CLASSIFIED INFORMATION SPILLAGE ON INFORMATION SYSTEMS

TIME-BASED SPILLAGE INCIDENT RESPONSE

For use of this form, see AR 25-2

Limit the number of affected systems and collateral damage by immediately disconnecting or isolating all affected systems. Emphasis is on urgency versus accuracy (i.e., less than 2 hours elapsed from origination to identification 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 EACH SYSTEM:

MACHINE NAME: _____

- ☐ YES ☐ NO 1. Identified/notified all TO recipients.
- ☐ YES ☐ NO 2. Identified/notified all CC recipients.
- ☐ YES ☐ NO 3. Identified/notified all BCC recipients.
- ☐ YES ☐ NO 4. Identified all auto process rules on system.
- ☐ YES ☐ NO 5. Delete file from all local systems.
- ☐ YES ☐ NO 6. Delete file from file storage areas.
- ☐ YES ☐ NO 7. Delete file from user's mailboxes.
- ☐ YES ☐ NO 8. Delete file from mail queues (sent, draft, etc.)
- ☐ YES ☐ NO 9. Delete messages saved in Personal Folders.
- ☐ YES ☐ NO 10. Empty "Recycle Bin" folder storage area.
- ☐ YES ☐ NO 11. Empty "Deleted Items" folder storage area.
- ☐ YES ☐ NO 12. Empty "Recover Deleted Items" folder storage area.
- ☐ YES ☐ NO 13. Conduct a search for similar files (e.g., same date/time stamp, dirty word search).
- ☐ YES ☐ NO 14. Delete all identified files from search.
- ☐ YES ☐ NO 15. Verify that no files were saved to network storage devices.
- ☐ YES ☐ NO 16. Delete contents of all temporary files/folders.
- ☐ YES ☐ NO 17. Delete contents of cached items (e.g., Internet Explorer or Netscape temporary files).
- ☐ YES ☐ NO 18. Remove all unauthorized files/software.

_____ _____

SIGNATURE: DATE SIGNED:

Administrator Actions Only:

- ☐ YES ☐ NO 19. Identified all auto process rules on server.
- ☐ YES ☐ NO 20. Files removed from affected servers and devices.
- ☐ YES ☐ NO 21. Compact folders or information stores.
- ☐ YES ☐ NO 22. Defrag the hard drives of all systems.
- ☐ YES ☐ NO 23. Reboot the system.
- ☐ YES ☐ NO 24. Record serial number of cleared hardware.
- ☐ YES ☐ NO 25. Backup tapes/device/storages drives moved to control/classified area.

_____ _____

SIGNATURE: DATE SIGNED: