AventIQ, a trademark of Mittal Software Labs Limited

IT and Cybersecurity Policy
Confidential and Restricted

Objective

AventIQ, a trademark of Mittal Software Labs Limited is committed to ensuring the security and integrity of its IT systems and data. This IT and Cybersecurity Policy outlines guidelines for protecting organizational assets, including data, systems, and networks, against unauthorized access, breaches, and cyber threats. It complies with the Information Technology Act, 2000, and relevant Indian laws.

Scope and Applicability

This policy applies to all:

- Employees (permanent, probationary, and contractual).
- Interns (paid or unpaid).
- Contractors and vendors with access to AventIQ's IT systems.
- Devices and systems owned or managed by AventIQ.

Key Principles

1. **Data Protection**:
   - Protect confidential, personal, and proprietary data from unauthorized access or breaches.
2. **Compliance with Laws**:
   - Adhere to the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and other applicable laws.
3. **Responsibility and Accountability**:
   - Define roles and responsibilities for IT usage and cybersecurity.
4. **Proactive Risk Management**:
   - Identify, assess, and mitigate cybersecurity risks.

Roles and Responsibilities

1. Management Responsibilities:

- Ensure adequate resources and tools for IT security.
- Conduct periodic audits and reviews of IT systems.

2. Employee Responsibilities:

- Use IT resources responsibly and in accordance with this policy.
- Report cybersecurity incidents immediately to the IT department.

3. IT Department Responsibilities:

- Monitor and secure IT systems against potential threats.
- Respond promptly to reported incidents.

Acceptable Use of IT Resources

1. **Access Control**:
   - Employees must use only authorized credentials to access IT systems.
   - Sharing of login credentials is strictly prohibited.
2. **Email and Internet Usage**:
   - Emails must be used for official purposes only.
   - Accessing or sharing inappropriate content is prohibited.
3. **Hardware and Software**:
   - Only authorized devices and software approved by the IT department may be used.
   - Installation of unapproved software is not allowed.
4. **Remote Work Security**:
   - Employees working remotely must use secure connections (e.g., VPN) and comply with the Remote Work Policy.

Data Security and Confidentiality

1. **Data Classification**:
   - Data must be categorized as Public, Confidential, or Highly Confidential.

2. **Encryption**:
   - Sensitive data must be encrypted during storage and transmission.
3. **Data Access**:
   - Access to sensitive data shall be granted on a need-to-know basis.
4. **Data Retention and Disposal**:
   - Data must be retained only for the duration necessary and securely deleted thereafter.

Cybersecurity Measures

1. **Network Security**:
   - Firewalls, intrusion detection systems, and anti-virus software must be in place.
   - Regular updates and patches must be applied to all systems.
2. **Incident Response**:
   - Cybersecurity incidents must be reported to the IT department within 24 hours.
   - An incident response team will investigate and resolve issues promptly.
3. **Phishing and Malware Prevention**:
   - Employees must undergo regular training to identify and avoid phishing and malware threats.
4. **Regular Audits**:
   - Conduct periodic audits of IT systems to identify vulnerabilities and ensure compliance.

Third-Party and Vendor Compliance

1. Vendors and contractors with access to AventIQ's IT systems must:
   - Sign confidentiality and data protection agreements.
   - Comply with AventIQ's cybersecurity policies.
2. Vendor systems and processes will be reviewed periodically to ensure compliance.

Incident Reporting and Management

1. Employees must immediately report:
    - Unauthorized access or breaches.
    - Loss or theft of company devices.
2. The IT department will:
    - Acknowledge the report within 4 hours.
    - Investigate and resolve incidents within a reasonable timeframe.

Policy Violations and Disciplinary Action

1. Non-compliance with this policy will result in disciplinary action, which may include:
    - Verbal or written warnings.
    - Suspension or termination of employment.
    - Legal action for severe violations.
2. Contractors and vendors found violating this policy may face contract termination.

Training and Awareness

1. All employees will undergo cybersecurity training during onboarding.
2. Periodic refresher sessions will be conducted to reinforce best practices.

Review and Amendments

This policy will be reviewed annually or upon significant changes in legal or organizational requirements. Amendments will be communicated to all employees and stakeholders.

Approved By: Nikhil Mittal
Effective Date: 01-Jan-2025
Last Updated: 26-Dec-2024