Information Security & Acceptable Use Policy

About IO Controls

Founded in 2004 and operating from offices in Milton Keynes, we specialise in Building Energy Management Systems offering Support Services, Project Delivery and Consultation.

Organisational Purpose

To make Building Energy Management Systems (BEMS) easy!

Organisational Vision

To provide all strategic and operational stakeholders with quality solutions through a highly engaged team working effectively and consistently.

Strategic Direction

We aim to generate profitable growth through organic and non-organic means around a core commitment to Quality, Customer Loyalty and Employee Engagement.

Policy Introduction

This policy outlines the Information Security and Acceptable Use guidelines for IO Controls Ltd. It ensures the protection of information assets and the responsible use of company resources. The policy is designed to meet the standards set by British Land and other relevant regulations.

Scope

This policy applies to all employees, contractors, and third parties who access IO Controls Ltd. systems and data. It covers all information assets, including hardware, software, networks, and data.

Objectives

- Protect the confidentiality, integrity, and availability of information assets.
- Ensure compliance with legal, regulatory, and contractual requirements.
- Promote responsible and secure use of company resources.
- Prevent unauthorized access, disclosure, alteration, or destruction of information.

Roles and Responsibilities

Management:

- Approve and support information security initiatives.
- Ensure compliance with this policy.

Information Security Officer:

- Oversee the implementation of this policy.
- Conduct regular security assessments and audits.
- Ensure staff receive regular cyber awareness training.

Employees and Contractors:

- Comply with this policy and report any security incidents.
- Protect their authentication credentials and use resources responsibly.

Information Security Policy

1. Risk Management

- Identify, assess, and manage information security risks.
- Implement risk mitigation measures and monitor their effectiveness.

2. Access Control

- User accounts must be authenticated to a single individual using unique identifiers.
- Implement a formal authorization process for creating, amending, and deleting accounts.
- Conduct regular user access reviews to validate appropriateness.
- Implement mover and leaver controls to amend or remove access promptly.
- Suspend dormant accounts not used for 60 or more consecutive days.

3. Data Protection

- Encrypt confidential and personal data at rest and in transit using industry standards.
- Maintain accurate Records of Processing (RoP) for personal data.
- Ensure secure destruction of information no longer needed.

4. Incident Management

- Document and communicate an incident management process.
- Report security incidents to the Information Security Officer within 24 hours.
- Maintain an incident log and review it regularly.

5. Backup and Recovery

- Conduct regular backup and restoration tests.
- Ensure backups are secure and recoverable.

6. Physical and Environmental Security

- Protect physical assets from unauthorized access, damage, and interference.
- Implement measures such as locked cabinets, access controls, and surveillance.

7. Network Security

- Maintain an updated network architecture diagram.
- Implement intrusion prevention and firewall protections.
- Regularly review and update firewall rules.

8. Penetration Testing

IO Controls will assist customers who conduct their own penetration testing using independent, reputable security providers. After these tests are completed, IT Security Teams follow up with IO Controls to ensure that any identified issues are resolved promptly.

Responsibilities:

- Cooperate with the customer's IT Security Team during the follow-up process.
- Address and remediate any identified vulnerabilities in a timely manner as specified by the customer.
- Provide regular updates to the customer's IT Security Team on the progress of remediation efforts.
- Ensure any changes made to resolve vulnerabilities are tested and validated.

Acceptable Use Policy

1. General Use

- Use company resources responsibly and for intended purposes.
- Do not engage in activities that could harm the company's reputation or operations.

2. Personal Use

- Limited personal use of company resources is permitted if it does not interfere with work performance or violate any policies.

3. Unacceptable Use

- Do not use company resources for illegal activities, harassment, or accessing inappropriate content.
- Do not share or expose authentication credentials.

4. Monitoring and Enforcement

- The company reserves the right to monitor resource usage.
- Violations of this policy may result in disciplinary action.

5. Reporting Incidents

- Report any suspected security incidents, breaches, or policy violations to the Information Security Officer immediately.

Policy Review and Maintenance

This policy will be reviewed annually or when significant changes occur. Updates will be communicated to all employees and relevant parties.

This policy has been approved & authorised by:

Name: Newton Parker
Position: Director

Signature:

Date: 1st January 2024

This Policy shall be reviewed annually or when otherwise required due to significant changes in circumstances.