DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
4710 KNOX STREET
FORT BRAGG, NORTH CAROLINA 28310-5010

AFRC-CI 15 November 2017

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Data Spillage and Negligent Disclosure of Classified Information Policy

1. References: See enclosure 1.

2. Purpose: This policy enforces United States Army Reserve (USAR) policy associated with suspected or confirmed cybersecurity incidents of data spillage, unauthorized disclosure of unclassified sensitive information, and negligent discharge of classified information (NDCI) on USAR managed networks (unclassified or classified).

3. Applicability: This policy applies to all users of unclassified and classified USAR information systems.

4. Policy:

a. Any person who willfully or negligently causes a data spillage or unauthorized disclosure is required to report the suspected cybersecurity incident using the classified data spillage checklist (encl 2) in accordance with reference c. Such individual may be subject to sanctions, disciplinary action, civil penalties, and/or criminal penalties.

b. When classified or sensitive material has been inadvertently placed on, or transferred to, an information system or media not authorized for that data sensitivity level, individuals are instructed to follow USAR-Computer Incident Response Team (CIRT) policy/procedures that require the associated hardware to be removed and destroyed (reference h).

c. USAR-CIRT will respond to and investigate all suspected or confirmed cybersecurity incidents.

5. Responsibilities:

a. All personnel. Safeguard and protect unclassified sensitive and classified information from data spillage and/or unauthorized disclosure. Immediately report all suspected or confirmed cybersecurity incidents and cooperate with any inquiry and investigation.

b. USAR-CIRT. Isolate and contain the data spillage; preserve evidence; preclude unauthorized access to information in question, while applying risk principles to maintain continuity of operations; and ensure all necessary reporting occurs.

c. Commanders and Leaders. Ensure incident response plans (IRPs) include data spillage and unauthorized disclosure (encl 3), as well as common data/information owners and reporting points of contact; ensure all users receive appropriate training on the IRP, incident handling, incident reporting, classified information, and unclassified sensitive information; hold all personnel accountable for their actions or lack thereof; impose sanctions as appropriate; ensure formal documentation of a plan to prevent a recurrence that addresses the root cause and contributing factors of the cybersecurity incident; and follow the additional responsibilities designated by the Under Secretary of the Army (reference g).

d. Information System Security Manager. Coordinate the reporting of and response to cybersecurity incidents; coordinate the initiation of protective or corrective measures; collaborate with the United States Army Reserve Command (USARC) G-2 and the local Security Manager; and direct cybersecurity personnel in assisting incident response, inquiries, and investigations.

e. USARC CIO/G-6 and Subordinate Unit Information Management Officers. Coordinate all cybersecurity incident response procedures and measures for containment, eradication, and verification between the reporting organization and the USAR-CIRT.

6. Effective Date: This policy is effective upon signature and will remain in effect until revised or superseded by the point of contact.

7. The point of contact for this policy is Mrs. Kimberly Register, Chief, USARC CIO/G-6 Cybersecurity Program Management Division, (910) 570-8653 or kimberly.m.register.civ@mail.mil.

Encl

DENIS L. GIZINSKI
Chief Information Officer
USARC Deputy Chief of Staff, G-6

DISTRIBUTION:

GEOGRAPHIC COMMANDS:
1 MSC
7 MSC
9 MSC
63 DIV (R)
- USAG-FHL

81 DIV (R)
- USAG-Fort Buchanan

88 DIV (R)
- USAG-Fort McCoy

99 DIV (R)
- ASA-Dix

FUNCTIONAL COMMANDS:
3 MCDS
76 ORC
79 TSC
200 MP CMD
311 SC(T)
335 SC(T)
377 TSC
412 TEC
416 TEC
807 MCDS
ARAC
ARCD
AR-MEDCOM
LEGAL CMD
MIRC
USACAPOC(A)
75 TNG CMD (MC)
80 TNG CMD (TASS)
83 US ARRTC
84 TNG CMD (UR)
85 USAR SPT CMD
108 TNG CMD (IET)
USAR SPT CMD (1A)

AREC/ARET:
USARPAC
ARNORTH
(CONT)

DISTRIBUTION: (CONT)
ARSOUTH
ARCENT
AFRICOM
CENTCOM
USAREUR
USARAF
8TH ARMY
NORTHCOM
USARJ
I CORPS
PACOM
SOUTHCOM
III CORPS
XVIII ABC
USASOC
EUCOM
SOCOM

COPY FURNISH:
USARC XOs
USARC DIR/DEP/CH/ASST
OCAR Directors & Deputies

References

a. Army Regulation (AR) 25-2, Information Assurance, 23 March 2009.

b. AR 25-1, Army Information Technology, 25 June 2013.

c. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

d. AR 380-67, Personnel Security Program, 24 January 2014.

e. AR 380-381, Special Access Programs (SAPs) and Sensitive Activities, 21 April 2004.

f. AR 380-40, Safeguarding and Controlling Communications Security Material (U//FOUO), 9 July 2012.

g. Memorandum, Under Secretary of the Army, 10 May 13, subject: Commander and Leader Responsibilities for Cybersecurity/Information Assurance (CS/IA) Incident.

h. United States Army Chief Information Officer (CIO)/G-6 Cyber Directorate Information Assurance Best Business Practice (IA BBP) 03-VI-O-0001, Classified Information Spillage on Information Systems, 20 April 2007.

i. Department of Defense (DoD) Manual (DoDM) 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information, 19 March 2013.

j. DoDM 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI), 13 February 2012.

k. Memorandum, Deputy Secretary of Defense, 14 Aug 14, subject: Unauthorized Disclosures of Classified Information or Controlled Unclassified Information on DoD Information Systems.

l. Committee on National Security Systems Instruction 1001, National Instruction on Classified Information Spillage, February 2008.

m. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, April 2013 (updated 22 January 2015).

n. United States Army Reserve Command (USARC) Incident Response Plan, https://xtranet/usarc/g6/ITG/G6%20SOPs/Forms/AllItems.aspx.

o. USARC Chief Information Officer (CIO)/G-6 Data Spillage and Non-Authorized Disclosure of Classified Information Standard Operating Procedure (SOP), https://xtranet/usarc/g6/ITG/G6%20SOPs/Forms/AllItems.aspx.

Classified Information Spillage on Information Systems

IMMEDIATE ACTION CHECKLIST

1. Classification of affected system:

UNCLASSSIFIED □ SECRET □ TOP SECRET □ OTHER □

2. Was file marked with classification markings? YES □ (GOTO 3) NO □ (GOTO 4)

3. Classification of data: CONFIDENTIAL □ SECRET □ TS □ OTHER □

IS TS information on unclassified system?

YES - Plan for destruction of all affected media. (GOTO 17)

NO - You may be authorized to clear or purge affected media (GOTO 4)

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

YES - Plan for destruction of all affected media. (GOTO 17)

NO - Then you may be authorized to clear or purge affected media (GOTO 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 spillage?

Army □ DOD □ Other government agency □ Contractor □ Commercial entity □

POC Name: ____________________ Phone Number: DSN: ______________________________
Rank ___________ Commercial: ____________________________
Position: _______________________ Email address: ______________________________________
Unit: _____________________________

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

Army □ DOD □ Other government agency □ Contractor □ Commercial entity □

Name of sender (FROM): LAST______________ FIRST ________
EMAIL ____________________ PHONE___________ OFFICE______

Name of recipient(s) (TO): LAST______________ FIRST ________
EMAIL____________________ PHONE____________ OFFICE______

Name of recipient(s) (CC): LAST______________ FIRST ________
EMAIL____________________ PHONE____________ OFFICE______

Name of recipient(s) (BCC): LAST______________ FIRST ________
EMAIL____________________ PHONE____________ OFFICE______

Classified Information Spillage on Information Systems

Original Subject of message: ______________________________

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

If yes, subject of subsequent message(s): ______________________________

10. View, copy, and print email header information: YES □ NO □

11. Has document or file been printed? YES □ NO □

12. Has document or file been saved? YES □ NO □

Where? ______________________________

13. Has the originator been notified? YES □ NO □

14. Is the originator the lead agency for the spillage? YES □ NO □

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

16. Has the DO or OCA been contacted? YES □ NO □

POC Name: _Phone Number: DSN:____________
Rank _________ Commercial:______________
Position:______________________Email address:______________________
Unit: ______________________

17. Unauthorized software on system that substantially increased risk or threat?

(i.e. IRC, Peer to Peer file sharing applications, etc) YES □ NO □
If Yes, CI investigators must be contacted and all clearing actions cease.

18. Can OCA/DO downgrade information? YES □ NO □

If Yes, to what category or classification? ______________________________
If NO, Destruction of all affected media is required.

19. Does downgraded classification or category affect response? YES □ NO □

If Yes, GOTO 5.
If No, Destruction of all affected media is required.

20. SYTEM IDENTIFICATION: OS of the affected system:___________Version:___________

21. Did you originate the spillage incident? YES □ NO □
NOTE: If Yes, your organization becomes the lead agency for reporting all actions unless DO/OCA takes control of the incident.

Classified Information Spillage on Information Systems

TIME BASED SPILLAGE INCIDENT RESPONSE

Limit the number of affected systems and collateral damage by immediately disconnecting or isolating all affected systems. 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	□	□	□	□
Identified/notified all CC recipients	□	□	□	□
Identified/notified all BCC recipients	□	□	□	□
Identified all auto process rules on system	□	□	□	□
Delete File from all local systems	□	□	□	□
Delete File from file storage areas.	□	□	□	□
Delete File from user's mailboxes.	□	□	□	□
Delete File from mail queues (sent, draft, etc)	□	□	□	□
Delete messages saved in Personal Folders	□	□	□	□
Empty "Recycle Bin" folder storage area	□	□	□	□
Empty "Deleted Items" folder storage area.	□	□	□	□
Empty "Recover Deleted Items" folder storage area.	□	□	□	□
Conduct a search for similar files (e.g. same date/time stamp, dirty word search).	□	□	□	□
Delete all identified files from search.	□	□	□	□
Verify that no files were saved to network storage devices.	□	□	□	□
Delete contents of all temporary files/folders	□	□	□	□
Delete contents of cached items (e.g.Internet Explorer or Netscape temporary files)	□	□	□	□
Remove all unauthorized files/software	□	□	□	□

Administrator Actions Only

Identified all auto process rules on server			□	□
Files removed from affected servers and devices			□	□
Compact folders or information stores			□	□
Defrag the hard drives of all systems.			□	□
Reboot the system.			□	□
Record serial number of cleared hardware.			□	□
Backup tapes/device/storages drives moved to control/classified area			□	□

Classified Information Spillage on Information Systems

CONTENT SPILLAGE INCIDENT RESPONSE

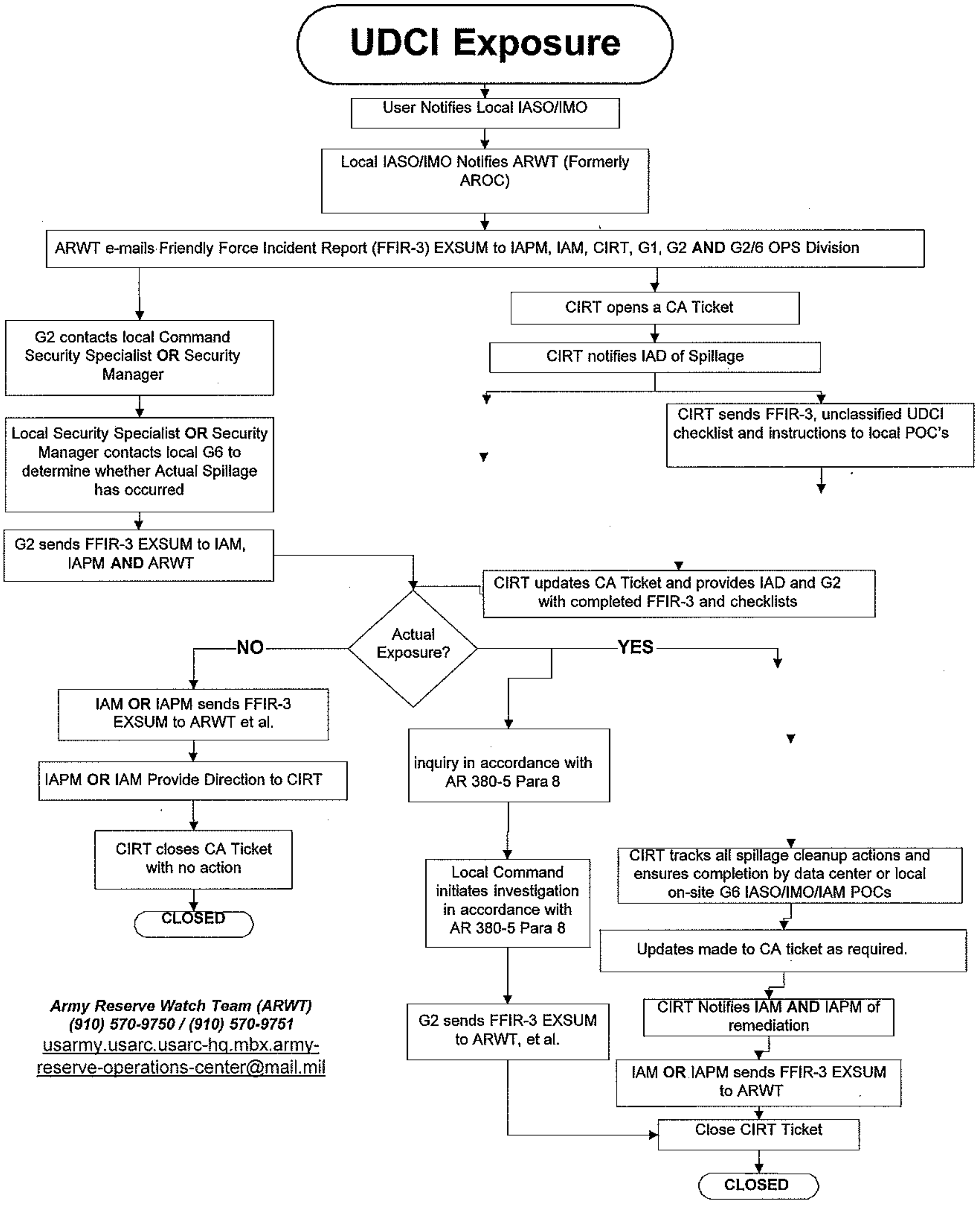
Deliberate identification and eradication of the data from every affected asset to protect the information, exclusive of operational or economical issues (removal and purging activities exclusively)

Complete the following for every system:

	USER		SA	
	YES	NO	YES	NO
Identified/notified all TO recipients	□	□	□	□
Identified/notified all CC recipients	□	□	□	□
Identified/notified all BCC recipients	□	□	□	□
Identified all auto process rules on system	□	□	□	□
Delete File from all local systems	□	□	□	□
Delete File from file storage areas.	□	□	□	□
Delete File from user's mailboxes.	□	□	□	□
Delete File from mail queues (sent, draft etc)	□	□	□	□
Delete messages saved in Personal Folders	□	□	□	□
Empty "Recycle Bin" folder storage area	□	□	□	□
Empty "Deleted Items" folder storage area.	□	□	□	□
Empty "Recover Deleted Items From" folder storage area.	□	□	□	□
Conduct a search for similar files (e.g. same date/time stamp, dirty word search).	□	□	□	□
Delete all identified files from search.	□	□	□	□
Verify that no files were saved to network storage.	□	□	□	□
Delete contents of all temporary files/folders	□	□	□	□
Delete contents of cached items (e.g. Internet Explorer or Netscape temporary files)	□	□	□	□
Remove any unauthorized files/software	□	□	□	□

Administrator Actions Only (in sequence)

Identified all auto process rules on server	□	□
Files removed from affected servers and devices	□	□
Use Purge tool to overwrite free space (1x; random).	□	□
Defrag the hard drive to reallocate the drive space.	□	□
Use Purge tools to overwrite free space (3x; 1s, 0s, then random).	□	□
Reboot the system.	□	□
Record serial number of cleared hardware.	□	□
Backup tapes/device/storages drives moved to control/classified area	□	□



UDCI Exposure

User Notifies Local IASO/IMO

Local IASO/IMO Notifies ARWT (Formerly AROC)

ARWT e-mails Friendly Force Incident Report (FFIR-3) EXSUM to IAPM, IAM, CIRT, G1, G2 **AND** G2/6 OPS Division

G2 contacts local Command Security Specialist **OR** Security Manager

Local Security Specialist **OR** Security Manager contacts local G6 to determine whether Actual Spillage has occurred

G2 sends FFIR-3 EXSUM to IAM, IAPM **AND** ARWT

CIRT opens a CA Ticket

CIRT notifies IAD of Spillage

CIRT sends FFIR-3, unclassified UDCI checklist and instructions to local POC's

CIRT updates CA Ticket and provides IAD and G2 with completed FFIR-3 and checklists

Actual Exposure?

NO

IAM **OR** IAPM sends FFIR-3 EXSUM to ARWT et al.

IAPM **OR** IAM Provide Direction to CIRT

CIRT closes CA Ticket with no action

CLOSED

YES

inquiry in accordance with AR 380-5 Para 8

Local Command initiates investigation in accordance with AR 380-5 Para 8

G2 sends FFIR-3 EXSUM to ARWT, et al.

CIRT tracks all spillage cleanup actions and ensures completion by data center or local on-site G6 IASO/IMO/IAM POCs

Updates made to CA ticket as required.

CIRT Notifies IAM **AND** IAPM of remediation

IAM **OR** IAPM sends FFIR-3 EXSUM to ARWT

Close CIRT Ticket

CLOSED

Army Reserve Watch Team (ARWT)
(910) 570-9750 / (910) 570-9751
usarmy.usarc.usarc-hq.mbx.army-reserve-operations-center@mail.mil