

---

**Policy Number:** 301.045  
**Title:** Perimeter Management  
**Effective Date:** 7/17/18

---

**PURPOSE:** To outline areas related to correctional facility perimeters so facilities may maintain specific operating procedures for those areas.

**APPLICABILITY:** All facilities

**DEFINITIONS:**

Drone – as defined in Policy 301.032, “Drone Intrusion.”

Facility tunnel – below-ground passageway linking one facility location to another. The facility must determine use and access authorization for each.

Unauthorized use – as defined in Policy 301.032, “Drone Intrusion.”

**PROCEDURES:**

- A. Perimeter security
1. Zones (e.g., camera, motion detector, etc.)
    - a) Signage;
    - b) Zone maps; and
      - (1) Storage of maps;
      - (2) Maintenance/updating responsibilities;
      - (3) Authorized use/access to maps; and
    - c) Nuisance fence/public signage.
  2. Security patrols
    - a) Training (documented in the electronic training management system);
    - b) Staff levels, relief, emergency staffing; and
    - c) Frequency of patrols
      - (1) Daytime/nighttime;
      - (2) Adverse weather (e.g., fog, snow, etc.); and
      - (3) Emergency/special situations.
  3. Perimeter inspections/monitoring (documented by the staff performing them)
    - a) System testing (e.g., method/frequency/documentation);
    - b) Sight lines;
      - (1) Vegetation control (e.g., trees/brush/tall grass);
      - (2) Trash/debris in perimeter; and
      - (3) Unintentional scaling device control near perimeter;
        - (a) Fixed (e.g., light poles, flag poles, etc.); and
        - (b) Movable (e.g., boxes, barrels, hoses, chains, ropes, etc.);
    - c) Manhole covers/storm drains; and
    - d) Detection of incipient tunnels/breaches in perimeter.

4. Identifying and responding to the unauthorized use of drones (refer to Policy 301.032, "Drone Intrusion")
  - a) Observance of an unauthorized drone within or above the grounds or land controlled by any DOC facility.
  - b) Evacuation of offenders from all outdoor areas and notification of appropriate staff (e.g. perimeter officer(s), officer of the day (OD), office of special investigations (OSI), law enforcement, etc.).
  - c) Securing the area beneath where the drone was observed and search/securing contraband.
  - d) Documentation of any drone incident/encounter by staff directly involved.
  
5. Unauthorized persons/object/vehicle on grounds (also refer to Policy 301.081, "Use of Force and Restraints - Adult," Policy 301.079, "Juvenile Restrictive Procedures Plan," and Policy 301.180, "Terrorist Incident Response – Facilities").
  - a) Trespassers;
  - b) Curiosity seekers/photographers;
  - c) News media; and
  - d) Threatening/suspicious individuals.

B. Perimeter lighting

1. Lighting controls (e.g., power switches, wiring, circuit breakers, etc.)
  - a) Location;
  - b) Access authorization/access control devices; and
  - c) Automatic controls – activation/deactivation/maintenance;
2. Special lighting conditions – adverse weather (e.g., fog, etc.);
3. Determination of compatibility with cameras and other security systems;
4. Inspection/nightly lighting checks/maintenance (documented by the staff performing them); and
5. Backup systems (power outage).

C. Perimeter access points (main, secondary/emergency, vehicle gates)

Vehicles within a facility secure perimeter must be kept secure and are subject to inspection for contraband (with inspections documented by the staff performing them).

1. Staffing levels/training (documented in the electronic training management system);
2. Gate operation procedure (electronic/manual);
3. Admittance authorization/identification (ID) cards;
4. Security surveillance (e.g., mirrors, intercom, cameras);
5. Searches/inspection – metal detection (documented by the staff performing the inspections);
  - a) People (staff/visitors/belongings);
  - b) Incoming/outgoing deliveries (e.g., laundry, trash, supplies, etc.); and
  - c) Procedures for admittance of large groups;

6. Documentation/logs
  - a) Visitors;
  - b) Staff in/out of facility; and
  - c) List of authorized individuals;
7. Procedures for compromised/inoperative entrance;
8. Sallyport (e.g., person limits, interlock procedures);
9. Use and access authorization for secondary/emergency access points;
10. Weapon locker/storage for visiting law enforcement officials;
11. Emergency vehicle entry
  - a) Authorization for entry;
  - b) Inspection (entrance/exit) (documented by the staff performing the inspection); and
  - c) Escort/security while in secure perimeter;
12. Pedestrian traffic through vehicle gates;
13. Process to secure deliveries/hazardous materials (e.g., ammunition, flammables, etc.); and
14. Inspections/testing (electronic/manual)
  - a) Frequency;
  - b) Staff responsible; and
  - c) Documentation by the staff performing them.

D. Facility tunnels

1. Maps – location and authorized use;
2. Security and access control (access control devices);
3. Security systems – cameras/alarms monitoring;
4. Radio communications/backup methods;
5. Inspection schedule/responsibility and documentation (e.g., maintenance, free of obstructions, etc.);
6. Special hazards;
7. Backup lighting/power;
8. Fire protection; and
9. Security level and access authorization.

E. Master control

1. Access authorization to master control;

2. Staffing levels – routine/peak/emergency;
3. Staff training (documented in the electronic training management system);
4. Armory regulations/access (if applicable);
5. Information
  - a) List of all firearms-qualified staff;
  - b) Emergency phone numbers/call list; and
  - c) Emergency plans;
6. Equipment checkout logs – issuance procedures
  - a) Radio;
  - b) Body alarms; and
  - c) Security equipment;
7. Checks/inspection of control panel, electrical equipment, life safety systems, security equipment (documented by the staff performing them);
8. Maintenance/housekeeping in master control;
9. Power failure procedure – manual gate operation/access;
10. Contingency plans;
  - a) Outside assault; and
  - b) Loss of master control (fire, riot, etc.); and
11. Staff in master control (secondary access methods).

**INTERNAL CONTROLS:**

- A. Perimeter inspections are documented by the staff performing them.
- B. All training is documented in the electronic training management system.

**ACA STANDARDS:** 4-4171, 4-4172, 1-ABC-2G-02, 1-ABC-2G-03

**REFERENCES:** [Policy 301.081, “Use of Force and Restraints - Adult”](#)  
[Policy 301.079, “Juvenile Restrictive Procedures Plan”](#)  
[Policy 301.180, “Terrorist Incident Response – Facilities”](#)  
[Policy 301.010, “Searches”](#)  
[Division Directive 300.032, “Admittance Authorization to Adult Facilities”](#)  
[Division Directive 300.030, “Tours – Adult Facilities”](#)  
[Division Directive 300.033, “Tours – Juvenile Facilities”](#)  
[Policy 301.050, “Security Systems Inspection \(SSI\)”](#)  
[Policy 301.030, “Contraband”](#)  
[Policy 300.400, “Physical Plant Maintenance”](#)  
[Policy 301.100, “Weapons Control”](#)  
[Policy 301.140, “Incident Command System”](#)  
[Policy 301.160, “Emergency Plans”](#)  
[Policy 301.060, “Access Control Devices”](#)

[Policy 301.032, "Drone Intrusion"](#)

**REPLACES:** Division Directive 301.045, "Perimeter Management," 7/26/16.  
All facility policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

**APPROVALS:**

Deputy Commissioner, Facility Services

Deputy Commissioner, Community Services

Assistant Commissioner, Facility Services

Assistant Commissioner, Operations Support