PHILADELPHIA POLICE DEPARTMENT DIRECTIVE 7.10

Issued Date: 09-19-07	Effective Date: 09-19-07	Updated Date: 05-11-12

SUBJECT: THE CORPORATE EMERGENCY ACCESS SYSTEM (CEAS)

1. POLICY

A. The policy of the Police Department is to assist the community and protect human life. During large-scale emergencies and certain planned events, access to area(s) of the City may be restricted. The City of Philadelphia's Mayor and Managing Director have authorized the use of the Corporate Emergency Access System (CEAS) to expedite recovery and minimize economic impact to private organizations and the business community. CEAS allows employees deemed critical by the private organization or business they work for, to gain access to restricted areas by using a secure identification card when those area(s) can be entered.

2. PURPOSE

A. CEAS is being adopted to expedite recovery and minimize economic impact to private organizations and the business community during a large-scale emergency and certain planned events that restrict normal access to an area.

B. The implementation of CEAS was done in partnership with the Business Network of Emergency Resources (BNET), the City of Philadelphia's Managing Director's Office Office of Emergency Management (OEM), Philadelphia Police Department, and members of the corporate community.

C. CEAS is activated by the Mayor of the City of Philadelphia (or other designated official.)

D. Once activated, individuals holding CEAS credentials and essential service providers will be permitted access into restricted area(s) when those areas can be entered by either:

1. Presenting a CEAS credential, or

2. Presenting an organization-issued identification card from a pre-approved Exempt Organization and demonstrating a legitimate reason to enter the restricted area.

3. PROCEDURE

A. When the CEAS program is activated, the nature of the activation will be announced by the City of Philadelphia's Managing Director's Office - Office of Emergency Management.

B. Upon activation, the duty Chief Inspector will ensure that the provisions of Directive 4.6 entitled "Fire, Disaster, Catastrophes and Other Emergencies Involving Joint Action of Service Department" are implemented.

C. The Police and Fire Departments and the Managing Director's Office - Office of Emergency Management will:

1. Identify the boundaries of the Restricted Area.

2. Determine if the Restricted Area can be safely entered.

3. Identify Access Point(s) that CEAS Cardholders must pass through to gain access.

4. Determine the authorized Access Level

REDACTED - LAW ENFORCEMENT SENSITIVE

5. Ensure sufficient police personnel to screen Cardholders at the Access Point(s).

6. Continually monitor conditions and adjust access level as warranted.

7. Ensure the proper notification of these decisions.

4. ACCESS PROCEDURES

A. Established CEAS Access Point(s)

1. CEAS Access Points will be staffed by police personnel including a supervisor.

2. Entry / Exit Logs will be maintained by police personnel and forwarded to the Homeland Security Unit after the event.

a. Access Procedures for **CEAS Cardholders**

1) Credentials cannot be loaned or given to another employee.

2) Officers will request to inspect the CEAS credential and another form of picture identification (organization ID or government issued ID) from persons requesting access.

3) Officers will physically inspect the individual's CEAS credential before permitting access by:

(a) Inspecting for the presence of the CEAS hologram imbedded in the card laminate by tilting the card in the light to expose the image (Appendix 'A').

(b) Verifying the identity of the cardholder through the photo on the front side of the card and cross-referencing to organization or government issued ID.

(c) Verifying that the cardholder's worksite is within the restricted area.

(1) Standard Card – Verify that the cardholder's worksite is within the restricted area by inspecting the address on the front of the card.

(2) Multi-Facility Card – Verify that the cardholder's worksite is within the restricted area by means of verbal inquiry. Attempt to confirm that named facility is within restricted area.

(3) All Access Card – Verify that the cardholder's worksite is within the restricted area by means of verbal inquiry. Attempt to confirm that named facility is within restricted area.

(d) Verifying that the Access Level of the cardholder coincides with the level announced by the City.

(e) Checking the expiration date. All expired credentials will be confiscated, reported, and forwarded to the Managing Director's Office - Office of Emergency Management.

(f) Cardholder will be informed that for safety reasons he/she must exit through the same access point.

(g) CEAS cardholders may NOT escort non CEAS cardholders through access points.

b. Access Procedures for **Employees of the following Exempt Organizations (the following organizations are Exempt from holding a CEAS credential to gain entry to restricted area(s):**

*1

REDACTED - LAW ENFORCEMENT SENSITIVE

REDACTED - LAW ENFORCEMENT SENSITIVE

c. Officers will request inspection of the individual's organization-issued ID and another form of picture identification (government issued ID) from persons requesting access.

d. Officers will physically inspect the individual's organization-issued ID card before permitting access by:

1) Verifying that the individual's organization is on the list of pre-approved Exempt Organizations.

2) Manually cross referencing the individual's ID to official sample organization ID provided on key-ring to ensure correct size, design, format, texture, etc. (Appendix "A")

3) Verifying the identity of the cardholder through the photo on the front side of the card.

4) Verifying that the cardholder's worksite is within the restricted area. Confirm by verbal inquiry, review of work-order, etc.

5) Checking the expiration date of organization ID (if applicable).

6) Cardholder will be informed that for safety reasons he/she must exit through the same access point. Employees of exempt organizations may **NOT** escort non exempt employees through access points.

3. If card/cardholder fails to meet the above requirements access will be denied.

4. Any challenges to the restricted admittance will be referred to the Police Command Post for resolution. Until resolved by the Incident Commander, admittance will be denied.

5. Officers are to use their discretion when allowing access to CEAS cardholders. If specific conditions warrant a higher level of restriction than announced, the Officer enforcing the access restrictions may enforce the restrictions at a higher level for safety reasons. A police supervisor will be notified if not on the scene.

B. Levels of Corporate Access

1. Each CEAS credential designates an access level. At the time of the emergency, the Managing Director or his/her designee will announce what access level will be authorized for travel into the affected area.

2. Access Level: There are five (5) access levels in the CEAS Program.

REDACTED - LAW ENFORCEMENT SENSITIVE

RELATED PROCEDURES	Directive 4.6,	Fire, Disaster, Catastrophes and Other Emergencies Involving Joint Action of Service Department

BY COMMAND OF THE POLICE COMMISSIONER

FOOTNOTE	GENERAL#	DATE SENT	REMARKS
*1	5126	05-11-12	Change

PHILADELPHIA POLICE DEPARTMENT DIRECTIVE 7.10

APPENDIX "A"

Issued Date: 09-19-07	Effective Date: 09-19-07	Updated Date:

SUBJECT: REDACTED - LAW ENFORCEMENT SENSITIVE

REDACTED - LAW ENFORCEMENT SENSITIVE

BY COMMAND OF THE POLICE COMMISSIONER