CRA RECRUITMENT SPECIALISTS

Specialists in Legal and Financial Recruitment

Information Security Policy

1. Introduction

This Information Security Policy outlines the principles, guidelines, and responsibilities governing the security of information assets at CRA Consulting Limited . This policy is designed to ensure the confidentiality, integrity, and availability of information. All employees, contractors, and third-party stakeholders are required to adhere to this policy.

2. Information Security Objectives

- Safeguard the confidentiality of sensitive information from unauthorized access or disclosure.
- Ensure the integrity of data by preventing unauthorised modifications.
- Maintain the availability of information systems and assets to support business opera-ons.
- Comply with relevant legal, regulatory, and contractual requirements pertaining to information security.
- Continuously improve the effectiveness of the information security management system (ISMS).

3. Information Security Responsibilities

Top Management: The senior management team is responsible for providing leadership, resources, and support for the establishment, implementation, and maintenance of the ISMS. They will also review and approve this policy periodically.

Information Security Manager: The designated Information Security Manager is responsible for developing, implementing, and managing the ISMS. This includes risk assessments, security controls, incident response, and ongoing monitoring.

Employees: All employees are responsible for understanding and complying with the information security policies, procedures, and guidelines. They should report any security incidents, vulnerabilities, or breaches to the Information Security Manager.

4. Risk Management

A risk assessment process will be conducted regularly to identify, assess, and manage information security risks. Risks will be evaluated based on their potential impact and likelihood, and appropriate controls will be implemented to mi-gate or manage these risks.

5. Information Classification and Handling

All information assets will be classified based on their sensitivity, criticality, and regulatory requirements. Access controls, encryption, and other safeguards will be applied according to the classification level to prevent unauthorized access, disclosure, or loss.

6. Access Control

Access to information and information systems will be granted based on the principle of least privilege. Users will only be given access to resources necessary for their roles. Strong authentication mechanisms and access controls will be implemented to ensure authorized access.

7. Security Awareness and Training

Regular training and awareness programs will be conducted to educate employees about information security best practices, risks, and their responsibilities. This will help in creating a security-conscious culture across the organisation.

8. Incident Response

An incident response plan will be established to address security breaches, incidents, and vulnerabilities. The plan will outline the procedures for identifying, reporting, and mitigating incidents, as well as for communicating with affected parties and regulatory authorities when required.

9. Compliance

CRA Consulting Limited is committed to complying with all applicable legal, regulatory, and contractual requirements related to information security. The ISMS will be regularly reviewed and updated to ensure alignment with evolving regulations and standards.

10. Continuous Improvement

Regular reviews and assessments of the ISMS will be conducted to identify areas for improvement. Feedback from security incidents, audits, and risk assessments will be used to refine security controls and enhance the effectiveness of the ISMS.

11. Policy Review

This Information Security Policy will be reviewed at least annually to ensure its relevance, adequacy, and effectiveness in addressing the organisation's security needs and evolving risks.

By adhering to this Information Security Policy, CRA Consulting Limited is committed to maintaining the confidentiality, integrity, and availability of its information assets while fostering a culture of security awareness and compliance.

CRA Consulting Reviewed January 2023

Directors

COO - Robert Addy

Caroline Naylor -Information Security Manager