INFORMATION SECURITY POLICY

CRI Group™ is a global leader in Employee Background Checks, Due Diligence, Risk Management and Investigative Solutions.

Corporate Research and Investigations Limited (CRI Group™) has been safeguarding businesses from fraud, bribery and corruption since 1990. Globally, we are a leading Compliance and Risk Management company licensed and incorporated entity of the Dubai International Financial Center (DIFC) and Qatar Financial Center (QFC).

CRI Group ensures the confidentiality, integrity, and availability of information and personally identifiable information (PII) by protecting against all types of threats and meeting all legal, regulatory, and contractual obligations.

OBJECTIVE

The purpose of CRI Group's Information Security Policy is to ensure business continuity and minimize damage caused by security incidents. The policy, compliant with ISO 27001:2022, BS 7858:2019, BS 102000:2013, and legal frameworks such as DIFC Law No. 1 of 2007, GDPR 2016/679, and Singapore's PDPA 2012, aims to protect CRI Group’s Information Assets from all internal and external threats. This includes limiting access to authorized individuals, ensuring operational continuity, and implementing controls to prevent and minimize the impact of security incidents.

POLICY

CRI Group’s Information Security Policy ensures the following:

1. **Confidentiality, Integrity, and Availability (CIA):**

   - Information assets shall be safeguarded to ensure confidentiality, integrity, and availability at all times.

   - Data classification will follow the CIA value and will be categorized as Confidential, Restricted, Protected, or Public.

2. **Data Protection and Access Control:**

   - Information shall be protected against unauthorized access, modification, or destruction, and handled according to its classification.

- Access to data will be limited to those with a legitimate business need and in line with appropriate access control mechanisms.

3. **Cybersecurity:**

- Robust cybersecurity measures will be implemented to protect CRI Group's digital infrastructure from malware, ransomware, phishing, and other cyber threats.
- Regular monitoring, detection, and response procedures shall be in place to mitigate cybersecurity incidents.
- Systems, networks, and applications will undergo regular vulnerability assessments and penetration testing to identify and remediate any security weaknesses.
- Multifactor authentication (MFA), encryption, and endpoint protection will be mandatory for all critical information systems.

4. **Incident Management:**

- All information security breaches, including cyber incidents, will be promptly detected, reported to the IT & ISMS Manager, and escalated to the Information Security Committee for investigation and corrective action.

5. **Awareness and Training:**

- Information security awareness training shall be provided to all employees and third parties, covering key aspects such as data protection, cybersecurity threats, classification, and access control.

6. **Regulatory Compliance:**

- CRI Group will meet all applicable ethical, regulatory, and legislative requirements concerning data protection and information security.

7. **Employee Responsibility:**

- Employees and third parties must always comply with this policy. Non-compliance may result in disciplinary actions, including termination.
- Suitable, anonymous reporting channels will be provided for employees to report any security incidents or vulnerabilities without fear of retaliation.

8. **Continuous Improvement:**

- The ISMS will be continually improved to adapt to emerging security threats and regulatory changes.

MEASUREMENT

1. **Audits and Compliance Checks:**

- Compliance with this policy and all applicable controls shall be audited at least once every three years, with a focus on continuous improvement.

2. **Business Continuity Testing:**

- Business continuity plans shall be tested annually to ensure preparation for potential disruptions.

3. **Training and Awareness:**

- Regular information security and cybersecurity training will be provided to all employees at induction and periodically thereafter.

4. **Access Reviews:**

- Access to IT systems, secure areas, and sensitive data will be reviewed every 90 days.

5. **Risk Assessments:**

- Risk assessments will be conducted annually or in response to any significant incidents or system changes.

IMPLEMENTATION

Information may exist in various forms (electronic, printed, verbal, etc.). The   is responsible for maintaining and updating the Information Security Policy and ensuring compliance across the organization. Managers are accountable for implementing the policy within their departments, providing necessary resources, and ensuring adherence by their teams.

All employees and third parties working with CRI Group are responsible for complying with this policy and reporting any security weaknesses or incidents to the IT & ISMS Manager.

CRI Group is committed to continually improving the information security compliances for the protection and safeguarding of the information assets that come under the scope of CRI Group

- Information security and privacy policy is reviewed annually or after any change/update and approved by management.
- CRI Group defines information security and privacy policy to meet its objectives in accordance with the business's requirements and applicable laws and regulations.

ZAFAR I. ANJUM

Group Chief Executive Officer