Data and Cybersecurity Policy

1. Purpose

The purpose of this Data and Cybersecurity Policy is to establish guidelines and procedures to protect the confidentiality, integrity, and availability of sensitive information handled by Industrial Recruitment Partners. This policy applies to all employees, contractors, and third-party vendors.

2. Scope

This policy covers all forms of data, including but not limited to:

- Personal data of employees and clients
- Financial information
- Business operations and proprietary data
- Electronic communications

3. Responsibilities

- **Management:** Ensure compliance with this policy and allocate resources for data protection measures.
- **IT Partners:** Implement and maintain technical safeguards, monitor systems, conduct regular security assessments and provide advice and preventative solutions.
- **Employees:** Adhere to the policy, report incidents, and participate in training programs.

4. Data Classification

Data will be classified into three categories:

- **Public:** Information intended for public disclosure.
- **Internal:** Information used for internal operations, requiring limited access.
- **Confidential:** Sensitive information that requires strict access controls and protection measures.

5. Access Control

- **User Authentication:** Implement strong password policies (minimum of 8 characters, including uppercase, lowercase, numbers, and special characters). Multi-factor authentication (MFA) is required for access to sensitive data.
- **Role-Based Access:** Access to data will be granted based on the principle of least privilege, ensuring employees have only the access necessary for their roles.
- **Access Reviews:** Conduct periodic reviews of access rights to ensure they align with current job responsibilities.

6. Data Handling and Storage

- **Data Encryption:** All sensitive data must be encrypted during transmission and at rest using industry-standard encryption protocols.
- **Data Minimisation:** Collect and retain only the data necessary for business purposes. Regularly review and securely dispose of unnecessary data.
- **Secure Storage:** Store confidential information in secure locations, such as encrypted databases or secure cloud services.

7. Cybersecurity Measures

- **Firewall and Antivirus Protection:** Implement firewalls and regularly update antivirus software on all devices.
- **Regular Updates:** Ensure all software and operating systems are regularly updated and patched to protect against vulnerabilities.
- **Network Security:** Use secure Wi-Fi networks and VPNs for remote access.

8. Incident Response

- **Incident Reporting:** Employees must report any suspected data breaches or cybersecurity incidents immediately to the IT department.
- **Incident Response Plan:** Develop and maintain an incident response plan to address potential breaches, including identification, containment, eradication, recovery, and communication.

9. Training and Awareness

- **Cybersecurity Training:** All employees must complete annual cybersecurity training, covering topics such as phishing awareness, safe data handling, and incident reporting.
- **Ongoing Awareness:** Provide regular updates and resources on emerging threats and best practices for data security.

10. Compliance and Legal Obligations

- **Regulatory Compliance:** Adhere to applicable laws and regulations regarding data protection, such as GDPR, CCPA, and industry-specific standards.
- **Third-Party Agreements:** Ensure that contracts with third-party vendors include data protection clauses to safeguard shared information.

11. Policy Review and Updates

- **Regular Review:** This policy will be reviewed annually or as needed in response to regulatory changes, technological advancements, or emerging threats.
- **Employee Acknowledgment:** All employees must sign an acknowledgment form confirming they have read and understood the policy.

Peter Spark

Director

16th January, 2023