Information Security Policy

RHG Consult Ltd, Harborough Innovation Centre, Market Harborough, LE16 7WB
Tel: 0345 603 9311 www.rhgconsult.co.uk Reg No: 4776603

Introduction

RHG Consult Ltd (RHG) is committed to ensuring the confidentiality, integrity, and availability of its information systems and data. This Information Security Policy establishes the framework for safeguarding RHG's information, whether it is stored electronically, physically, or transmitted over networks. All employees, contractors, and third parties who access or use the RHG's information are expected to comply with this policy.

Purpose

The purpose of this policy is to:

- Protect the RHG's information from unauthorised access, disclosure, alteration, or destruction.
- Ensure compliance with relevant legal, regulatory, and contractual requirements related to information security.
- Mitigate the risks to the RHG's information assets and systems.
- Establish a culture of security awareness within the organisation.

Scope

This policy applies to all employees, contractors, consultants, temporary staff, and any third parties who have access to the RHG's information systems and data, both internal and external. This policy covers all forms of information, including digital and physical records, emails, communications, and any other business-critical data.

Roles and Responsibilities

- **Directors**: The Directors are responsible for the overall implementation and monitoring of this policy, including managing risks, conducting regular security audits, and ensuring compliance with legal and regulatory requirements.
- **Employees**: All employees are responsible for adhering to the guidelines and procedures set forth in this policy, including protecting sensitive data and reporting security incidents.
- **Managers**: Managers are responsible for ensuring that all staff members within their teams are aware of and comply with this policy. They should also assist in implementing security practices in day-to-day operations.
- **Third Parties**: Any third-party vendors or partners with access to the RHG's data must adhere to the requirements outlined in this policy and the terms specified in any data protection or security agreements.

Data Protection and Privacy

- **Personal Data**: RHG will adhere to the principles set out in the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 for the processing of personal data. Personal data will be handled and processed only for legitimate business purposes and will be protected from unauthorised access, loss, or misuse.

- **Data Minimisation**: Only the minimum amount of data necessary for business operations will be collected and processed. Data will not be retained for longer than is necessary for the purpose for which it was collected.

- **Data Access**: Access to sensitive or personal data will be restricted to those employees who require it to perform their duties. Access controls will be in place to ensure that data is protected from unauthorised access.

Data Retention

- **Personal Data:** RHG only keep personal data for as long as long as necessary for the purpose we have stated. Awarding bodies and Awarding Bodies and UK funding agencies may require RHG to retain personal information for a duration defined by statutory requirements.

    - **ESFA:** Learner files should be retained securely for 6 years from Financial Year End after end of course, qualification or apprenticeship
    - **Awarding bodies:** Learner files should be retained for 7 years from the date of learner registration

Access Control

- **User Access Management**: All users must have a unique user ID and strong password. Access to systems and data will be granted based on job roles and the principle of least privilege. Access rights will be regularly reviewed to ensure appropriateness.

- **Authentication**: Strong authentication methods (e.g., multi-factor authentication, where applicable) will be used for accessing sensitive or critical systems.

- **Remote Access**: Employees working remotely or from other locations must use secure Virtual Private Network (VPN) connections to access the RHG's internal systems. Personal devices must be secured according to the RHG's device security guidelines.

Physical Security

- **Office Premises**: Physical access to the RHG's office premises will be restricted to authorised personnel only. Visitors must be met in reception and escorted by an RHG member of staff at all times.

- **Device Security**: Devices such as laptops, desktops, and mobile phones must be securely stored when not in use. Employees must not leave sensitive information unattended in open spaces.

- **Data Destruction**: When data is no longer required, it will be securely destroyed. This applies to both physical (e.g., paper) and electronic (e.g., hard drives) media.

Incident Response

- **Reporting**: All employees must report any security incidents or breaches immediately to the Directors or their line manager. This includes any loss of data, unauthorised access, suspicious activity, or system malfunction.
- **Incident Management**: RHG will maintain an Incident Response Plan to guide the response to and resolution of security incidents. All incidents will be documented and investigated to prevent recurrence.

Risk Management

- **Risk Assessment**: Regular risk assessments will be conducted to identify potential threats to the RHG's information systems and data. Appropriate controls will be implemented to mitigate identified risks.
- **Business Continuity**: RHG will maintain a Business Continuity Plan (BCP) to ensure the continuity of critical business operations in the event of a major incident or disaster.

Training and Awareness

- **Employee Training**: All employees will receive regular training on information security best practices, including recognising phishing attacks, handling sensitive data, and reporting security incidents.
- **Ongoing Awareness**: Information security awareness campaigns and annual refresher training will be conducted to ensure employees stay informed about evolving threats and the RHG's security practices.

Compliance

RHG will comply with all applicable legal, regulatory, and contractual information security requirements, including but not limited to:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The UK Computer Misuse Act 1990
- Industry standards and best practices

Security Policy Enforcement

Non-compliance with this policy will result in disciplinary action, which may include warnings, termination of employment, or legal action depending on the severity of the breach. Violations will

be investigated thoroughly, and corrective measures will be taken to address weaknesses in the security program.

Policy Review and Updates

This policy will be reviewed annually, or more frequently if necessary, to ensure it remains up to date with changes in the business environment, emerging security threats, and updates to laws or regulations. Any changes to this policy will be communicated to all employees.

Signed: 

Name: Lee Patterson

Position: Managing Director

Date: 29/10/2024

Date of next review: 28/10/2025