PG&E Security Control CONFIDENTIAL NOT FOR EXTERNAL DISTRIBUTION

SUBJECT: Access Control Alarms

TITLE: Response to Access Control Alarms

EFFECTIVE: March 16, 2009
June 21, 2012

FOR USE BY: General Office (GO) Security Control and Fairfield Security Control (FSC) Personnel

SUMMARY: Procedure for Security Control response to alarms from the AMAG Access Control System

I. Alarms

A. Generation of alarms:

1. An alarm is generated when an alarmed door is
   a. Opened by means other than an access card,
   b. Propped open or held open too long.
   d. Unauthorized entry had occurred.

II. Response to Alarms

A. Security Control personnel will monitor the AMAG access control system for alarms at unattended sites and will immediately advise mobile security personnel, if applicable, of any alarms received.

1. Mobile or foot patrols will respond, if available, and investigate the reason for the alarms.

2. FSC CCTV surveillance or for GO site contact(s) notification should be initiated if security guard dispatch is not feasible.

3. If there is a security infraction, Security Control personnel will contact the site Responsible Party or their secondary and/or on-call PG&E Corporate Security Department (CSD) Area Investigator will be contacted. If applicable, law enforcement will be notified.

4. If an alarm is received from an alarmed perimeter door, the area shall be assessed via cameras, if available, or investigated / searched by the on-duty security officer, on s personnel, or designated site responders. If a door is found to have been forcibly op or found to be unsecured, indicating that unauthorized entry into the building may hav been made, the GO/FSC will follow site specific contact call listing and the on-call C Area Investigator will be advised. If necessary, local law enforcement will be notified and a search of the building will be conducted.

5. If there is any security infraction (i.e. trespassing or theft) involving a non-emplo contractor reported to the FSC personnel, local law enforcement will be notified and a report of the incident will be made.

6. Four or more unauthorized attempts indications under one minute duration (due to invalid card or wrong PIN), forced door, expired card, or entrant is at non-programme door -
area is to be checked visually or in person and contact made with site Responsible Par or on-duty supervisor of the area to ascertain if entry was made. SC personnel will m entry in daily journal as well as fill in the Alarm Checklist with type of alarm, time response.

7. If there is an unauthorized entry into a NERC site, after notifying law enforcement an the site contact(s), the following steps should occur to check the internal ESP (Electr Security Perimeter) within the NERC site to determine possible tampering:

- Contact the TCC to report a potential cyber event and request that they check the sit IT network (i.e., strange system operations or computers malfunctioning).

- Contact the TOC (425/973-9490 or Company 8-223-9490) to be alert for any electric systems fluctuations or malfunction.

- Immediately check access control logs to determine any unusual activity in the last hours.

- Notify the SC Supervisor who will gather the pertinent data and contact CSD

8. CSD (8-223-6920 or 415/973-6920) will be kept appraised of all security violations. (Security Control personnel will complete an incident report for any security violation)

9. Should CSD not be available (i.e., non-business hours), the on-call CSD Area Investigator
will be advised of the situation.

III. The AMAG system has alarms in place requiring specific response from Security Control personnel.

A. Tamper Alarm

1. The on duty SC Operator (SCO) will check with the area Corp. Real Estate*, lead building mechanics to ascertain if any work is being performed at the site, prior to dispatching a Security Officer, if available, and determine the cause for this alarm. Notification to site Responsible Party, CSD on-call Investigator, and CSD Physical Security management will be made.

2. The Security Alarm vendor will be notified unless otherwise specified by CSD Physical Security management.

3. SC will complete a security Incident Report and brief the next SCO shift if the is still ongoing.

Tamper Alarms may come from the following equipment:

a) Control Panel
b) Node
c) Card Reader
e) Equipment boxes (Hoffman Enclosures)
f) Other tamper alarms

B. A/C Power Failure

1. If any system receives an A/C Power Loss, the SCO will monitor the alarm for approximately 10 minutes to ensure a restoral is received. If a restoral is received, SCO will indicate such in the comment box in AMAG. If a restoral NOT received, the SCO will check with the area Corp. Real Estate*, lead building mechanics to ascertain if any work is being performed at the site, prior to immediate notification to the CSD Physical Security management will be made. The SCO will then note in the comment box in AMAG of all actions taken.

2. CSD respondents will initiate alternate security measures (i.e., hard key entry, security officer placement for access control) if needed, should power restoral be prolonged.

3. SC will complete a security Incident Report and brief the next SCO shift if the is still ongoing.

C. Low Battery

1. The SCO will notify CSD Physical Security management upon receipt of this alarm.

2. The responsible Line of Business will be notified so that a Service Tag can be issued the FMC for the security alarm vendor to be notified unless otherwise specified by the contacted CSD Physical Security management

3. SC will complete a security Incident Report and brief the next SCO shift if the is still ongoing.

D. Communications Failure

1. If any system receives a Communications Failure alarm (no connection to the remote site), the SCO will monitor the alarm for approximately 10 minutes to ensure a restoral received. If a restoral is received, the SCO will indicate such in the comment box in AMAG If a restoral NOT received, the SCO will check with the TCC to ascertain if any work is being performed at the site, .The SCO will notify CSD Physical Security management upon receipt of this alarm.

2. In the event a restoral is not received for communication loss alarm, CSD Physical Security management will request that the TCC be notified (223-9000, Option 3) and a repair ticket will be issued.

3. The security alarm vendor will be notified during normal business hours unless otherwise specified by CSD Physical Security management if needed.

3. SC will complete a security Incident Report and brief the next SCO shift if the incident still ongoing.

E. Node Time Out Alarm

1. If any system receives a Communications Failure alarm indicating a Node Timed Out indication (no connection to the remote site), the SCO will monitor the alarm for approximately 1 hour to ensure a restoral is received. If a restoral is received, the will indicate such in the comment box in AMAG If a restoral is NOT received, the SCO will check with the TCC to ascertain if any work is being performed at the site that would effect the communication path to the site. The SCO will notify FSC Supervisor when Node outage is greater than 2 hours

2. Node loss could be due to:

a) Loss of a communication path
b) Loss of a Wireless Connection
c) AC power failure
d) Loss of a Network Router Port (Port timed out/Locked out due to errors)
e) Network cable unplugged

3. FSC Supervisor to contact site contact(s) to verify if electrical or other work done at site to cause disruption

4. SC will complete a security Incident Report and brief the next SCO shift if the incident is still ongoing.

F. Glass Break Alarms

1. Glass Break alarms are considered as "Burglary". In the event of one of these alarms, they should be checked to determine if they are actual or nuance alarms. For Manned facilities, SCO should contact the facility and ascertain if the alarm is valid, if no response to the manned facility, you should consider the alarm valid and take appropriate action. Should tl alarm be determined to be a nuance alarm, no action should be taken other than log the eve

For unmanned facilities, the SCO should contact the facility responsible person and determ if there is any indication of work in progress, if the indication is that no work is in pr this alarm should be taken as an actual alarm and appropriate action should be taken.

G. Panic Alarms

1. A Panic Alarm is an indication that someone is under "Duress" at a facility and has presse the Panic Alarm button. When this alarm is received, the SCO should contact the facility a ascertain if the alarm is valid, If no response to the manned facility, you should conside alarm valid and take appropriate action. (Call the site supervisor and contact the Corp. Security On-Call)

There are no Panic Alarm in unmanned facilities.

H. Trouble Log

1. All equipment failures, including communications failures, shall be logged in the trouble log for tracking and restoral.

*This could be CRE, Substation Maintenance (TSM&C), Gas Maintenance or Generation/Hydro Maintenance, depending on the monitored site.