INTRODUCTION

This Data Security and Protection policy is applicable to Rhino Engineering Group Limited (REGL) and all subsidiary companies including Rhino Systems Limited (RSL), Rhino Site Systems Limited (RSSL) and Rhino HySafe Limited.

The policy commits REGL to meeting applicable data protection laws such as the EU's General Data Protection Regulation (GDPR) and outlines organisational measures for protecting sensitive and critical data, such as personal information or client provided security documentation.

Data Security and Protection is managed by the Rhino Group Commercial Director assisted and advised by an IT Support Consultancy to protect REGL's IT infrastructure.

PURPOSE

REGL will restrict access to confidential and sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers, incurring penalties for non-compliance or suffering damage to our reputation. At the same time, users will require access to data as required for them to work effectively.

It is not anticipated that this policy can eliminate all malicious data theft. Its primary objective is to increase user awareness and avoid accidental loss scenarios, so it outlines the requirements for data breach prevention.

SCOPE

In Scope

This data security policy applies all electronic or printed personal and/or and customer data. In the case of electronic data, it applies to every server, database and IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks. Users should also apply security measures to printed data.

Out of Scope

Information that is classified as Public is not subject to this policy. Other data can be excluded from the policy by company management based on specific business needs, such as that protecting the data is too costly or too complex.

POLICY

Principles

The company shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible.

Electronic Data

General

a) Each user shall be identified by a unique user ID so that individuals can be held accountable for their actions.
b) The use of shared identities is permitted only where they are suitable, such as training accounts or service accounts.
c) Each user shall read this data security policy paying particular regard to User Responsibilities.
d) Records of user access may be used to provide evidence for security incident investigations.
e) Access shall be granted based on the principle of least privilege, which means that each program and user will be granted the fewest privileges necessary to complete their tasks.

Access Control Authorisation

Access to company IT resources and services will be given through the provision of a unique user account and password. Accounts are provided by the IT Support Consultancy based on details approved by the Group Commercial Director.

Passwords are managed by the IT Support Consultancy.

Network Access

a) All employees shall be given network access in accordance with business access control procedures and the least-privilege principle.
b) Network routing controls shall be implemented to support the access control policy.

User Responsibilities

a) All users must lock their screens whenever they leave their desks to reduce the risk of unauthorized access.
b) All users must keep their workplace clear of any sensitive or confidential information when they leave.
c) All users must keep their system access passwords confidential and not share them.

Application and Information Access

a) All company staff shall be given access to the data and applications required for their job roles.
b) All company staff shall access sensitive data and systems only if there is a business need to do so and they have approval from higher management.
c) Sensitive systems shall be isolated in order to restrict access to authorized personnel only *(e.g. accounts data, personnel data, etc.).*
d) Information to contactors may be forwarded by e-mail if necessary for the task in hand. Contractors shall not be given direct access to company IT systems.

Access to Confidential, Restricted information

a) Access to data classified as 'Confidential' or 'Restricted' shall be limited to authorised persons whose job responsibilities require it, as determined by higher management.
b) In the case of client based information, access privileges shall be by agreement between the Project Lead and the client.
c) The responsibility to implement access restrictions lies with the Group Commercial Director.

Paper Data & Records

a) Paper data and records shall be treated securely.
b) Confidential or restricted records printed on communal printers shall be collected promptly by the user.
c) Any confidential or restricted information shall not be left 'lying about' on desks.
d) Paper records of confidential or restricted information shall be filed in a secure location.

OWNERSHIP AND RESPONSIBILITIES

- **Data owners** are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.
- **Users** include everyone who has access to information resources, such as employees, trustees, consultants, temporary employees and volunteers.
- **Group Commercial Director** is responsible for liaison with the IT Support Consultancy and controlling access of individuals to electronic information resources.
- **IT Support Consultancy** is an external company that provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources. More specifically it provides advice / technical support regarding IT systems, cloud services, cyber security controls, communications and infrastructure and backup & disaster recovery.
- **CIS LTD.** is the IT Support Consultancy used by REGL at the time authorisation of this policy.

ENFORCEMENT

Any user found in violation of this policy will be subject to disciplinary action, up to and including termination of employment.

Any third-party partner or contractor found in violation of this policy may have their contract terminated.

Stuart Lawrence **Policy Confirmed 30 November 2021**

Group Managing Director