI. If a locking system or other protective device is compromised, what procedures and/or actions are taken?**
- VII. Are intrusion detection devices adequate? Could they be compromised? What changes would improve security?**
- VIII. How effective is wall, ceiling, hallway, or office construction in preventing compromise of high risk areas?**
- IX. Is there an effective level of employee vigilance?**

## **Procedural security and policy formulation**

### **Identification of essential needs for a written security policy with well-defined procedures**

- I. Is there written company policy regarding security practices and procedures? Are there specific statements pertaining to the protection of company secrets, information, documents, etc.?**
- II. Does policy incorporate specifics with regard to enforcement and penalties?**
- III. Will the company prosecute?**
- IV. Is policy translated into actual practice?**
- V. Does the policy make an effort to cover all possible situations?**
- VI. Do employees understand the policy? Is it made available?**

### **Procedures and rules specify operational areas**

- I. Are specific guidelines provided to all personnel with particular emphasis on operational areas?**
- II. Do guidelines cover the locations and operations of the high risk and sensitive locations, such as: visitor control points; files and cabinets; labs and research; safes and vaults; library storage; copy centers; document storage areas; computer sites/centers; production/process areas; critical office areas; blueprint rooms; office equipment/machines; other special areas.**
- III. Are there checks and balances to ensure proper security regarding check-out, check-in, borrowing, loan, etc.?**

**Procedures, rules, and policies are clear-cut and understood with regard to all levels of operation in high risk locations within the company:**

- 1- Employee orientation programs and training**
- 2- Signed statements by employees attesting to policies, procedures, etc. (e.g. nondisclosure agreements)**
- 3- Assignment of certain personnel (security staff) for monitoring, enforcement, etc.**
- 4- Selective monitoring and evaluation (undercover officers, investigators, etc.)**
- 5- Enforcement applied to everyone in a fair manner without regard to position or level in company**
- 6- Security practices emphasized on regular basis**
- 7- Opening and closing procedures**
- 8- Log-in and log-out procedures followed closely**
- 9- I.D. badges worn at all times where required (if applicable)**
- 10- Centralization of access points, entrances, exits, etc.**
- 11- Disposal areas and trash collection points monitored**
- 12- Appropriate use of security systems and devices**
- 13- Unannounced inspections and checks**
- 14- Inventories and audits on regular basis**

## Procedure security planning

I. Is management satisfied that appropriate steps have been made to ensure reasonable security procedures to safeguard property, equipment, tooling, other assets, & sensitive and critical information, processes, materials, etc.?

II. Is every effort made to ensure that personnel understand that a certain product, process, or information is classified as secret or confidential, or some other sensitive classification?

III. Has every effort been made to enforce and restrict the access to sensitive areas and materials? Have procedures been followed in a consistent manner?

IV. Have guidelines been published within the company, listing those materials, assets, documents, processes, information, papers, etc., that are classified as sensitive and restricted? Are these provided for each specific group or project area?

V. Have levels of sensitive classification been established? (For example, "secret," "classified," "confidential," "restricted," etc.)

VI. Are restrictive signs posted in sensitive areas?

VII. How effective are current procedures with regard to:

1.
  - a. Access controls
  - b. Opening and closing
  - c. Control of documents
  - d. Supervision/monitoring
  - e. Property control
  - f. Check-in and check-out
  - g. **Control of contractors**, vendors, repairmen, janitors etc
  - h. Disposal/removal of records, papers, etc.
  - i. Key control and key usage
  - j. Locking and unlocking
  - k. Shipping/receiving controls
  - l. Storage of materials, etc.
  - m. Employee vigilance/surveillance
  - n. Security systems/devices
  - o. Other procedures and controls

## **General Recommendations**

**Security protection, and prevention is not only effective for asset, and access control, but also in the event of potential lawsuits. It can be shown that preventative security planning has been implemented for the security, and safety of employees, visitors, suppliers, vendors etc.**

**1- An effective methods of closed circuit television surveillance and materials screening should be in place at all access/egress points. FENCING**

**2- Plan for Access Control to manufacturing plants. (Locks can be picked or manipulated)during working hours, and especially on weekends or off shifts.**

**3- Control your access to documents, blueprints , client contacts, bids etc. with control of who has access and when they have access , with sign in, and out procedures, for control. A safe room should be considered.**

**4- Screen your employees thoroughly, they will have access to your assets, equipment, tooling, documents, and sensitive information.**

**5- Random property, and plant location, security patrol spot checks. Who controls keys, access, etc. Who has keys ?? Duplication!!**

**6- Control WSIB and insurance claims with investigations, And follow ups.**

**7- Special attention should be dedicated.... in control of suppliers, vendors, trades entering your plants, and controlling their access to the specific area of business. Possible solution...proximity readers.**

**8 Time Theft ....what precautions are in place? Employees leaving plants prior to shift end, or managers/ sales personnel not on the job as required.**

**9- DO NOT ALLOW INDIVIDUAL LOCATIONS TO CONTROL THEIR OWN SECURITY. THIS IS INEFFECTIVE & IS EASILY BREACHED !**

**CORPORATE MUST CONTROL SECURITY...INTERNALLY & EXTERNALLY.**