HUNTSWOOD

INFORMATION SECURITY POLICY ASSOCIATE VERSION

APPROVAL CONTROL

ROLE	NAME	DATE
CEO	Matthew Bonfield	28/02/2018
Chief Technology and Risk Officer	Steve Mills	28/02/2018

VERSION CONTROL

VERSION	AUTHOR NAME	VERSION CHANGES	DATE
0.1	Ethan Moore	Draft of new policy	22/02/2018
1.0	Matthew Bonfield	Sign Off	28/02/2018
1.02	Ethan Moore	Minor wording updates	22/03/2018

TABLE OF CONTENTS

OBJECTIVE

This policy is based on ISO27001:2013 the recognised international standard for information security. This standard ensures that Huntswood CTC Ltd. complies with the following security principles:

TERM	PRINCIPLES
Confidentiality	All sensitive information will be protected from unauthorised access or disclosure
Integrity	All information will be protected from accidental, malicious and fraudulent alteration or destruction
Availability	Information will be available throughout the times agreed with the users and be protected against accidental or malicious damage or denial of service

APPLICABILITY

This policy applies to all of Huntswood CTC Ltd and to Huntswood representatives

MANAGEMENT RESPONSIBILITIES AND COMMITMENT

Huntswood is committed to ensuring that all these aspects of information security are complied with to fulfil its statutory functions.

Huntswood management are committed to satisfy all applicable requirements within this policy and to the continual improvement of the Information Security Management System ('ISMS'), and therefore have established this policy so that:

- it is appropriate to the purpose of the organisation
- it includes information security objectives and provides the framework for setting continual information security objectives

This information security policy shall be available as documented information; be communicated within the organisation; and be available to interested parties, as appropriate.

Compliance with this policy and all other security policies and procedures is mandatory for all Huntswood representatives.

The Chief Executive Officer approves this policy. The Information Security Working Group has the responsibility for ensuring that the policy is implemented and adhered to across the business covered by the scope of the ISMS.

The security policy confirms Huntswood's commitment to continuous improvement and highlights the key areas to effectively secure its information.

LEADERSHIP AND COMMITMENT

Huntswood management will continue to demonstrate leadership and commitment with respect to the information security management system by:

- ensuring the information security policy and information security objectives are established and are compatible with the strategic business direction of the organisation
- ensuring the integration of the information security management system requirements into the organisation's processes
- ensuring that the resources needed for the information security management system are available
- communicating the importance of effective information security management and of conforming to the information security management system requirements
- ensuring that the information security management system achieves its intended outcome(s)
- directing and supporting persons to contribute to the effectiveness of the information security management system
- promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility and accountability

INFORMATION SECURITY OBJECTIVES

Information security objectives have been established and are compatible with the strategic direction of the organisation. The key objective is to work in line with the sections of the information security standard ISO 27001:2013 detailed below.

Furthermore, security objectives will be set by management as an ongoing task and at ISMS Management Review Meetings and an Information Security Objectives Policy will be produced and implemented as part of the ISMS.

Management objectives for Information Security will be continually set and monitored to ensure they are achieved.

POLICY PRINCIPLES

Organisation of Information Security
The importance attached to information security within Huntswood is demonstrated by the existence of the Information Security Working Group. The function of the Information Security Working Group is outlined below:

- reviewing and progressing strategic security issues
- establishing relationships outside of Huntswood with other security advisers
- assessing the impact of new statutory or regulatory requirements imposed on Huntswood
- monitoring the effectiveness of the Information Security Management System ("ISMS") (e.g. from the results of Internal Audit reports and Security Incident Reports)
- recommending /endorsing changes to the ISMS

The Information Security Working Group meets regularly to address the above activities in order to assure the continuing effectiveness of Huntswood ISMS. The review process is defined in the 'Information Security Working Group Policy'.

Human Resource Security
All Huntswood representatives must sign up to the Acceptable Usage Policy which requires them to work in accordance with all policies and procedures which includes information security specific requirements. Furthermore, the Acceptable Usage Policy ensures that Huntswood representatives are made aware that they are required to follow best practices regarding information security established by Huntswood.

All new starters must be trained on procedures in the areas described above as part of their induction programme. Ongoing training must be provided in the form of a programme of regular updates and training sessions. There is also a procedure to disable the network account and recover all items of property for Huntswood leavers.

Asset Management
Huntswood information must be classified according to its sensitivity and an information owner assigned. Classification shall be undertaken in line with the Classification and Labelling Policy.

Access Control
Huntswood representatives must be aware of and follow a number of controls and procedures, which exist to limit access to confidential information. The Huntswood Technology Team are responsible for both establishing and maintaining robust logical access controls as defined by the information asset owners. An Access Control Policy must be in place and complied with by all Huntswood representatives and third parties.

Cryptography
Where cryptographic controls are employed by Huntswood a policy on the use of cryptographic controls for protection of information must be developed and implemented.

Physical and Environmental Security
Huntswood representatives must be aware of and follow the detailed set of measures, controls and procedures that exist to ensure adequate control of physical security. These include;

- building and individual alarm systems
- restricted access to the building and further restricted access within it
- secure lockers, drawers, safes and storage, fireproof storage
- secure offsite backups and archiving
- clear desk and clear screen policy – Acceptable Usage Policy

Operations Security
Huntswood will ensure correct and secure operations of information processing facilities.

Communications Security
Huntswood representatives must be aware that the use of technology and communications are established, controlled and managed by the Huntswood Technology Team. The Technology Team is responsible for ensuring that the appropriate security measures and processes are in place. Huntswood will ensure that security around the network, mobile and remote working are adequately protected.

System Acquisition, Development and Maintenance
The Huntswood Technology Team must ensure that the appropriate information security processes are included in all technology projects. A secure development approach including policy, procedures and environment and testing will be implemented.

Supplier Relationships
Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets must be agreed with the supplier and documented.

Information Security Incident Management
Security incident management records must be centrally maintained, updated and monitored. Huntswood representatives must be aware of what constitutes an actual or potential security incident, how to report the incident and who to report the incident to.

The responsibility for the oversight of breaches of technical and physical security rests with the Information Security Manager.

Information Security in Business Continuity Management
Huntswood shall ensure a consistent and effective approach to the management of major information security incidents, including communication on security events and weaknesses and the implications for business continuity management.

Compliance
Huntswood must take technical and organisational measures to protect personal data against accidental or unlawful destruction, or accidental loss or alteration, and unauthorised disclosure or access. As well as avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Huntswood takes measures that are intended to ensure that anyone managing and handling personal data understands that they are contractually responsible for following good data protection practice and appropriately trained to do so.

TABLE OF DEFINITIONS

The table of definitions provides definitions of terms used within the policy document.

TERM	DEFINITION
Huntswood Representative	Permanent, temporary and fixed term employees, consultants, contractors, agents and subsidiaries acting for, or on behalf of Huntswood

POLICY RESPONSIBILITIES

The following table defines the business roles and their responsibilities in regard of the policy document.

RESPONSIBILITY	ROLE	DEFINITION
Owner	Chief Executive Officer	The Owner ensures the policy is reviewed and maintained on a regular basis
Reviewer	Risk & Audit Committee Informaiton Security Working Group	The Reviewer ensures the policy document aligns with relevant legislation and company requirements
Author	Information Security Manager	Shall update the policy document in a succinct time frame on receiving updates from the reviewer and in accordance with company policy writing guidelines
Policy Audience	Huntswood Representatives, Contractors & Third parties	Must apply the business policy to the business they undertake on behalf of Huntswood

Due to the potential serious nature of any information security incident, after investigation, any person found to be negligent will face the disciplinary process, which may lead to dismissal or termination of contract.

APPLICABLE STANDARDS AND LEGISLATION

ISO/IEC 27001:2013

Data Protection Act 1998