harbinger

Harbinger Escrow Services
Backup and Archiving Policy

Document version:	2.8
Issued to:	Harbinger Escrow Services
Issued by:	Harbinger Group Pty Limited
Delivered on:	18 March 2015

Table of Contents

1 Introduction

1.1 Summary

This document provides Backup and Archival Policy to promote effective maintenance and custody of digital information assets and IT systems and data in accordance with the Australian and International Recordkeeping Standard AS/ISO15489.1 and to enable their efficient restoration to support business continuity of Harbinger Escrow Services's operations.

For further information contact the policy owner defined in Section 6.

1.1 Objective

The overall objective of the Backup and Archival Policy is:

- to ensure that IT systems and data are protected in accordance with their value / risk profile by systematically "making a copy" of, or "backing-up" each IT resource to facilitate its effective recovery for continuance of Harbinger Escrow Services's operations; and
- to ensure that the Vault Manager effectively supports the legal capture, retention and disposal of digital information assets in accordance with current legislation and standards through the maintenance of associated IT systems and adherence to their associated business rules.

Related objectives of the Backup and Archival Policy include:-

- To appropriately mitigate the threat to Harbinger Escrow Services operations and its clients from degraded or unavailable IT systems and data
- To facilitate the design and implementation of appropriate IT systems and data recovery strategies that are aligned with IT resource value / risk profiles
- To educate Harbinger Escrow Services staff, contractors and suppliers in their responsibilities to Harbinger Escrow Services in relation to the protection of corporate and client IT systems and data.
- Protect return on investment in the information management solutions.

1.2 Scope

This policy provides the rules and guidelines to facilitate the efficient and effective archiving and backup for company and client data and IT systems including:

- Databases, structured and unstructured information and IT systems residing on the following categories of infrastructure:-
    - **Category 0:** Client Material
    - **Category 1:** Core Databases and Systems
    - **Category 2:** Desktop and Laptop Computers
    - **Category 3:** Other Storage Technologies.

Further this policy provides directives to guide:

- Archiving and Back-up frequency
- The addition, modification or deletion of a data back-up profile in a defined backup cycle
- The testing of archived data and system backup and restoration processes
- The testing of the validity of data and system restoration.

[1] Digital information assets include electronic files, images, documents, instant messages, reports, multimedia, emails and other electronic records.

- The execution of good management of the IT systems used to archive and backup digital records
- Vault Manager maintaining the technology systems that manage archived digital assets
- Vault Manager providing digital record archival and backup governance
- Account Managers administering their day-to-day operational adherence with HES Backup and Archival Policy

1.3 Audience

Overall, this policy is relevant to all Harbinger Escrow Services employees and contractors that maintain data and IT systems.

Specifically this policy is relevant to the Vault Manager who is involved in the implementation of IT operational processes.

2 Policy Statement

2.1 General

The Vault Manager is responsible for the design, development, testing, installation, operation and maintenance of all routine and specialised archiving, backup, disposal and restoration procedures and processes required to protect Harbinger Escrow Services's IT systems and data. Procedures should include:

- Metrics for the measurement of demand and volume growth for backups and archives
- A definition of what constitutes appropriate storage and appropriate storage conditions to ensure records are:
    - stored in the most appropriate format to retain the value of the record for its prescribed life
    - protected from conditions of deterioration, loss, non-authorised destruction, theft, disaster and unauthorised access
    - accessible to authorised individuals
    - stored against documented risk and security profiles
    - managed in a cost effective way
- Audit cycles to demonstrate that records have not been compromised through system outage or malfunction
- A time period for the reassessment of storage requirements to cater to changing business requirements.

Backup cycles and archiving arrangements will incorporate evaluations of data sensitivity and IT system criticality to Harbinger Escrow Services operations.

In the event of no Data Owner's instructions to an alternative, IT systems and associated data will be backed up in accordance with a minimum standard of archiving and backup.

The Vault manager will produce, maintain and publish a register of data and IT systems included in backup cycles to clearly communicate the backup cycle frequency, backup type (e.g., full or incremental), approximate backup time, approximate restoration.

2.2 Backup and restore

2.2.1 Category 0: Client Material

The Vault Manager is responsible for the backup routine and the effective restoration of all client material, residing on Harbinger Escrow Services data vault

The Managing Director is responsible for notifying the Vault Manager of changes to service requirements. The Vault Manager will provide advice and guidance on such changes.

The Vault Manager is responsible for the restoration of data and information in client material and will regularly perform and monitor the results of trial restorations of client material.

2.2.2 Category 1: Core Databases and Systems

The Vault Manager is responsible for the backup routine and effective restoration of all core databases, files and systems residing on Harbinger Escrow Services's servers and detached storage facilities.

The Vault Manager is responsible for the restoration of data and information in core databases and systems. ITS will regularly perform and monitor the results of trial restorations of core databases and systems.

2.2.3 Category 2: Desktop and Laptop Computers

Corporate data must not reside on any electronic devices including desktop, laptop or hand-held computers, smart phones or other electronic storage capable devices. Users of these devices (e.g. Harbinger Escrow Services employees and contractors) are responsible for ensuring that all corporate data and information is only stored on Harbinger's corporate storage facilities (e.g. Corporate: *Cinderella* and *Ariel*, Client Material: *Mulan*).

Desktop, laptop, hand-held computers or PDA devices local disks and memory will not be systemically backed-up.

The Vault Manager is responsible for the development of the procedures and processes that perform backup of Harbinger's corporate storage facilities that are designated for access and use by desktop, mobile (ie. laptop and held-hand computer) devices. Backup of these storage facilities will be performed in accordance with the agreed and published backup routine (Category 1).

2.2.4 Category 3: Other Storage Technologies

Corporate data must not reside or be backed-up on any storage technologies including floppy disks, memory sticks or flash memory, CDs, DVD,s or portable disks. Harbinger employees and contractors must be made aware such actions are in contravention of their Confidentiality and Non-disclosure undertakings, and Harbinger's Code of Conduct.

2.2.5 Backup and Restore Routine

Category	Backup type	Media	Frequency	Storage
Category 0	Incremental	D2D	Daily	Disk
	Full	Tape	Weekly	on-site
	Full	Tape	Monthly	off-site
	Restore	As required (8 working hrs)		
Category 1	Incremental	D2D	Weekly	Disk
	Full	Tape	Monthly	off-site
	Restore	As required (16 working hrs)		

2.3 Archive and Disposal

2.3.1 Authorisation

All records identified for archive and / or disposal must be authorised for archive or disposal by the Managing Director AND by the Vault Manager.

Valid method of archiving of digital records is (2 x copies)

- encrypt
- transfer to magnetic tape
- I x stored in onsite tape storage facility
- 1 x stored in offsite secure vault facility

Valid methods of disposal of digital records and their backups are:

- irreversible reformatting or rewriting
- physical destruction of storage media.

2.3.2 Archive and Disposal Routine

Category	Type	Media	Frequency	Condition
Category 0	Archive	Tape	Annual 1st July	Not less than 12 months old Duly authorised
	Destroy	n/a	Annual 1st July	Client no longer active for 2 years (all agreements terminated) Notice of intention to destroy issued to Vendor and End-user Notices contact + 21 days Duly authorised
Category 1	Archive	Tape	Annual 1st July	Not less than 7 years old Duly authorised
	Destroy	n/a	Annual 1st July	Not less than 10 years old Duly authorised

Important:
Do not employ delete-instructions to destroy records as all system pointers and alias files referencing the records may not be destroyed.

2.4 Process and Roles

2.4.1 Process Description

The effective execution of this policy involves the following procedures:

- Identify data, information and IT systems requiring backup / restoration, archive or disposal services
- Categorise backup / restoration, archive or disposal according to the Category 0,1,2,3 classification scheme
- Commence backup / restoration, archive or disposal processes
- Monitor and measure backup / restoration, archive or disposal

- Test and review of backup / restoration, archive or disposal

2.4.2 Role Description

The above procedures involve a number of different roles with specific responsibilities described below.

- Desktop, Laptop and Hand-held Computer Users: Those individuals that use such devices in the execution of their job. Individual users are responsible for adherence to this policy and ensuring that Harbinger's data, information and IT systems are only stored on approved storage devices. Further they are responsible for the prudent use of allocated infrastructure and accept full responsibility for the backup of personal data and information stored on located assets.
- Account Managers: Those individuals that perform roles that assume accountability for client materials. Data Owners must ensure that client materials within their ownership portfolio are protected in accordance with this policy. They trigger requests for new, amended and cessation of service with the Vault Manager.
- Vault Manager: Individual that performs the roles that assume accountability and responsibility for the execution of backup / restoration services.

3 Compliance Statement

Compliance to this backup and archive policy is critical to the continuance of Harbinger Escrow Services's operations and service delivery.

Conformance to this policy will be monitored annually.

Trial execution of it's backup and restoration services will be tested quarterly.

Execution of Archive and Disposal will be undertaken annually (on or around 1 July).

4 Background Material & References

4.1 Background Material

Best Practices, Disaster Recovery and Business Continuity Planning (Harbinger Group 2007).

5 Related Documents

HES040149 Harbinger Escrow Services Recordkeeping and Retention Policy

6 Roles, Responsibilities and Contacts

Roles & Responsibilities	Contact Details
Issuing Authority	This document is produced under the authority of Managing Director, Harbinger Escrow Services, who authorised its publication on 18 03 2008.
Change Authority (Authority to change the Policy or give exception waivers)	Managing Director, Harbinger Escrow Services.
Owner	Managing Director HES
Further information	Please contact members of HES

7 Review Timetable

This policy will be reviewed every 12 months by the policy owner to maintain its currency and validity. Its next scheduled review will occur in September, 2012.

harbinger

Harbinger Group Pty Ltd
ABN 58 120 491 554

Melbourne
Level 4, 34 Queen Street
Melbourne, VIC 3000
Ph: (61 3) 9618 2000

info@harbinger.com.au
www.harbinger.com.au