The Commercial Group

Information Security Policy

High Level Information Security Policy

Document reference: ISMS 00

Document version: 1.8

Classification: Confidential

Applies to:	All Commercial Group Staff and Third Parties
Reviewed / Updated	January 2021
Next Review Date:	January 2022

Document Control

Title	Information Security Policy
Author / Originator	*Paul Hutchings*
Business Area	*Information Security*

Change Control

Version	Date	List Changes made to document	Document Status
1.0	*July 2011*	*New Document*	*Final Draft*
1.1	September 2013	Update IS Manager Name	Draft
1.2	September	Approved draft	Issued
1.3	January 2014	Fix typos and changed to Confidential	Issued
1.4	June 2014	Control alignment	Issued
1.5	February 2015	Review and update for ISO 27001:2013	Issued
1.6	March 2017	Re brand	Electronic
1.7	January 2019	Review, Document location updated	Issued
1.71	January 2020	Review	Issued
1.8	January 2021	Review and Update	Issued

Document Ownership

The Commercial Group's IT Director is the owner of this document, and is therefore responsible for ensuring that this policy is reviewed in line with the review requirements of the Commercial Group Information Security Management System.

1 OBJECTIVES

The Commercial Group's objectives of Information Security are to ensure business continuity and minimise business damage by the preventing and minimising the impact of security incidents. In deploying the Information Security Management System ("ISMS"), the Commercial Group's Board of Directors aims to reduce information security risks to an acceptable level.

2 POLICY

The purpose of the Information Security Policy is to protect both the organisation's and its customers' Information Assets from information security threats, whether internal or external, deliberate or accidental.

It is Commercial Group Policy

- Information and data will be protected against loss, damage and unauthorised access.
- The Confidentiality of information and data will be maintained.
- The Integrity of information and data will be maintained.
- Business requirements for the availability of information, data and information systems will be met.
- All applicable statutory, regulatory and legislative requirements will be identified and effectively implemented.
- Disaster Recovery plans will be produced, maintained and regularly tested for appropriateness and effectiveness.
- Mandatory Information security awareness and policy training will be undertaken when required, also contractors where appropriate.
- All information security events and incidents, actual or suspected, are to be reported to and investigated by the Information Security Manager.
- Appropriate continual information security improvement will be implemented.

3 IMPLEMENTATION

- Detailed Information Security Policies and Procedures are documented in the ISMS to support staff in the implementation of this policy covering all aspects of the organisation's business activities including human resources, change control, physical security, operational security and business continuity.

4 RESPONSIBILITIES

- The Managing Director and the Board of Directors are responsible for agreeing the overall Company strategy and commitment to Information Security, for establishing and approving this High Level Information Security Policy, and for providing adequate resource for the establishment, implementation, monitoring, improvement and effectiveness of the ISMS.
- The Information Security Manager has direct responsibility for maintaining this High Level Information Security policy, the ISMS, its associated policies, procedures and standards and for providing advice and guidance on their implementation.
- The Senior Management Team is responsible for the management of information security risks and for associated decision making.
- The Information Security Forum is responsible for the management, monitoring and appropriated continual improvement of the ISMS on behalf of the Board of Directors.
- All managers within the Company are directly responsible for the implementation of ISMS policies, procedures and standards within their business areas as applicable, and for adherence by their staff.
- All Company staff and agency approved users are responsible for the effective implementation of the ISMS policies, procedures and standards applicable to their activities.

Arthur Hindmarch, Chairman Date: 5th January 2021