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 UK'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 and supply chain security.

PURPOSE

REGL will restrict access to confidential, Restricted and Official Sensitive data to protect it from being lost or compromised in order to avoid adversely impacting our customers or the wider supply chain, 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.

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.

The company shall make employees aware of their responsibilities by suitable training at the start of employment. Training will be updated at least annually or when policies are modified and guidance is required. Records of training shall be maintained. Employees to whom these policies apply will be required to sign off annual acceptance of the policies.

The company will provide users at an appropriate level and frequency with Cyber Awareness Training and/or use relevant information security awareness campaigns promoted by the NPSA. Training may include simulated phishing testing and other information security checks.

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.
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 and generated using a random password generator. Passwords will be passed to the Group Commercial Director for supply to the user. Passwords will be set to "change at next logon" to allow the user to set a password secret known only to them.

Password length is set to a minimum of 10 characters and must be complex (passwords must contain three of the following – Capital Letter, Lowercase Letter, Number or Character)

Password recycling is discouraged, and this is enforced by the previous 24 passwords being remembered so they cannot be reused. Minimum password age is set to 1 day.

In the event of passwords or information being compromised, the Group Commercial Director should be advised, and the IT Support Consultancy informed. The IT Support Consultancy will coordinate activities to secure the breach and with the Group Commercial Director, assess any potential risks to the business.

In the case of Ministry Of Defence Identifiable Information (MODII) being breached, the External Security Contacts identified in the REGL Business Continuity Plan (BCP-01) Section 13 must be informed by the Group Commercial Director.

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 take precautions to ensure their display screens cannot be overlooked through windows by unauthorized persons (e.g. by using blinds or aligning screens away from the window).

c) All users must keep their workplace clear of any sensitive or confidential information when away from their desks or at the end of the day.
d) All users must keep their system access passwords confidential and not share them.
e) All users must report any issues with their company provided IT equipment to the REGL IT Support Consultancy. Specifically, any issues with the Antivirus and Malware Protection software installed.
f) All users must report any suspected or perceived weaknesses in any IT System to the Group Commercial Director in the first instance.

Application and Information Access

a) Company staff shall be given access to the data and applications required for their job roles.
b) Users may use applications on mobile devices to assist their work activities provided they have been downloaded from the device's native app store.
c) 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. This access will be reviewed at least annually for all staff. Access will also be reviewed following any significant role change.
d) Sensitive systems shall be isolated in order to restrict access to authorized personnel only *(e.g. accounts data, personnel data, etc.).*

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.

Information Transfer

All documents and drawings received from 3rd Parties with a classification of Official Sensitive shall not be shared with any other 3rd Party or outside of a project team who have authorised access.

Any information or drawings produced by REGL and shared with 3rd parties shall not contain any information shared of an Official Sensitive nature and will only contain necessary details required for the 3rd party to carry out their work.

All documents shared to 3rd parties will be recorded.

Cryptographic Keys

Cryptographic keys are required to secure websites, provide repudiation, and to encrypt data. They may be utilised and stored on the Companies behalf by 3rd parties to provide services. Keys will be managed in the following manner by our 3rd party suppliers.

Access to cryptographic keys is restricted to authorised staff only of the 3rd Party providers, the Rhino Group Commercial Director and Rhino Group Managing Director

Procedures are in place to ensure that requests for cryptographic keys are appropriately authorised by the Rhino Group Commercial Director, provided in a timely manner and appropriately recorded.

Cryptographic keys are securely managed and protected though their whole lifecycle from initial generation and storage to archiving, retrieving, distributing, retiring and eventual destruction.

Cryptographic algorithms, key lengths and use is in accordance with professional best practices.

Cryptographic keys are protected through their whole lifecycle against modification, loss, unauthorised access/use or disclosure by the 3rd party.

Equipment used to generate, store and archive keys is physically protected using appropriate, secure access controls.

Awareness of encryption/decryption passwords for systems is limited to authorised personnel only.

In the event of a cryptographic key being compromised, the existing key must be revoked and a new key (or key pair) must be generated.

Access to Confidential, Restricted, or Official Sensitive information

a) Access to data classified as 'Confidential', 'Restricted' or Ministry of Defence (MOD) 'Official - Sensitive', 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.
d) Access to MOD Official Sensitive information is restricted to employees who are cleared to HMG Baseline Personal Security Standard.
e) Employees who leave the business are reminded they continue to be subject to this Data Security and Protection Policy and must continue to keep information confidential.
f) Information classified as Official-Sensitive must not be written to physical or removable media.

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.

- **CSG Ltd.** is the IT Support Consultancy used by REGL at the time of 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.

Infringements under the Official Secrets Act by employees, third party partners, or contractors could result in criminal prosecution.

Stuart Lawrence
Group Managing Director