AUGUST 2012

Data Spill Management Guide

1. A data spill is the accidental or deliberate exposure of classified, sensitive or official information into an uncontrolled or unauthorised environment or to persons without a need-to-know. A data spill is sometimes referred to as unintentional information disclosure or a data leak.

2. Data spills usually fall into one of two categories:

   a. The transfer of sensitive information to a system which is not accredited to handle the information. Such a transfer may be performed via email or digital media.

   b. The disclosure of sensitive information on the Internet, including web forums, social networking websites, Internet search engine caches and other types of cloud-based storage.

3. This document provides guidance to agencies on managing data spills in their environment.

4. Data spills are considered cyber security incidents and are reportable under the DSD Cyber Security Incident Reporting scheme.

5. Agencies should refer to the latest version of the *Australian Government Information Security Manual* (ISM) for sanitisation guidance for specific media. Further advice is provided in DSD's *Data Spill Sanitisation Guide* and the *Cyber Security Incidents* chapter of the ISM.

Data spill management overview

6. Educating users on agency system and web usage policies, as well as how to appropriately identify and handle information with protective markings, can greatly assist in preventing data spills (ISM controls: 0251, 0252, 0255, 0818, 0820, 0922, 1339).

7. However, in the event of a data spill, agencies should use the following five step process:

   a. **Identify**. Recognise that a data spill has taken place and commence this process.

   b. **Contain.** Determine the breadth of the data spill to prevent further dissemination of sensitive data.

   c. **Assess.** Decide on the most appropriate method to sanitise the data spill for your situation and desired level of residual risk.

   d. **Remediate.** Remediate the data spill based on your assessment.

e. **Prevent.** Implement prevention measures to stop similar incidents from occurring in the future.

8. This process should be followed for every data spill which occurs, as each instance is different and may require a distinct response.

Step 1: Identify

9. Data spills are usually identified by system users. In accordance with the ISM, agencies must include in standard procedures for all personnel with access to systems that they notify an IT Security Manager of a suspected data spill or access to data that they are not authorised to see (ISM control 0130).

10. Data spills can also be identified through monitoring, auditing and logging. For example:

a. Preventing non-protectively marked e-mails from being sent or received by an agency's e-mail server or e-mail client (ISM controls 0562, 0875 and 1022).

b. Using data loss prevention tools like SpillGuard[1] that can warn system users and alert administrators of possible security classification violations.

11. When a data spill is identified, agencies must assume that the spilled data is compromised and base remediation procedures or risk management on a worst-case scenario (ISM Control 0129).

12. An immediate assessment should be performed to:

a. Track data flow, movement and storage locations of the spilled data to assist in determining what devices and systems are affected.

b. Identify affected system users, including any external to the agency.

c. Determine the length of time between the data spill and the identification of the data spill.

13. Personnel required to assist in the management of the data spill should also be identified. This can include:

a. information owners

b. subject matter experts

c. the Agency Security Advisor (ASA)

d. the IT Security Advisor (ITSA)

e. IT Security Managers (ITSM) or IT Security Officers (ITSO)

[1] SpillGuard is a freely available proof-of-concept plugin for Microsoft Office designed to help prevent the opening, saving or printing of Microsoft Office files containing classification markings higher than the classification of the user's computer. Available at http://sourceforge.net/projects/spillguard/

f. communications security officers (COMSO).

Step 2: Contain

14. Containment may involve physically isolating or logically separating affected systems from the network (ISM control 0136). Logical separation can be achieved by temporarily removing software functionality or applying access controls to systems to prevent further exposure.

15. For example, the containment process taken by the ITSM for a data spill involving an internal email may include:

a. The sender and recipients of the email are identified, contacted and told not to forward or access the sensitive email.

b. Determine if it is necessary to retain a copy of the email so that the classification of the material can be verified by the information owner for a damage assessment.

c. Determine if it is necessary to delete the email from affected users' inboxes as quickly as possible to prevent dissemination of the sensitive email.

d. Proceed to the assessment phase to determine what further actions are required, including potential sanitisation of the email server and workstations.

16. Selection of containment actions should be made in consideration of an agency's environment.

Step 3: Assess

17. After containment, to prevent further access and exposure of the data, a thorough assessment should be performed. This includes:

a. **Identifying affected system users, systems and devices.** While the identification process highlights the systems and users that are initially affected, a more thorough assessment should be performed after the containment process. This should include devices such as workstations, backup storage, printers, print servers, network shares, email inbox and servers, content filtering appliances, web mail and external systems. Agencies should involve their system and network administrators in this process.

b. **Contacting the information owner.** The information owner must be contacted and notified of the data spill (ISM control 0133). The information owner will be able to provide guidance on whether the data is correctly classified and indicate the approach to minimise exposure. Codeword related data spills must be reported to the compartment holder.

c. **Contacting relevant authorities.** Data spills must be reported to the CSOC under the Cyber Security Incident Reporting scheme. (ISM controls 0132 and 0140).

d. **Perform a damage assessment.** Agencies should perform a damage assessment to determine what harm was caused by the inadvertent disclosure of data. Agencies must assume that the spilled data was accessed by unauthorised individuals and determine actions to manage and mitigate the extent of the data spill (ISM Control 0129).

Step 4: Remediate

18. Agencies should work in collaboration with the information owner to determine a satisfactory remediation of the data spill. DSD is available for consultation in the event that an agreed clean-up solution cannot be reached.

19. Remediation is usually achieved through a balance of technical sanitisation controls and risk management. For data spills involving classified data, agencies should review specific sanitisation requirements from the latest version of the ISM.

20. For each of the systems identified during the assessment stage, a remediation strategy should be developed that takes into account:

a. access controls to the data and the systems that hold the data

b. utilisation rate of memory storage (i.e. ability for the system to naturally overwrite free space through data attrition and growth)

c. criticality of the system to the business (e.g. mission critical SAN or a user workstation)

d. the duration of exposure of the data (i.e. is it a recent exposure or has the data been exposed for a long period of time)

e. sanitisation options available for the media (e.g. raw disk overwrite, file overwrite or physical destruction)

f. disposal consideration of the asset at end of life (i.e. will the asset be resold or physically destroyed)

g. balancing the risk of drawing attention to the data versus accepting the damage

h. resources, impacts and financial costs to business to replace or sanitise affected systems.

21. All remediation actions should be documented and appropriately stored based on the classification of the remediation plan.

Step 5: Prevent

22. The action causing the data spill must be reviewed to determine why it occurred (e.g. non-adherence of policy, gaps in existing procedures or absence of a technical control).

23. The review should result in implementing preventative measures to reduce the likelihood of future data spills occurring. This may include additional user training or improved technical controls between data of different sensitivities.

24. ASAs should perform a protective briefing for users who may have been inadvertently exposed to the data spill.

Further information

25. For further information on technical controls and sanitisation advice, see DSD's *Data Spill Sanitisation Guide*.

26. Further advice on managing data spills 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.