DOC A5 Information Security Policy

Overview

The Board of Directors and senior management of Hornbill Ltd (Hornbill) are committed to preserving the confidentiality, integrity and availability of all physical and information assets owned and controlled by the company. This ensures Hornbill can preserve its competitive advantage, cash-flow, profitability, legal, regulatory and contractual compliance, encompassing commercial reputation.

Information and information security requirements will continue to be aligned with Hornbill's vision and strategic objectives. Hornbill is committed to implementing a Secure Operating Model structured and conformant with the internationally recognised standard for an Information Security Management System (ISMS) ISO/IEC 27001:2013.

The ISMS is intended to be an enabling mechanism for safeguarding commercially sensitive information and Personal Identifiable Information (PII) processed within electronic systems and manual filing systems, for reducing information-related risks to acceptable levels.

Definitions

In this policy information security is defined as:

> "Preserving the confidentiality, integrity, and availability of physical and information assets across Hornbill".

Confidentiality:

> This involves ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorised access to Hornbill's information and proprietary knowledge and its systems including networks, websites, and associated software applications.

Integrity:

This includes safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data.

Availability:

The information and associated assets should be accessible to authorised users when required, and therefore be physically secure. Internal and external networks must be resilient and Hornbill must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information.

Physical assets:

The 'physical assets' of Hornbill include, but are not limited to, networking hardware, data cabling, telephone systems, laptops, desktops, mobile phones, physical filing systems.

Information assets:

The 'information assets' include information printed or written on paper, transmitted by post, shown in films, or spoken in conversation, as well as information stored electronically on servers, the website, desktops, laptops, shared drives and mobile phones, as well as on CD ROMs / DVDs, USB sticks, backup tapes and any other digital or magnetic media, and information transmitted electronically by any means.

In this context, 'data' also includes the sets of instructions that tell the systems how to manipulate information (i.e. the software: operating systems, applications, system utilities, etc).

Security breach:

A 'security breach' is any incident or activity that causes, or may cause, a break down in the confidentiality, integrity, or availability of the physical or information assets of Hornbill.

Objectives

Hornbill operates an ISMS which complies with ISO/IEC 27001:2013 across all its products and services and meets the requirements of the;

- Data Protection law (UK DPA 98).

Where security management controls are required over and above the ISMS baseline the policy of the company is to review the risks which will inform any improvement activities and capability to be incorporated into the ISMS.

The objectives of this policy are:

- Safeguard and protect Hornbill's customer information and commercially sensitive information within its custody, ensuring the preservation of the confidentiality, integrity and availability of the data;
- Establish safeguards to protect Hornbill's information resources from theft, abuse, misuse or any form of damage;
- Establish responsibility and accountability for information security across Hornbill;
- Encourage Hornbill's management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimise the occurrence and severity of security incidents;
- Ensure that Hornbill is able to continue its commercial activities in the event of significant information security incidents; and
- Achieve and maintain accredited certification to ISO/IEC 27001:2013.

These high level objectives are supported by the following subsidiary objectives:

- Ensure consistency in practices across Hornbill, including facilitating continual improvement;
- Ensuring information security training is available to all staff;
- Ensuring information security is considered in defining and assessing Hornbill's relationship with clients and third party suppliers;
- Ensure timeliness of reporting and responding to information security incidents and events;
- Ensure and demonstrate on-going compliance with relevant legislation e.g. Data Protection Act 1998; and
- Ensure that business continuity plans are formed, maintained and tested.

These objectives require, amongst other measures, that:

- Senior management provide verifiable commitment and continuing support for the Hornbill's ISMS;
- Information security training is available to all staff upon induction and as a refresher cycle;
- Customer and supplier relationships are built on contractual terms which include an information security focus;
- All breaches of information security, actual or suspected, are reported to, and investigated by the nominated security investigation team;
- All applicable legislation is identified and measures are put in place to confirm Hornbill's level of legal compliance; and
- Robust business continuity plans are in existence and staff are aware of their accountability and responsibilities.

Responsibilities

The Hornbill UK Chief Executive Officer (CEO) is accountable for ensuring compliance with this policy including allocation of resources and responsibilities for implementation and compliance.

The CEO delegates authority to Jeffrey Smith for overseeing the control and effectiveness of Hornbill's ISMS.

The Directors and managers are responsible for implementing the policy, monitoring of compliance and reporting performance.

Operational groups exist within the respective lines of responsibility for co-ordinating information security efforts and aligning activity to ensure continual improvement and overall ISMS effectiveness at a strategic and operational level.

Senior management, full and part time employees, sub-contractors, project consultants and any other external parties have, and will be made aware of, their responsibilities to preserve information security, to report security breaches, and to act in accordance with the requirements of the Hornbill's ISMS. The consequences of security policy violations are described in Hornbill's disciplinary processes contained with the HR policy.

All employees will receive information security awareness training and specialist employees will receive appropriately focused training as required to meet Hornbill's business, contractual, and regulatory requirements and obligations.

Risk Management

The Hornbill strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and the maintenance of an ISMS. The Risk Assessment, Risk Treatment Plan (action plans), and Statement of Applicability (SoA) identify how information-related risks are managed.

Supporting Policies and Procedures

Supporting policies and procedures are available in the context of Hornbill's ISMS and should be read in conjunction with this policy. Key areas deemed essential for effective security control cover; technical vulnerability management, business continuity / contingency planning, management of information security incidents etc.

Associated policies and procedures can be found on the Hornbill intranet.

Compliance

All employees of Hornbill and relevant external third parties are expected to comply with this policy and with the ISMS that implements this policy. All employees and external parties (where applicable), will receive appropriate information security training.

The ISMS is subject to continuous, systematic review and improvement.

This policy will be reviewed to respond to any changes in the Hornbill ISMS risk environment.

Document history

Version	Date	Changes	Other policies affected	Approved by
1.0	10/07/2012	Initial Issue		Gerry Sweeney
2.0	16/03/2015	Update to 2013 standard		Gerry Sweeney