

Site Security Evaluation

A site security survey is similar to a physical exam conducted by a doctor, in that he/she is attempting to discern what, if anything is wrong with the patient before prescribing any course of treatment, medicine. The survey form that follows is by no means the work of a single individual; the questions posed having come from a multitude of sources over a period in excess of fifteen years. This is not to say the form is old, because it is reviewed on a regular bases, questions added as new areas, such as violence in the workplace, surface and impact the Security Profession.

Administrative/General Data

1. Site:
 - Function:
 - Address:
 - Telephone No.:
 - Manager:
 - Assistant Manager:
 - Human Resources Superintendent:
 - Control Superintendent:
 - Number of Employees:
 - Area covered (acres):
 - Operating hours:
 - Products Manufactured:
2. Review last finance department audit of this site for any exceptions relating to security. What action(s) has been taken relative to these exceptions?
3. Since the last survey has the site terminated anyone for theft, fraud, etc., or drug related activities?
4. Relative to the preceding, have any investigations been conducted on the site since the last survey?
5. Survey should include review of theft reports prepared by this site for an appropriate period of time. Where appropriate, has corrective action been taken? Do theft reports reflect patterns, trends, or particular problems at this location?
6. What does site management regard as the most prevalent or serious security problems?
7. Has the person responsible for day-to-day site security received any formal training in the subject; and if so, what?
8. What are the sites most theft attractive assets?
9. Have you under your control (including in your manufacturing process) any precious metals, controlled substances, precursor chemicals, or anything else readily convertible to cash on the illicit market?
10. Does the site have the latest revision of the Precursor Chemical List?
11. Identify off-site locations which should be included in survey, to include warehouses, river pumping stations, outflow lines, well-heads, purchase power substations, magazines, etc.?
12. Does the site have a security committee? Who are the members, do they rotate, and how often do they meet?
13. Is the site properly posted with respect to search and trespass?
14. What police agency has jurisdiction over the site? Does the plant have a dedicated phone line to this agency? Has management established a continuing relationship with this agency? Have they been called for in the recent past; and if so, what has been their response? Do they normally include any of our perimeters in their patrols? If requested, would they?

15. Are police emergency numbers readily available to plant security personnel?
16. Is information readily available on how to reach the proper agency for assistance with illegal narcotics, bomb threats, obscene calls, etc.?
17. Do you have a policy of reporting identifiable items of stolen property to the local police?
18. Does your law enforcement agency have a Crime Prevention Unit qualified to speak on such topics as drug usage, personal and residential security and highway safety?
Comments
External Security
19. Is the manufacturing/operations area perimeter adequately lighted?
20. Is site exterior lighting checked on a regular basis to be certain it is functioning properly? How frequently and by whom?
21. Is lighting compatible with CCTV?
22. Is power supply adequately protected?
23. Is lighting properly maintained and cleaned?
24. Are sensitive areas (parking lots, computer areas, stores, tool rooms, shipping/receiving areas) adequately lighted?
Comments
Security Force
25. Proprietary or Contract? If contract, name of agency and telephone number. If proprietary, how are personnel selected? Security Officer pay rate? Site filling rate?
26. Are posts rotated; what is the frequency?
27. How many officers per shift?
28. a. What type of training and supervision do officers receive?
b. Where a solitary security officer is on duty after normal business hours, is there a procedure in place requiring that individual to call, or be called, to verify his/her well being?
c. Do security officers possess any type of defensive weapons such as mace, nightsticks, etc.? If so, is there a written policy in effect governing their use? Have officers received training in their use? Company policy prohibits lethal weapons except on specific authorization of Director of Corporate Security.
29. Are security facilities adequate and are unauthorized people kept out of the gatehouse(s)?
30. Is a current list of authorized signatures (for passes, etc.) maintained at the gate house? Who monitors property passes for returnable items?
31. Is an incident log maintained?
32. Is the log reviewed daily and by whom?
33. Are security personnel utilized for non-security related duties?
34. Does site utilize photo I. D. cards? Who administers it? Are all employees required to show a photo I. D. card to security personnel upon entry? Is duplicate copy kept in security daily?
35. Does facility have on-site parking? Are vehicles registered? Can an individual reach a vehicle without passing a guard?
36. If needed, does the security force have a properly equipped and maintained patrol vehicle?

37. Does the site have a receptionist in place at all times? Are visitors required to sign in? Are they provided with an identifying badge, and if non-employees, escorted while on site? Is visitor identification verified, e.g., vending company I.D., etc.?
Comments
Perimeter Protection
38. Is the site completely fenced? Describe type of fencing.
39. Is it secure against the ground especially on uneven terrain? Are there rivers, ponds, trees, buildings or other structures on the perimeter that can be utilized to achieve unauthorized entry? Are articles susceptible to theft stored close to the fence?
40. Is a 10 ft clear zone maintained around the entire perimeter, on each side of the fence, where physically possible?
41. If outside building walls form part of the perimeter, are all doors and windows secured against surreptitious entry? Can entry be achieved via the roof? Can hinge pins be removed from doors? Are all entry/egress points manned when opened? Is fence line patrolled? If so, how often? By vehicle or on foot?
Comments
Internal Security
Lock/Key Control
42. With whom does physical and administrative key control rest?
43. Describe control of keys, including issuance to non-personnel.
44. Is master key system in use? How many grandmasters/master keys have been issued?
45. Is a cross control system (name versus key number) in use? What type of numbering system is in use? Is the entire system, including blanks, inventoried on a regular basis?
46. Are keys stamped "Do Not Duplicate?"
47. What level of management authorization is required for issuance of keys?
48. Are plant keys, particularly masters, permitted to be taken home? Are keys signed in/out in a daily log?
49. Are locks rotated?
50. How long has the present lock/key system been in use?
51. Have keys been reported lost?
52. Is a record of locations of safes and their combinations maintained?
53. How frequently are combinations changed?
Comments
Alarms and Electronics
54. Is an electronic security alarm system in use here?
55. Is a card access system in use here?
56. Do alarms terminate on the site or at an outside central station?
57. Who responds to alarms? Has service/response been satisfactory?
58. Does the site have a radio network? Separate frequency for security? Battery back-up?
59. Are portable radios, chargers and cellular phones properly secured when not in use?
Comments
Theft Control Procedures
60. Does this location have a program of pedestrian inspections?
61. What is the frequency of these inspections?
62. Does this location have a vehicular inspection program? If so, briefly describe procedures.

63. Does this location have a locker inspection program? If so, briefly describe procedures.
64. Does the site have a policy of marking theft sensitive items (TSI) (such as PCs, VCRs, electronic scales and hand tools) as company property? Describe the program. Is someone responsible for accountability of all TSI at the end of the day? Who maintains the list of theft sensitive items?
65. Are serial numbers of all items recorded?
66. In the event of theft, is this information furnished to the police for identification purposes in event of subsequent recovery?
67. Are items susceptible to theft left out in the open (e.g., unbanded laydown areas)?
68. Are trash receptacles periodically inspected by supervision to determine whether items of value may be removed from the site via them?
69. Can the trash receptacles be locked at night?
70. Is the trash truck followed to the dump on a random basis? Is what is dumped checked to be certain that nothing of value, including documents, is deposited, possibly for later pickup?
71. Is scrap metal segregated by type? Does the site have a salvage removal program? Are printer sequentially numbered scrap passes utilized? Does security inspect scrap items versus the pass?
72. Describe the site's toolcrib system?
73. What is the procedure during off hours?
74. Are all stores attended when open? What is the procedure for admittance when no attendant is present?
75. Is access to telephone switching equipment (frame room) restricted?
76. Are shipping/receiving functions performed from the same dock?
77. Does that area have secure facilities (lockable cages) for high value items?
78. Are these high value items checked/inventoried regularly?
79. Are other than shipping/receiving personnel permitted in the area?
80. Has a restricted waiting area been designated for drivers?
81. Are seals used?
82. Is documentation for Federal Express and UPI shipments spot checked, audited?
83. Is there a truck or railroad scale on site? Is it operable or accessible to non-company personnel? How is the operation supervised?
84. Do you utilize printer sequentially numbered weight tickets?
85. Who performs custodial services?
86. Are they bonded?
87. Are they required to wear ID badges?
88. Which areas are serviced?
89. Are they inspected by guards as they leave? Are the janitors vehicles inspected on the way off the site?
90. Do the janitors have access to restricted or sensitive areas (shipping/receiving, stores, tools and computers)?
91. Are the janitors permitted to take keys off the site with them?
92. How much cash is kept on site? Describe cashier's operation.
93. Where are checks held?
94. Considering the products you manufacture, the required raw materials or intermediates, the neighborhood the site is located in, and the amount of cash on site, how do you assess your vulnerability to robbery?
95. Is there a monitoring procedure for fuel consumption? Gasoline and diesel?

96. Is fuel stored on site? If so, can unauthorized people access it?
Comments
Proprietary Information
97. a. Is there proprietary data on site; and if so, in what form?
b. Has critical information been identified?
c. How vulnerable is this information to unauthorized access and reproduction?
d. Have the owners, custodians, or security people identified any potential threat or possible adversaries or vis-a-versa of this information?
98. Describe site's PIP program.
99. Does the site have a PIP Committee?
100. Are PIP posters in evidence?
101. a. Is copying equipment controlled and locked after hours, or can anyone use it?
b. Are facsimile machines located behind lockable doors so messages received after hours are not available to unauthorized persons?
c. If you have reproducing blackboards (whiteboards), are they the type that store information in memory and copy from that memory, or do they copy on command and then automatically erase? If they copy from memory, does someone ascertain that the memory has been cleared when that information is no longer needed?
102. Are PIP inspections made during off hours?
103. a. Do you have a specific method for destroying sensitive proprietary information? If so, what is it?
b. Is anyone at this site involved in the acquisition of competitive intelligence? If so, who?
Comments
Personnel Security
104. Are background checks conducted prior to employment?
105. Are previous employment dates verified?
106. Are personnel and medical records properly safeguarded?
107. Is security included in the new hire orientation?
108. Is company property (credit cards, I.D., Keys, PCs) retrieved during exit interviews?
Comments
Emergency Procedures
109. Do you have a current bomb threat procedure?
110. Who implements it (searches area)?
111. Does the procedure include a checklist for the switchboard operator?
112. Is there a contingency plan for acts of violence?
113. Does the site have and up-to-date strike plan?
114. If personnel are required to work alone, are they periodically checked?
115. a. Identify the most critical areas on the site, the disruption of which could cause the plant to shut down.
b. Have any steps been taken to protect or at least alarm these areas against unauthorized entry or trespass?
116. Has an individual been identified whose job it will be to interface with the media in an emergency/disaster situation?
Comment
Electronic Information/Data Security
117. Has the site received a copy of Electronic Information Security (ELIS) standards? Are you working toward complete implementation?

118. Does a member of management review computer audit trails for evidence of hacking attempts and /or improper use of DP facilities by employees? Has anyone been terminated for abuse/improper use of data processing function/systems since the last survey?
119. Are records kept that will ensure that a person cannot clear a site (transfer, etc.,) with company property (PC, etc.,) in his/her possession?
120.
 - a. Are site employees aware of rules/limitations relative to reproducing copyrighted or licensed software?
 - b. Have you reviewed all PCs to insure all software is covered by appropriate licenses?
 - c. Are all personnel aware of the prohibitions against introducing outside (possibly contaminated) software into company systems?
121. Is physical access to data center restricted? Locked when not in use? Visited by patrolling guards?
122.
 - a. Are terminated employees immediately separated from electronic information?
 - b. Are their passwords/access ability invalidated?
123. Is tape library maintained physically separate from machine room?
124. Are laptop PCs locked in cabinets/closets when not in use? Are they branded/marked?
125. Are users aware of good electronic information security practices and the ramifications of not following them? Do users know where to go for help?
126. Are passwords checked for conformity with ELIS Standards regarding structure, minimum length, and expiration? Do users write down their passwords or share them with other users?
127. Have all critical applications been included in a disaster recovery plan and has that plan been tested? Do PC owners back up their data on a regular basis consistent with the value of their data?
128. Do users leave their terminals/PCs "in session" while they are out of the office? Is there confidential information left on the screen?
129. Do travelers leave portable PCs unattended in their hotel rooms? Is confidential information displayed on the screen of portable PCs in public locations?
130. Do application programmers (those who maintain/change an application's source code) have the system access to install revised code in a production environment?
131. Do users of cellular phones discuss confidential information on them? Do users access their voice mail via cellular phone?
132. Are requests for E-mail accounts on company computers for non-employees evaluated for suitability of MCI mail instead? Are accounts for non-employees on company computers documented using ELIS Form 0002?
133. Are computer rooms, telecom rooms, wiring closets, PBX rooms, etc., locked at all times? Are desktop computing systems protected from physical removal?
134. Are all electronic documents older than three years destroyed? Are documents classified other than for "Internal Use Only" marked with the proper classification?
Comments
135. What overall security improvements do you feel could be made at this location? What would you like to see done here to enhance security?
136. What can we in corporate security do to help you in the security field?