

### Employee/Visitor Identification

<b>Term</b>	<b>Definition/Description</b>
<b>VISITOR CONTROL/SECURITY SYSTEM</b>	Visitors should be readily apparent in Level I facilities. Other facilities may ask visitors to sign-in with a receptionist or guard, or require an escort, or formal identification/badge.
<b>VISITOR ID ACCOUNTABILITY SYSTEM</b>	Stringent methods of control over visitor badges will ensure that visitors wearing badges have been screened and are authorized to be at the facility during the appropriate time frame.
<b>ESTABLISH ID ISSUING AUTHORITY</b>	Develop procedures and establish authority for issuing employee and visitor IDs.

### Utilities

<b>Term</b>	<b>Definition/Description</b>
<b>PREVENT UNAUTHORIZED ACCESS TO UTILITY AREAS</b>	Smaller facilities may not have control over utility access, or locations of utility areas. Where possible, assure that utility areas are secure and that only authorized personnel can gain entry.
<b>PROVIDE EMERGENCY POWER TO CRITICAL SYSTEMS</b>	Tenant agency is responsible for determining which computer and communication systems require back-up power. All alarm systems, CCTV monitoring devices, fire detection systems, entry control devices, etc. require emergency power sources. (ALARM SYSTEMS, RADIO COMMUNICATIONS, COMPUTER FACILITIES, ETC.)

### Occupant Emergency Plans

<b>Term</b>	<b>Definition/Description</b>
<b>EXAMINE OCCUPANT EMERGENCY PLAN (OEP) AND CONTINGENCY PROCEDURES BASED ON THREATS</b>	Review and update current OEP procedures for thoroughness. OEPs should reflect the current security climate.