harbinger

Harbinger Escrow Services
Recordkeeping and Retention Policy

Document version:	3.5
Issued to:	Harbinger Escrow Services
Issued by:	Harbinger Group Pty Limited
Delivered on:	22 July 2015

© Harbinger Group Pty Limited, Commercial in Confidence

Table of Contents

CONFIDENTIAL

No part of this document may be reproduced, transcribed, translated into any language or transmitted in any form electronic or mechanical for any purpose whatsoever without the prior written consent of Harbinger Group Pty Ltd. Names of programs and computer systems are registered trademarks of their respective companies.

1 Introduction

1.1 Policy Summary

The Recordkeeping and Retention Policy describes Harbinger Escrow Services (HES)'s processes, roles and responsibilities for the management of digital information assets.

For further information contact the policy owner defined in Section 6 Roles Responsibilities and Contacts.

1.2 Policy Objective

The objective of the Recordkeeping and Retention Policy is to:

- ensure HES complies with the legal capture, retention and disposal of physical and digital information assets.
- ensure that HES can refer to accurate historical records of business.

1.3 Policy Scope

Archiving and recordkeeping practices at Harbinger Escrow Services are predominantly managed by the Vault Manager.

The Vault Manager:

- Maintains the technology systems that manage escrowed material and archived digital assets and other digital information assets
- Provides retention and recordkeeping governance and coordinates digital records administration

Account Manager's ensure day-to-day operational adherence with HES retention policies.

This scope of this policy addresses how Harbinger complies with its recordkeeping and retention policy. This includes the management of digital information assets including:

- Digital assets (lodgements) created and made by Harbinger's clients
- Digital assets created and made by Harbinger
- Transaction records created from the conduct of business
- Internal records created as a consequence of running Harbinger.

Harbinger Escrow Services administration staff, contractors and clients may be responsible for the production of these records which may include items as diverse as source code, intellectual property records, blueprints, third-party software, reports, contracts, documents, manuals, emails, invoices and receipts.

1.4 Audience

This policy is relevant to all Harbinger staff, contractors and third-party service providers that are involved in the creation, maintenance and disposal of digital records for and on behalf of Harbinger Escrow Services.

2 Policy Statement

All HES management, staff, contractors and service providers (Staff) that are involved in the creation, maintenance and disposal of digital and physical records for and on behalf of Harbinger Escrow Services must meet the following requirements.

2.1 General requirements

All Staff are responsible for the maintenance of records. All Staff must:

- ensure that *controlled digital information* assets exist only on Harbinger's *controlled file servers*
- ensure that no *controlled digital information* assets exist on computer workstations and other electronic devices
- ensure that no electronic device contains evidence of Harbinger business activities
- de-duplicate all file stores under their custodial management
- back up records by ensuring they are placed and then exist only on Harbinger's *controlled file servers*
- dispose of records in accordance with Harbinger's authorised approval process.

Information assets to be regarded as *controlled digital information* assets include:

- all Harbinger electronic assets and Harbinger's clients electronic assets (escrow lodgements) and electronic and physical data, documents, records and other information that is not expressly and clearly marked as exempt from from digital information asset control - including but not limited to:
    - escrow lodgements and client digital assets
    - email containing evidence of business activity, actions and decisions
    - business related correspondence received and sent by email
    - official information related to vendors, contractors, personnel and other staff
    - multimedia, sound and video based files that record evidence of business activity.

Vault Manager is responsible for maintaining single copies of all escrow lodgements and client digital assets and ensuring duplicate copies are destroyed using an appropriate method of disposal (see Archival Policy).

Account Managers are responsible for maintaining single copies of all records and ensuring duplicate copies are destroyed using an appropriate method of disposal (see Archival Policy).

The following documents must be treated as records:

- technology plans and seasonally released business reports
- minutes and documentation resulting from all board meetings
- evidence of financial transaction
- any plans relating to quality and change management activity and programs
- internal policies, processes, procedures and guidelines and associated communications to the business relating to the use of IT, online services and networks
- charters of individual business units
- all personnel policies and procedures
- project management and project output documents which capture specifications, instructions, testing and evaluation results, schematics, architectures and blueprints
- all licenses, contracts and asset management documentation
- physical and digital information assets that contain intellectual property content or significant knowledge management content that has a retention value
- communications and media releases that expose HES to the public
- all IT registers (eg. security, asset, software libraries etc).

- all versions and iterations of the HES website, knowledge management system, escrow management system, customer relationship management system, accounting and financial system, library and any externally accessable information

2.2 Managing records

Account Managers will be required to continually support the training of other Harbinger staff in Recordkeeping and Retention Policy.

The Managing Director is responsible for ensuring that Vault Manager and Account Managers comply with the Recordkeeping and Retention Policy.

All records are required to be maintained in a way that is usable and accessible to authorised users.

Records which are no longer in operation should be periodically scheduled for offline digital storage. Contact Vault Manager for assistance.

Automated procedures for the management of digital records must also be able to be performed manually in the event of system inoperability or unavailability.

The Vault Manager must maintain a Records Management Plan that must identify:

- what records are to be associated with which escrow process
- the minimum information requirements for each of these records
- the appropriate format the record should take (eg. digital or physical, PDF, Microsoft Excel, etc.)
- the appropriate method of storage
- procedures for the use, retrieval and transmission of records
- appropriate retention periods and preferred disposal methods (see Archive Policy)
- a contingency plan

2.3 Creating records

When creating records it is important that they can be trusted by the end user. Records need to accurately reflect what has taken place, for example:

- the record presents evidence of being created at the time either through digital timestamp or a date stamp in the content
- any authorised actions / decisions are documented stating who authorised the action and nominating a time period in which the action is to be executed
- there is no evidence to suggest that the document has been altered or edited, preferably presenting the document in an uncompromised format (eg. locked PDF or certified hardcopy).

All digital information assets deemed to be records must be protected from unauthorised alteration or annotation.

3 Compliance Statement

All records produced on behalf of HES by its staff and contractors must comply with this policy.

4 Background

Harbinger Escrow Services may need to be able to provide its clients and perhaps the judicial system with historical evidence of its business decisions and publications. This information may also be important for annual client and internal management reporting. As a supplier to Federal and State government, and large private sector businesses, HES may fall under scrutiny from the public and by authorities such as legal and tax. Effective recordkeeping and archiving practices will ensure that Harbinger Escrow Services is in a position to provide evidence of its business activities and accountability for internal decisions to any authorised scrutineers.

5 Related Documents

5.1 Existing policies

HES040147 Archiving and Backup 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 01 09 2008
Change Authority (Authority to change the Policy or give exception waivers)	Manging Director, Harbinger Escrow Services. Please refer to the HES Manging Director for changes and alterations to this policy
Policy Owner (Responsible for the implementation and enforcement)	HES Vault Manager
Author	Nigel Brown
Further information	Please contact

7 Review Timetable

This policy will be reviewed every 12 months by Managing Director to ensure 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

No part of this document may be reproduced, transcribed, translated into any language or transmitted in any form electronic or mechanical for any purpose whatsoever without the prior written consent of Harbinger Group Pty Ltd. Names of programs and computer systems are registered trademarks of their respective companies.