Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

PROTECT

JULY 2018

Data Spill Sanitisation Guide

Introduction

1. This document provides guidance on common sanitisation techniques for data spills.
2. Data spill sanitisation techniques vary according to the system and devices involved, as well as their configuration. Organisations should therefore only use this document as a guide.
3. The techniques outlined in this document are attempts to minimise, rather than eliminate, risks to exposed data. In the first instance, organisations should follow the advice in the *Australian Government Information Security Manual* (ISM).
4. Before commencing any sanitisation process, this document should also be read in conjunction with the Australian Cyber Security Centre's (ACSC's) *Data Spill Management Guide* publication.

Storage Area Networks (SANs)

5. Different disk sanitisation techniques provide different confidence levels. The following list provides disk sanitisation options from highest to lowest levels of confidence:
   a. physical destruction
   b. zeroing entire media
   c. zeroing the affected file and file record
   d. deleting the affected file and file record.
6. Sanitisation of the affected Logical Unit Number (LUN) for a SAN can be conducted by overwriting the media, or if a sensitive file has not been deleted, securely deleting the sensitive file (i.e. overwriting the contents before deleting the file).
7. A low level search of the disk should also be conducted to verify that all references to the sensitive data are removed.
8. In certain cases involving large SANs, or critical storage services, organisations may be able to take a risk-based approach without being required to destroy affected disks immediately.
9. To take a risk-based approach, an organisation should consider:
   a. **Physical security.** There is controlled and restricted physical access to the affected media.

b. **Personnel security.** Only authorised and cleared personnel have 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. This includes:

i. maintenance and repairs are conducted by authorised and cleared personnel

ii. media is appropriately identified and will not be reused for another purpose (or in a lesser sensitive environment)

iii. media is destroyed at end-of-life and is not returned to the vendor, reused in another lesser sensitive environment or sold.

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

Email servers

10. The majority of organisations use Microsoft Exchange as their corporate email server. To sanitise an Exchange Database:

a. Hard delete the sensitive email from the affected inboxes on the Exchange server. This can be done using shift+delete on the sensitive email or by deleting the email from users' 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 be changed back to the original value once the clean-up process has completed.

c. Enable page zeroing on the Exchange server.

11. When an email 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.

12. Further information on page zeroing is available from Microsoft[1] [2].

Workstations

13. User workstations may also require sanitisation, depending on the type of data spill.

14. The volatile and non-volatile memory of a workstation involved in a data spill should be initially treated as the same sensitivity of the spilled data and should be sanitised.

15. Remnants of a data spill can reside in files designed to maintain a system's 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.

16. If it is not possible to sanitise a workstation's memory, it should either be reused in a network of the same sensitivity as the spilled data or destroyed.

[1] For Exchange 2010, https://docs.microsoft.com/en-us/previous-versions/office/exchange-server-2010/gg549096(v=exchg.141).

[2] For Exchange 2013, https://technet.microsoft.com/en-us/library/gg549096(v=exchg.150).aspx.

Further information

17. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

Contact details

18. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).