AUGUST 2012

Data Spill Sanitisation Guide

1. This document provides guidance on some of the common sanitisation techniques for systems used by Australian government agencies involved in a data spill.

2. Data spill sanitisation varies according to the system and devices involved, as well as the detailed system configuration. Agencies should therefore only use this document as a guide.

3. The techniques outlined here are attempts to minimise, rather than eliminate, risks to the exposed data. In the first instance, agencies should follow the advice in the *Media Security* chapter of the *Australian Government Information Security Manual* (ISM). Implementing the ISM controls for media sanitisation provides agencies with high assurance that exposed data has been removed from media affected by a data spill.

4. Before commencing any sanitisation process, this document should also be read in conjunction with DSD's *Data Spill Management Guide* and the *Cyber Security Incidents* chapter of the ISM.

Storage Area Networks (SANs)

5. Different disk sanitisation techniques provide different sanitisation confidence levels. The following list provides disk sanitisation options from highest to lowest levels of confidence:

   a. physical destruction (highest confidence)

   b. zeroing entire media

   c. zeroing the affected file and file record

   d. deleting the affected file and file record (lowest confidence).

6. Sanitisation of the affected Logical Unit Number (LUN) can be conducted by either:

   a. overwriting the media as per the ISM requirements, or

   b. if the sensitive file has not been deleted, securely deleting the sensitive file (i.e. overwriting the contents before deleting the file). Note if the name of the file is also sensitive, agencies cannot only use this method for sanitisation. The new filename must have a minimum length of the original filename.

7. A low level search of the disk should be conducted to verify that all references to the sensitive data are removed.

8. In certain cases involving large SANs or critical operational servers where sanitisation does not change the treatment of the non-volatile media, agencies may be able to take a risk managed approach. In some situations, an agency may be able to securely delete the sensitive file without being required to destroy the affected disks immediately.

9. To take a risk managed approach, an agency must consider:

a. **Physical security.** There must be controlled and restricted physical access to the affected media.

b. **Personnel security.** Only authorised and cleared personnel have physical access to the affected media.

c. **Process and procedure**. There are processes and procedures in place to ensure that the affected media is handled and maintained securely until end-of-life. Areas to consider include:

i. Physical access to the system for maintenance and repairs are conducted by authorised and cleared personnel.

ii. The media is appropriately identified and will not be accidentally reused for another purpose (or in a lower classified network).

iii. The media is destroyed at end-of-life and is not returned to the vendor, reused in another lower classified system or sold.

d. **Acceptance of residual risk.** The information owner is satisfied with the actions taken to clean-up the data spill including the controls put in place to protect the affected asset until end-of-life.

Email servers

10. The majority of Australian government agencies use Microsoft Exchange as their corporate email server. This section provides advice for the most common versions of Microsoft Exchange used in agencies.

11. To sanitise the Exchange Database (*.edb):

a. Hard delete the sensitive email from the affected Inbox on the Exchange server. This can be done using shift+delete on the sensitive email or deleting the email from the system user's trash through the Exchange management interface.

b. Configure the deleted items retention period to 0 days on the Exchange server. This is a temporary setting which may be can changed back to the original value once the clean-up process has completed.

c. Enable page zeroing on the Exchange server.

Page zeroing (Microsoft Exchange)

12. When a message is deleted, the index marks the disk or page as unused. However, the raw data remains on the disk until it is eventually overwritten. Enabling page zeroing (or page scrubbing) overwrites the raw data, reducing the risk of conventional data recovery.

13. **For Exchange versions 4.0 to 5.5 (SP1):** You will need to use a series of command line software tools available from Microsoft. Detailed information is available in four Microsoft Knowledge Base articles:

a. Q196169: Option to zero out deleted messages on Exchange server

b. Q228938: Understanding deleted item recovery

c. Q232006: How to delete a confidential message from Exchange

d. Q260037: How to remove a message from Exchange using ExMerge

14. **For Exchange versions 5.5 (SP2) to 2007 (RTM):** The Extensible Storage Engine (ESE) page zeroing option was introduced to administrators in Exchange 5.5 SP2. When selected, it overwrites unused pages in the Exchange database during the backup process. When using ESE page zeroing:

a. **Consider the performance impact.** This process will have a performance impact the first time it is performed. Future backup processes will have a minimal performance impact as only newly deleted pages will need to be zeroed. Agencies should consider leaving this setting enabled after first use.

b. **Consider replication issues.** If your agency uses continuous replication in your environment, the pages in the passive copy of the database may not be zeroed and the active copy pages are only zeroed in streaming backup mode.

c. **Consider volume shadow-copy service issues.** If your agency uses volume shadow-copy service backups, both active and passive copies of the database will not have their pages zeroed. (Note: this issue was addressed in 2007 SP1).

d. **Ensure that ESE Page Zeroing is enabled.** For Exchange 5.5, enable ESE page zeroing in the backup configuration options. For Exchange 2000 and 2003, enable ESE Page Zeroing via the Exchange System Manager console.

e. **Trigger the Exchange server to conduct an online normal (full) backup.** This forces Exchange to perform the page zeroing process on the Exchange database.

Further information is available in Microsoft Knowledge Base article Q223161: *Information on ESE Zeroing*.

15. **For Exchange versions 2007 (SP1) to 2010 (RTM):** Exchange 2007 SP1 introduced a new online maintenance task called "Zero Database Pages During Checksum", which is disabled by default. Agencies should also consider leaving this setting enabled after first use. To enable this task:

a. **Consider the performance impact.** This process will affect server performance and place a significantly increased load on the database cache. Agencies should consider enabling the "Throttle Checksum" registry entry to limit the performance impact.

b. **Watch system log space and system resources.** The page zeroing activity is logged as Event 718 in the Windows Server Event Log. This activity should not be run during peak periods of email usage.

c. **Confirm the process is completed.** When the page zeroing process is complete, it is logged as Event 722 in the Windows Server Event log.

Further information is available in Microsoft Knowledge Base article BB676537: *Online Maintenance Database Scanning in Exchange 2007*.

16. **For Exchange Server 2010 (SP1 and SP2):** According to Microsoft documentation, ESE page zeroing is on by default and there is no mechanism to disable it. This automated process performs page zeroing milliseconds after the deletion record via an asynchronous thread.

17. On the Exchange Server SAN, increase disk utilisation to a high level to ensure the infected area is overwritten. Agency IT staff will need to determine how high to set utilisation to avoid storage issues. SAN disks are to be appropriately classified. The *Media Security* chapter of the ISM should be consulted for further guidance on classifying sanitised hard disks.

18. Further information is available in Microsoft Knowledge Base article GG549096: *Understanding Exchange 2010 Page Zeroing*.

Workstations

19. End user workstations may also require sanitisation, depending on the type of data spill. As most workstations are replaceable, risk-managed approaches to sanitisation are usually not required.

20. The volatile and non-volatile memory stores of a workstation involved in a data spill should be initially treated as the same classification of the spilled data. The memory stores should be sanitised to the classification of the agency's network.

21. Remnants of a data spill can reside in files designed to maintain the system state while it is hibernating. Zeroing the affected file (usually C:\hiberfil.sys) will help sanitise the data spill. Where practical, disabling hibernation will assist in preventing future data spills.

22. If it is not possible to sanitise the memory stores to the required classification, then the hard disks must either be reused in a network of the same classification as the spilled data or destroyed per requirements in the ISM.

23. If the memory stores are reused in a network of the same classification, the spilled data should still be sanitised in accordance with the need-to-know principle.

Further information

24. Further security controls on sanitisation can be found in the ISM. This document assists in the protection of official government information that is processed, stored or communicated by Australian government systems: http://www.dsd.gov.au/infosec/ism/index.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.