



DEPARTMENT OF THE ARMY  
HEADQUARTERS 2ND INFANTRY DIVISION  
UNIT # 15041  
APO AP 96258-5041

REPLY TO  
ATTENTION OF

EAID-CG

TO AUG. 2012.

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

1. References:

- a. AR 380-5, Department of the Army Information Security Program, 29 Sep 00.
- b. Department of the Army, Office of Information Assurance and Compliance Best Business Practice (BBP), 03-VI-O-0001, Classified Information Spillage on Information Systems, version 1.5, 20 Apr 07.
- c. Department of the Army, Office of Information Assurance and Compliance Best Business Practice (BBP), 06-VI-M-0009, Network Incident Classification, version 1.0, 22 Sep 06.
- d. AR 190-45, Law Enforcement Reporting, 30 Mar 07.
- e. AR 25-2, Information Assurance, 24 OCT 2007, with RAR 001, 23 Mar 09.
- f. AR 25-1, Army Knowledge Management & Information Technology, 4 Dec 08.
- g. 2ID Command Policy Letter #6-1, Information Assurance, 28 Feb 12.
- h. 1<sup>st</sup> Signal Brigade, Army in Korea UNCLASSIFIED / CLASSIFIED LandWarNet (AKULWN/AKCLWN), Incident Response Policy, 1 Nov 11.
- i. DoD Data Spill Procedures Guide for BlackBerry Smartphones, 24 Mar 11.
- j. ALARACT 079/2007, Handling of Information Spillage Incidents, 20 Apr 07.

2. Applicability. This policy applies to all personnel assigned, attached, or under operational control of 2ID, including Department of Defense (DoD) civilian employees, invited contractors, and technical representatives.

3. Definition. An Unauthorized Disclosure of Classified Information (UDCI) is a serious security incident that occurs when classified information is processed or posted on an unclassified information system or on a classified information system being operated at a lower level than the classification assigned to the information or data.

EAID-CG

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

4. Background. The severity of an unauthorized disclosure is greatly compounded when classified information is included in or attached to an e-mail message and transmitted to multiple addressees across a network not authorized to transport that level of information, mandating an immediate, time consuming, and costly sanitization and response process. Most UDCI incidents are accidental and occur when personnel are stressed to meet suspenses and fail to adequately review information extracted from classified sources.

5. Purpose. This policy is intended to enhance leader awareness of the serious nature of UDCI occurrence and provides notification, response, and corrective procedures in the event of a disclosure incident. Proper reporting, coordination, and clean up of an unauthorized disclosure is critical to limiting the compromise of classified information.

6. Policy. All personnel cleared to access classified information are obligated to safeguard that information and comply with the Army Information Security Program. They must be knowledgeable of the processes and procedures for assigning security classifications, and for marking, storing, and transmitting classified information. Personnel who believe they have received classified information on an unclassified information system (IS) will immediately notify their commander, unit security manager, and IA Support Officer (IASO)/Information Management Officer (IMO). IAW 2ID Command Policy Letter #6-1, para 3.d., Commanders will ensure notification of the 2ID Information Assurance Manager (IAM) for all IA incidents.

7. Command Responsibility.

a. All Commanders will ensure administrative, physical, and technical safeguards to protect classified material against disclosure, unauthorized access, or misuse. Commanders will also publish local procedures for managing unauthorized disclosures, and appoint an official to oversee and manage the incident reporting and notification process. Commanders must plan and practice sanitizing and UDCI implementation measures **before** an incident occurs, incorporating current policy and procedures outlined in other applicable regulations. Activity Security Managers/IASOs/IMOs will ensure that all UDCI incident response procedures are included in their organization's annual security training requirements in accordance with this policy.

b. Upon notification of a suspected UDCI, ensure completion of the Division UDCI Immediate Response Procedures outlined in Paragraph 9, which will be executed concurrently with requirements detailed in items 7(d) through (j) below.

c. The O-6 Memorandum. The UDCI Validation Memorandum is a mandatory document which will be signed by the first O-6 in the originating organization's chain of command upon determination by the S2 / SSO that the data is classified at a level higher than the classification of the impacted network or IS. This memorandum is required IAW 1<sup>st</sup> SIG BDE Incident Response Policy, para 6.1, and is intended for notification purposes to provide the Area NEC and K-TNOSC with a timely report as to the unit's determination of UDCI occurrence and in order to initiate network and IS remediation, isolation, and containment actions. It is not intended to initiate adverse personnel actions.

d. Conduct a preliminary investigation IAW AR 380-5, chapter 10, to determine the level of

EAID-CG

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

compromise, including a potential damage assessment of the loss to national security (if applicable). The organization originating the spillage is the lead agency responsible for all actions.

e. Ensure that all BlackBerry smartphones, Personal Data Assistants (PDA), wireless devices, or text messaging devices that have been contaminated with classified information are brought under immediate control and accountability of the IASO until sanitization methods are developed and approved by the Department of the Army (DA). Wipe or destroy BlackBerry smartphones IAW criteria established in DoD Data Spill Procedures Guide. Prior to any destruction, check for updated PDA policy at <https://powhatan.iije.disa.mil/stigs> and at [https://www.milsuite.mil/login/Login?goto=https%3A%2F%2Fwww.milsuite.mil%3A443%2Fwiki%2FBest\\_Business\\_Practices](https://www.milsuite.mil/login/Login?goto=https%3A%2F%2Fwww.milsuite.mil%3A443%2Fwiki%2FBest_Business_Practices).

f. Personally-owned devices that receive official communications from official Army sources (i.e. AKO e-mail), or devices that are used to access protected information are also vulnerable to UDCI incidents. If any personally-owned devices are subjected to an UDCI incident, ensure the devices are surrendered to Army investigators or activities until sanitization methods are developed and approved by DA. Possession of protected or classified information on personal devices is prohibited.

g. When a security incident is confirmed as an UDCI, Commanders and Supervisors at all levels will ensure that appropriate remedial actions are taken and hold violators accountable. Sanctions established IAW 2ID Command Policy Letter #6-1, para 4.c., including the immediate suspension of network access and privileges, will apply if an UDCI occurs as a result of negligence, carelessness, non-compliance with regulatory requirements, or failure to follow established procedures. Privileges will not be restored until offense memorandums have been received and corrective actions have been verified by the 2ID IAM. Additionally, unit commanders will, at a minimum, initiate an informal AR 15-6 inquiry within 72 hours of a confirmed UDCI and report findings to the 2ID SSO and IAM upon completion. All attempts should be made to complete the investigation within seven working days. Exceptions to this suspense may be granted on a case by case basis by the 2ID SSO.

h. Prepare a final close-out report IAW AR 380-5 documenting all activity, notifications, and actions taken during the UDCI incident. The Immediate Action Checklist (IAC) (Enclosure 3) and the appropriate Response Checklist (Enclosure 4 or Enclosure 5) will be included in the final report. All personnel involved with identification, purging, rebuilding, and verification will be debriefed and sign applicable Non-Disclosure Agreements if required.

i. Implement measures to reduce the potential of reoccurrence through additional training and technical configurations. If the organizational process that generated the UDCI involved is relevant to another process, such as transferring data, this process will be terminated until additional training and safeguards are implemented to preclude another unauthorized disclosure incident.

j. A serious incident report (SIR) will be generated and reported per AR 190-45.  
**NOTE:** *If the UDCI is TS, SCI, SAP, or Codeword; see ALARACT 079/2007. This ALARACT contains a list of references to address UDCIs of this nature. Only personnel with the same level of clearance are authorized to perform the cleanup of the affected systems. If this occurs contact the Command Group for guidance.*

EAID-CG

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

8. IASO/IMO/SA Responsibility. Technical support personnel will ensure completion of Technical Remediation and Removal Procedures listed in Enclosure 6.
9. 2ID UDCI Immediate Response Procedures (IRP). The procedural checklist in Enclosure 1 will be executed upon discovery or notification of a potential unauthorized disclosure of classified information. UDCIs are coordinated through the S2/SSO, the S6 IAM, and the 2ID IAM. Communication of UDCI incidents are via SIPR and secure phones.
10. Emergency Response Points of Contact. Refer to Enclosure 7 for a list of emergency contacts.
11. Expiration. Policy Letter #6-2 is effective immediately and remains in effect until rescinded or superseded.
12. Proponent for this policy letter is 2ID G6, 732-6081.



EDWARD C. CARDON  
Major General USA  
Commanding

7 Encls

- 1 - Immediate Response Procedures
- 2 - Unit Information Sheet for UDCI Incident
- 3 - Immediate Action Checklist
- 4 - Time Based UDCI Incident Response Form
- 5 - Content UDCI Incident Response Form
- 6 - Technical Remediation and Removal Procedures
- 7 - Emergency Response Points of Contact

DISTRIBUTION:

A

## Enclosure 1: IMMEDIATE RESPONSE PROCEDURES

- a. \_\_\_\_\_ Identify affected systems and disconnect network connections. **DO NOT TURN OFF THE IS.**
- b. \_\_\_\_\_ Isolate and guard the affected IS(s).
- c. \_\_\_\_\_ Contact the Security Manager / S2 and S6 IASO/IAM.
- d. \_\_\_\_\_ Restrict physical access to the IS or media until your Security Manager or IAM/IASO provides guidance.
- e. \_\_\_\_\_ Identify impacted users.
- f. \_\_\_\_\_ Complete initial Unit Information and Immediate Action Checklists.
- g. \_\_\_\_\_ Provide Immediate Action Checklist to designated individuals (i.e. SA/IASO/IAM/SSO).
- h. \_\_\_\_\_ The S2 / Security Manager coordinates with the SSO to determine classification of the data pertaining to the incident through the Original Classification Authority (OCA) as required.
- i. \_\_\_\_\_ If the S2 / SSO determines that the data is classified at a level higher than the classification of the impacted network or IS, prepare an O-6 UDCI Validation Memorandum
- j. \_\_\_\_\_ Notify 1<sup>st</sup> SIG BDE EOC that a UDCI has occurred and more information will be forthcoming.
- k. \_\_\_\_\_ The first O-6 in the chain of command signs the UDCI Validation Memorandum, declaring the incident.
- l. \_\_\_\_\_ Send 5W report to 2ID IAM and Area NEC via SIPR. Depending on severity, the G2, G3, and CofS are informed for situational awareness and guidance as required.
- m. \_\_\_\_\_ Provide the O-6 UDCI Validation Memorandum to the 2ID IAM and Area NEC.
- n. \_\_\_\_\_ S6 System Administrator and IAM complete ARKLANT Incident Reporting Form (<https://8army.korea.army.mil/ia/Incident%20Reponse%20and%20Reporting/ARKLANT%20Incident%20Reporting%20Form.doc>) and forward to 2ID IAM and 1<sup>st</sup> SIG BDE EOC via SIPR.

EAID-CG

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

- o. \_\_\_\_\_ The 2ID IAM notifies 8<sup>th</sup> Army IA and coordinates with 1<sup>st</sup> SIG BDE EOC, the Area NEC, K-TNOSC, and RCERT-K via secure phone and SIPR e-mail message.
- p. \_\_\_\_\_ As required, use Universal Purge Tool (UPT) to purge impacted systems. NEC and K-TNOSC will coordinate purging military exchange accounts.
- q. \_\_\_\_\_ Continue to take instructions from higher.
  
- r. NEVER! Investigate actions on the IS until authorized by Commander or Information Security Personnel
- s. NEVER! Contact any commercial Internet Service Provider (ISP) or ISP account identified in the investigation.
- t. NEVER! Confirm or deny any UDCI or compromise of sensitive or classified information in the public sector.
- u. NEVER! Delay implementation of containment procedures while awaiting notification of key personnel.

EAID-CG

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

## Enclosure 2: **UNIT INFORMATION FOR UDCI INCIDENT**

### POINT OF CONTACT

RANK: \_\_\_\_\_ NAME: \_\_\_\_\_

POSITION: \_\_\_\_\_

EMAIL ADDRESS: \_\_\_\_\_

CONTACT NUMBER: \_\_\_\_\_

### UNIT INFORMATION

UNIT: \_\_\_\_\_

UNIT COMMANDER: \_\_\_\_\_

EMAIL ADDRESS: \_\_\_\_\_

CONTACT NUMBER: \_\_\_\_\_

### INFORMATION ASSURANCE SUPPORT OFFICER

RANK: \_\_\_\_\_ NAME: \_\_\_\_\_

EMAIL ADDRESS: \_\_\_\_\_

CONTACT NUMBER: \_\_\_\_\_

FORMALLY TRAINED? YES  NO

### PHYSICAL LOCATION OF SYSTEM

ROOM \_\_\_\_\_ BUILDING \_\_\_\_\_ INSTALLATION \_\_\_\_\_

### Enclosure 3: IMMEDIATE ACTION CHECKLIST

1. Classification of the System:

- UNCLASSIFIED       SECRET       TOP SECRET       OTHER

2. Was the file marked with classification markings:

- YES (Go to 3)       NO (Go to 4)

3. Classification of data:

- CONFIDENTIAL       SECRET       TOP SECRET       OTHER

Is TS information on unclassified system?

YES – Plan for destruction of all affected media (Go to 17)

NO – You may be authorized to clear or purge affected media (Go to 4)

4. Is Category of Information SPECAT, SAP, SCI, SI, or CODEWORD?

YES – Plan for destruction of all affected media (Go to 17)

NO – You may be authorized to clear or purge affected media (Go to 5)

5. DTG of the message: \_\_\_\_\_ DTG of identification: \_\_\_\_\_

Is difference of DTG less than 2 hours?

YES – Implement time-based clearing actions.

NO – Implement data-based actions to contain and purge

6. How was the classified information distributed/received/identified?

- EMAIL       ATTACHMENT       DESKTOP FILE  
 FILE SERVER FILE       WEB POSTING       REMOVABLE MEDIA

7. Who reported/identified the UDCI?

- ARMY       DOD       OTHER GOVERNMENT AGENCY  
 CONTRACTOR       COMMERCIAL ENTITY

POC NAME: \_\_\_\_\_ CONTACT NUMBER: \_\_\_\_\_

RANK: \_\_\_\_\_ POSITION: \_\_\_\_\_

EMAIL: \_\_\_\_\_

UNIT: \_\_\_\_\_

8. Who distributed the UDCI? (if not reporting agency)

- ARMY                       DOD                       OTHER GOVERNMENT AGENCY  
 CONTRACTOR                       COMMERCIAL ENTITY

Name of sender (FROM): \_\_\_\_\_

Email: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Name of sender (TO): \_\_\_\_\_

Email: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Name of sender (CC): \_\_\_\_\_

Email: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Name of sender (BCC): \_\_\_\_\_

Email: \_\_\_\_\_ Contact Number: \_\_\_\_\_

Original Subject of Message: \_\_\_\_\_

9. Has the subject been changed from original message?                       YES                       NO

If yes, subject of subsequent message(s): \_\_\_\_\_

10. Has the document or file been printed?                       YES                       NO

11. Has the document been saved?                       YES                       NO

Where: \_\_\_\_\_

12. Has the originator been notified?                       YES                       NO

13. Is the originator the lead agency for the UDCI?                       YES                       NO

14. Is the originator the original classification authority (OCA)?                       YES                       NO

EAID-CG

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

15. Has the OCA been contacted?  YES  NO

NAME: \_\_\_\_\_ CONTACT NUMBER: \_\_\_\_\_

RANK: \_\_\_\_\_ POSITION: \_\_\_\_\_

EMAIL: \_\_\_\_\_

UNIT: \_\_\_\_\_

16. Is unauthorized software on a system that substantially increases risk or threat? (IRC, Peer to Peer file sharing applications, etc.)

YES  NO

If yes, CI Investigators must be contacted and all clearing actions cease.

17. Can the OCA downgrade the information?  YES  NO

If YES, to what category or classification? \_\_\_\_\_

If NO, Destruction of all affected media is required.

18. Does downgraded classification or category affect response?

If YES, go to 5.

If NO, Destruction of all affected media is required.

19. SYSTEM IDENTIFICATION:

OS: \_\_\_\_\_ VERSION: \_\_\_\_\_

20. Did you originate the UDCI incident?  YES  NO

If YES, your organization becomes the lead agency for reporting all actions unless OCA takes control of the incident

## Enclosure 4: TIME BASED UDCI INCIDENT RESPONSE

Limit the number of affected systems and collateral damage by immediately disconnecting or isolating all affected system. Emphasis is on urgency versus accuracy with an acceptable risk that data will be removed and inaccessible through normal operational procedures and the system (drive) will be overwritten multiple times during normal operations.

Complete the following for every system:

	USER		SA	
	YES	NO	YES	NO
Identified/notified all "TO" recipients	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identified/notified all "CC" recipients	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identified/notified all "BCC" recipients	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identified all auto process rules on system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from all local systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from file storage areas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from user's mailboxes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from mail queues (sent, draft, deleted, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete messages saved in Personal Folders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Empty "Recycle Bin" folder storage area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Empty "Deleted Items" folder storage area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Empty "Recover Deleted Items" folder storage area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Conduct a search for similar files (i.e. same date/time stamp, word search, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete all identified files from search	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verify that no files were saved to network storage devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete contents of all temporary files/folders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete contents of cached items (i.e. Internet Explorer or Netscape temporary files)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remove all unauthorized files/software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Administrator Actions Only</b>				
Identified all auto process rules on server			<input type="checkbox"/>	<input type="checkbox"/>
Files removed from affected servers and devices			<input type="checkbox"/>	<input type="checkbox"/>
Compact folders or information stores			<input type="checkbox"/>	<input type="checkbox"/>
Defrag the hard drives of all systems			<input type="checkbox"/>	<input type="checkbox"/>
Reboot the system			<input type="checkbox"/>	<input type="checkbox"/>
Record serial number of cleared hardware			<input type="checkbox"/>	<input type="checkbox"/>
Backup tapes/device/storages/drives moved to controlled/classified area			<input type="checkbox"/>	<input type="checkbox"/>

## Enclosure 5: CONTENT UDCI INCIDENT RESPONSE

Concentrate on the deliberate identification and eradication of the data from every affected asset to protect the information, exclusive of operational or economical issues (removal and purging activities exclusively).

Complete the following for every system:

	USER		SA	
	YES	NO	YES	NO
Identified/notified all "TO" recipients	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identified/notified all "CC" recipients	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identified/notified all "BCC" recipients	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Identified all auto process rules on system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from all local systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from file storage areas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from user's mailboxes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete file from mail queues (sent, draft, deleted, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete messages saved in Personal Folders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Empty "Recycle Bin" folder storage area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Empty "Deleted Items" folder storage area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Empty "Recover Deleted Items" folder storage area	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Conduct a search for similar files (i.e. same date/time stamp, word search, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete all identified files from search	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verify that no files were saved to network storage devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete contents of all temporary files/folders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete contents of cached items (i.e. Internet Explorer or Netscape temporary files)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Remove all unauthorized files/software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Administrator Actions Only (in sequence)</b>				
Identified all auto process rules on server			<input type="checkbox"/>	<input type="checkbox"/>
Files removed from affected servers and devices			<input type="checkbox"/>	<input type="checkbox"/>
Use Purge tool to overwrite free space (1x: random)			<input type="checkbox"/>	<input type="checkbox"/>
Defrag the hard drive to reallocate the drive space			<input type="checkbox"/>	<input type="checkbox"/>
Use Purge tools to overwrite free space (3x: 1s, 0s, random)			<input type="checkbox"/>	<input type="checkbox"/>
Reboot the system			<input type="checkbox"/>	<input type="checkbox"/>
Record serial number of cleared hardware			<input type="checkbox"/>	<input type="checkbox"/>
All Backups moved to controlled/classified area			<input type="checkbox"/>	<input type="checkbox"/>

## Enclosure 6: Technical Remediation and Removal Procedures

- a. Assist the user and commander in the completion and gathering of all enclosed checklists.
- b. After all information has been gathered, clear/purge information for the IS, media and/or peripheral devices, and complete a Time Based (Enclosure 4) or Content UDCI Incident Response Form (Enclosure 5) for each IS, media, and/or peripheral device.
- c. Record the serial number of the hardware and maintain records of the location to ensure it is never released outside Army channels. The hardware must be regularly inventoried, and the final disposition for an IS and/or media involved in any UDCI incident will be destruction only. The IS case and physical hard drive will be permanently marked showing they contain classified information that was cleared/purged, date cleared/purged, original level of classification, level of classification after unauthorized disclosure event, and the tool used to purge the drive.
- d. Delete all files, file attachments, or “Saved As” files associated with UDCI from network shares, file storage areas, e-mail boxes, and the server information stores or mail queues. Ensure a check is done for nested files with original messages.
- e. Delete contaminated messages saved in Microsoft’s Outlook Data Files (.pst) on the IS. If .pst files are saved on a network drive, the user must delete the contaminated message, and the Network Enterprise Center (NEC) Exchange administrator must overwrite or purge the network drive containing the deleted file. Once the file has been deleted from a .pst, a new .pst must be created, and all messages from the existing .pst must be copied into the new one. After all messages that need to be saved have been copied, delete the original .pst and replace it with the new one.
- f. Conduct a search on media and network storage for similar or potentially associated files (same date/time stamp, word search, word variations, etc.), and delete all identified files.
- g. Delete or empty the contents of all temporary or cached items such as temporary internet files. Empty any “recycle bin” and “deleted items” folder storage area.
- h. After removal of the suspected files, remove all additional configurations or files that are not operationally required.
- i. Purge the hard drive(s) of each affected local IS using a three pass overwrite (Army BBP setting). The Army Overwrite Utility (Universal Purge Tool) may be obtained from <https://www.acert.1stiocmd.army.mil/tools/>.
- j. Reload the IS.

EAID-CG

SUBJECT: Policy Letter #6-2, Unauthorized Disclosure of Classified Information (UDCI) Violations and Corrective Measures

## Enclosure 7: Emergency Response Points of Contact

- a. 2ID IAM and IA Section, 732-6059, [usarmy.redcloud.2-id.list.g6-ia@mail.mil](mailto:usarmy.redcloud.2-id.list.g6-ia@mail.mil)
- b. 2ID SSO, 732-7258, [usarmy.redcloud.2-id.list.g2-sso@mail.mil](mailto:usarmy.redcloud.2-id.list.g2-sso@mail.mil)
- c. Area 1 NEC IA Section, 732-7068/7062,  
[usarmy.redcloud.1-sig-bde.list.bn-41-co-552-a1-nec-ia@mail.mil](mailto:usarmy.redcloud.1-sig-bde.list.bn-41-co-552-a1-nec-ia@mail.mil)
- d. Area 2 NEC IA Section, 723-4799,  
[usarmy.yongsan.1-sig-bde.list.bn-41-co-201-area2-nec-ia-dl@mail.mil](mailto:usarmy.yongsan.1-sig-bde.list.bn-41-co-201-area2-nec-ia-dl@mail.mil)
- e. Area 3 NEC IA Section, Mr. William Murdock, 754-8558,  
[william.t.murdock.civ@mail.mil](mailto:william.t.murdock.civ@mail.mil), and Mr. Rosendo A. Favor, 754-7002,  
[rosendo.a.favor.civ@mail.mil](mailto:rosendo.a.favor.civ@mail.mil)
- f. 1<sup>st</sup> Signal Brigade Operations Center (BOC/EOC), 723-5016/5019,  
[usarmy.yongsan.1-sig-bde.mbx.bde-eoc@mail.mil](mailto:usarmy.yongsan.1-sig-bde.mbx.bde-eoc@mail.mil) / [1SIGEOC@korea.army.smil.mil](mailto:1SIGEOC@korea.army.smil.mil)
- g. RCERT-K, 764-5956, [usarmy.walker.rcert-k.mbx.korea@mail.mil](mailto:usarmy.walker.rcert-k.mbx.korea@mail.mil)
- h. K-TNOSC, 764-3925, [usarmy.walker.1-sig-bde.mbx.ktnosc-arc@mail.mil](mailto:usarmy.walker.1-sig-bde.mbx.ktnosc-arc@mail.mil)