



DEPARTMENT OF THE ARMY  
US ARMY INSTALLATION MANAGEMENT COMMAND  
HEADQUARTERS, UNITED STATES ARMY GARRISON DAEGU  
UNIT #15746  
APO AP 96218-5746

3 SEP 2013

IMDA-PLO

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: US Army Garrison (USAG) Daegu Policy Letter #34, Operations Security (OPSEC)

1. This policy, effective immediately, remains in effect until rescinded or superseded.
2. References:
  - a. DoD Directive 5205.02E, DoD Operations Security Program, 20 Jun 12.
  - b. Joint Publication 3-13. 3, Operations Security, 4 Jan 12.
  - c. Army Regulation 530-1, Operations Security, 19 Apr 07.
  - d. Army Regulation 381-12, Threat Awareness and Reporting Program, 4 Oct 10.
  - e. Army Regulation 25-55, Freedom of Information Act Program, 1 Nov 97.
  - f. US Forces Korea (USFK) Command Policy Letter #5, Operations Security (OPSEC), 17 Oct 11.
  - g. Army in Korea Regulation 530-1, Operations Security (OPSEC), 9 Jan 10.
  - h. Installation Management Command Operations Security Program, 23 Jan 13.
  - i. AR 360-1, The Army Public Affairs Program, 25 May 11.
3. This policy applies to USAG Daegu Military Members, DoD Civilian Employees, Contractors, Local National Employees, and Family Members.
4. The primary purpose of the OPSEC program is to ensure the Command practices OPSEC to deny critical sensitive information to adversaries. The OPSEC process is a proven means to protect operations and planning information and will support the USAG Daegu mission and operations objectives.
5. Proper use of the OPSEC process will minimize conflicts between operational and security requirements. The OPSEC process requires that each operation be individually analyzed to determine the level of acceptable risk.

IMDA-PLO

SUBJECT: US Army Garrison (USAG) Daegu Policy# 34 Operations Security (OPSEC)

6. Therefore, commanders must actively participate in the program by providing guidance and decisions to ensure continuous and thorough attention by all personnel in order to assure proper protection of critical information and OPSEC indicators. Within USAG Daegu, OPSEC will:

a. Be used to deny enemy intelligence gathering organizations information about friendly capabilities, intentions, and operations. We will accomplish this by controlling or protecting indicators associated with planning and conducting military operations.

b. Be integrated into the planning and execution phases of all military operations.

c. Include frequent evaluations and identification of Essential Elements of Friendly Information (EEFI). Each OPLAN should be evaluated and refined annually in order to develop critical information specific to that plan.

d. Be a consideration in the day-to-day operations of each directorate.

7. Securing classified information is well understood and enforced. However, everyone must understand that sensitive unclassified information must also be protected and denied to our adversaries. Small bits of information can be fused together to reveal a larger picture.

8. Each Soldier, DoD Civilian employee and Contractor at all levels, must protect both classified and sensitive unclassified information that could potentially be exploited by our adversaries. We must make OPSEC a priority and integrate OPSEC practices into our daily activities.

9. The successful enforcement of OPSEC procedures will prevent serious injury and possibly death of USAG Daegu members; damage to our key infrastructures; or loss of critical technological capabilities.

10. Military personnel who fail to comply with these orders, directives, or policies may be punished as violations of a lawful order under Article 92 of the Uniform Code of Military Justice (UCMJ) or under other disciplinary, administrative, or other actions as applicable.

11. Personnel not subject to the UCMJ who fail to protect critical and sensitive information from unauthorized disclosure may be subject to administrative, disciplinary, contractual, or criminal action.

IMDA-PLO

SUBJECT: US Army Garrison (USAG) Daegu Policy# 34 Operations Security (OPSEC)

12. DOCUMENT SECURITY:

- a. Managers will establish and enforce a "shred as you go policy."
- b. 100% of all Unclassified Work Related Documents, i.e., "Personally Identifiable Information" (PII), "For Official Use Only" (FOUO), "Sensitive But Unclassified" (SBU), "Limited Official Use Information", "Law Enforcement Sensitive", "Sensitive Information" in accordance with the Computer Security Act of 1987, and information contained in technical documents must be shredded prior to their disposal.
- c. Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties.
- d. PII and FOUO spot checks of trash bins, garbage cans, recycling plant, etc., are conducted by 524th MI and garrison OPSEC personnel.
- e. For offices without a shredder, utilize the USAG Daegu Shred Facility, Cp Henry, Building # 1624, Tuesday & Thursday, 0900-1200 and 1300-1630. The Shred Facility is managed by Mr. Kim, Kyong T., 768-7020, kyong.t.kim6.in@mail.mil.
- f. In the unlikely event the USAG Daegu Shred Facility is unavailable for more than 30-days, disposal of bulk paper products through commercial shredding service is authorized, provided regulatory steps are taken to ensure no work related documents identified in para 12b. above, are provided to commercial sources for destruction.
- g. Other documents which are no longer required for operational purposes will be disposed of in accordance with the provisions of the Federal Records Act (44 USC chapters 21 and 33) as implemented by AR 25-400-2.

13. Any questions regarding this policy must be addressed to the Commander, USAG Daegu, ATTN: DPTMS OPSEC Officer, at 768-7737 or 765-7898.

  
JIM M. BRADFORD  
COL, IN  
Commanding

DISTRIBUTION:

A