Harbinger Escrow Services
Information Privacy and Data Collection Policy

Document version:	3.2
Issued to:	Harbinger Escrow Services
Issued by:	Harbinger Group Pty Limited
Delivered on:	22 July 2015

Table of Contents

1 Introduction

1.1 Summary

The Information & Data Protection Policy describes the actions required to be undertaken to ensure Harbinger Escrow Services's information management procedures comply with the Privacy Act 1988 (Cth). It provides **general guidelines** on the handling, granting of access rights to, use, storage and disposal of data, records and information for which Harbinger Escrow Services has an obligation protect.

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

1.2 Objective

The objective of the policy is to ensure that Harbinger Escrow Services staff and contractors handle the data, records and information of Harbinger's customers in a way that meets the expectation of those customers.

1.3 Scope

Harbinger Escrow Services has various obligations to protect data, records and information against unauthorised access, use, loss, disclosure, modification, destruction or other misuse.

This policy is subordinate to the Harbinger Escrow Services Privacy Policy. It applies to the collection and management of all Harbinger Escrow Services records (hardcopy or electronic), containing structured data, records or unstructured information.

1.4 Audience

The audience for this policy includes all staff, contractors and external providers acting on Harbinger Escrow Services's behalf, who collect or manage the data, records and information of Harbinger Escrow Services customers, whether it's in electronic or hardcopy format.

2 Policy Statement

2.1 Business Considerations

Consideration of information privacy/data protection risks and impacts are in addition to the strategic, prudential, financial and other business risk factors forming part of Harbinger's change management processes.

Harbinger must consider specific information privacy/data protection obligations when, amongst other things, we:

- develop new products and services
- change or enhance existing products and services
- develop, review or amend policies, procedures or processes
- develop new, or amend existing forms (paper or electronic)
- enter into strategic alliances or joint ventures
- recruit staff
- engage consultants or outsource non-core functions and activities
- acquire, build or modify computer systems, applications or software.

2.1.1 Group Input and Review

Prior to implementation of internal or external changes involving data, records and information handling, Harbinger must

- ensure that risk factors are assessed and included in all relevant decision making processes, and
- obtain input, or where appropriate, formal sign-off from the Vault Manager.

2.2 Obligations

The following policy statements indicate, in general terms, some of Harbinger's data, records and information privacy/data protection compliance obligations:

2.2.1 Collection of customer information:

How much, when and the way we collect customer information is affected. Collection of customer information must be reasonably necessary for our activities, be made by fair means and not in an unreasonably intrusive way.

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

2.2.2 Disclosure of data, records and information:

We are restricted from disclosing data, records and information for another purpose unrelated to the original purpose of collection.

In order to disclose data, records and information to an End-user, consent must be obtained from the Vendor or the use must be authorised or required by law. Such consent may be express or implied and will depend upon the particular circumstances.

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

2.2.3 Data Quality:

We must endeavour to keep data, records and information accurate, complete and up-to-date.

Data that is stored on behalf of Harbinger Escrow Services customers is to be managed in accordance with the principles outlined in the DVM Data Maintenance and Cleansing Policy (HES050003). It is also subject to the disposal rules outlined in the DVM IT, Archival Policy (HES040170).

The context of data, records and information under management is to be maintained to ensure that the information does not become misplaced or mis-filed.

Where data is to be updated by the Vendor, amendments are to be propagated across all official copies of the information, see DVM IT, Data Maintenance and Cleansing Policy (HES050003).

2.2.4 Data Security:

We must take reasonable steps to keep data, records and information secure and safe from misuse, loss, unauthorised access, modification or disclosure. Refer to the following resources for assistance:

- HES040110 Harbinger Escrow Services IT Systems Security Policy,
- HES040114 Harbinger Escrow Services Software Security Policy,
- HES040113 Harbinger Escrow Services Information Classification Scheme and
- HES040112 Harbinger Escrow Services Third Party Network Connection Policy for information on IT system security privileges, access rights, audit trails, and controls
- Vault Manager for further information on IT Security policies, procedures and tools, including the procedures for granting access rights and the tools for monitoring of Audit Trails.

All electronic and hard copy storage facilities and mediums used for the storage of data, records and information shall apply appropriate security to the protection of the data, records and information. Reasonable steps must be taken to ensure the information is protected:

- against unlawful or unauthorised physical and virtual access
- against unlawful or unauthorised use
- from corruption (error related or intentional), modification or unauthorised change
- against unlawful or unauthorised disclosure
- during transit from one location to another
- during maintenance of the data vault storage facility or programs associated with its operation.

The method of security is to be documented and an audit trail of access maintained by the Vault Manager. This security record is to be made available to an appointed internal auditor on request. The security record must be current and complete to be deemed to be compliant with this policy. The security record must include:

- Identification of the individual Harbinger employee that initiated the data collection
- A statement of the nature and volume of the data, records and information under management
- A statement of the currency of the information, retention period and nominated disposal method
- A metadata record of the information under management providing a clear indication of the information under management
- The agreement number, Vendor and End-user to which specific data, records and information relates
- Documented procedures for gaining authorised access to the information
- Any instructions that alter the conditions of storing and releasing data from that which is documented within HES040119 Harbinger Escrow Services Release Event Process
- Any exemption clauses that preclude access to the information under law.

2.2.5 Access & Correction:

We must, subject to certain exceptions, provide customers with access to the data, records and information we hold concerning them if requests for information are made under:

- Privacy Act 1988 (Cth)
- Subpoena, warrant or court order

Where a customer requests access to data, records and information, report the request to the Vault Manager who will coordinate Harbinger's response or redirect the enquiry to an appropriate officer within Harbinger.

2.2.6 Deposit Materials and Additional Materials:

Special steps must be taken when managing and handling Deposit Materials and Additional Materials. This material includes secrets and other confidential data, records and information that belongs to Harbinger's customers. The treatment of this data must be in accordance with and subject to strict process flow.

For further or more specific information regarding the management and handling of Deposit Materials and Additional Materials:

- refer to HES040119 Harbinger Escrow Services Release Event Process,
- contact the Vault Manager defined in Section 6 Roles, Responsibilities and Contacts.

3 Compliance Statement

All data, records and information must comply with this policy.

4 Background Material & References

Harbinger Escrow Services is committed to the adoption of best-in-class information management practices. These practices are required to protect Harbinger's operating information and data stored on behalf of its customers. This policy provides guidance on how to manage the information management requirements relating to the Privacy Act 1988 (Cth).

To obtain clarification on any data, records and information issue not addressed in this policy, contact the Managing Director – Harbinger Group Pty Ltd.

5 related documents

HES040110 Harbinger Escrow Services IT Systems Security Policy

HES040112 Harbinger Escrow Services Third Party Network Connection Policy

HES040113 Harbinger Escrow Services Information Classification Scheme

ES040114 Harbinger Escrow Services Software Security Policy

HES040170 Archival Policy

HES050003 Data Maintenance and Cleansing 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 22-07-2008.
Change Authority (Authority to change the Policy or give exception waivers)	Vault Manager, Harbinger Escrow Services Please write to vaultmanager@harbinger.com.au for alteration and authorisation of changes and waivers to this policy.
Business Sponsor	Managing Director, Harbinger Escrow Services
Owner (Responsible for the implementation and enforcement)	Vault Manager, Harbinger Escrow Services
Author	Harbinger Group Pty Ltd
Further information	Please contact: Vault Manager, Harbinger Escrow Services vaultmanager@harbinger.com.au
Specific Roles	A staff member to spot check and audit the compliance with this policy throughout the organisation.

7 Review Timetable

This policy will be reviewed every 12 months by the Vault Manager to ensure its currency and validity. Its next scheduled review will occur in April 2010.

8 Glossary

BIC	Business Information Committee
CIS	Corporate Information Strategy
DVM	Data Vault Management
CPO	Chief Privacy Officer
End-user	A named beneficiary to a valid escrow agreement
Vendor	A named party to a valid escrow agreement that has legal ownership of the data, records and information
Customer	A Vendor or End-user
Deposit Materials	A group of electronic data files that contains all of the objects nominated or described as Deposit Materials in an Escrow Agreement that contain the critical and important items which the End-User requires to be held in escrow. The group of files is compressed, encrypted and is associated with a Lodgement data file
Additional Materials	A group of electronic data files that contains all of the objects nominated or described as Additional Materials in an Escrow Agreement which contains necessary items the End-User requires to be held in escrow. The group of files is compressed, encrypted and is associated with a Lodgement data file

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