IT Security Policy for WBCI

1.Introduction

1.1 Purpose

This IT Security Policy establishes the framework for protecting WBCI's technology assets, data, and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The goal is to ensure the confidentiality, integrity, and availability of information, while supporting construction operations and complying with applicable laws and regulations.

1.2 Objectives

- Minimize risks to IT systems and data used on-site and offices.
- Promote a culture of security awareness among office staff, field workers, and subcontractors.
- Safeguard project designs, bidding documents, and employee/client data.
- Outline procedures for incident response and recovery.

2. Scope

This Policy applies to all company employees, contractors, venders, and third parties who access WBCI's IT resources, including but not limited to:

- Hardware (e.g., computers, servers, mobile devices).
- Software (e.g., applications, operating systems).
- Networks (e.g., intranet, internet, cloud services).
- Data (e.g., electronic files, databases, emails). It covers all company locations, construction sites, remote work environments, and company-owned and personally owned devices used for business purposes.

3. Definitions

- **Confidential Information**: Any data designated as sensitive, including customer data, financial records or bids, intellectual property, project blueprints, or personal identifiable information.
- **Incident**: Any event that compromises the security, confidentiality, or integrity of IT assets (e.g., breach, malware infection).

- **User**: Any individual covered under the Scope section.
- **IT Assets**: All technology resources owned, managed, or used by the company.

4. Roles and Responsibilities

Role	Responsibility
Designated Lead	Develop, implement, enforce Policy
Contracted IT Provider	Manage access controls, system maintenance, backups, and vulnerability scans; support field and office users
Employees/Subcontractors	Comply with policy; report incidents immediately; use devices securely on-site and off-site.
Project Managers	Ensure team adherence; approve access to project specific systems; conduct security briefings for site workers.
Human Resources	Manage onboarding/offboarding security protocols.
Venders/Third Parties	Adhere to this Policy: sign security agreements before accessing company resources.

5. Acceptable Use

- **Permitted Use**: Company IT resources are for business purposes only. Limited personal use is allowed if it does not interfere with work or violate laws.
- All internet, email, and network activity on company devices may be monitored
- **Prohibited Activities**:
    - Unauthorized access to projects or system.
    - Sharing credentials or using unauthorized software or apps.
    - Connecting unapproved devices to company networks.
    - Downloading/installing unapproved applications.
    - Sending sensitive data via unsecured channels.
    - Sending spam, engaging in harassment, or accessing illegal content.
    - Using company resources for personal gain or competitive activities.

6. Access Control

- **User Authentication**: Multi-factor authentication is required for all accounts accessing project management tools, email, or financial data. Passwords must be at least 12 characters, complex, and change every 90 days
- **Principle of least Privilege**: Access granted only for job-specific needs. Project managers approve access requests.
- **Remote/ Site Access**: Use company-approved VPN for all remote connections. Company- issued devices preferred; requires enrollment in Device management.
- **Account Management**: Inactive accounts are disabled after 30 days. Upon termination, access is revoked immediately.
- **Physical Security**: Secure devices on construction sites. Report lost/stolen devices immediately.

7. Data Protection

- **Classification**: Data must be classified as Public, Internal, Confidential, or Restricted. Handle accordingly (e.g., encrypt Restricted data).
- **Encryption**: All sensitive data in transit (e.g., email attachments) and at rest (e.g., on laptops) must be encrypted using approved tools.
- **Backup and Recovery**: Critical data backed up daily to secure, offsite locations.
- **Data Handling**: No storage of unnecessary data. Dispose of data securely (e.g., shredding, secure wipe) when no longer needed.
- **Cloud Services**: Only approved providers with company configurations.

8. Incident Response

- **Reporting**: Report suspected incidents to IT immediately via [Micro-Ram Computers]
- **Response Plan**:
    1. **Detection**: Monitor logs and alerts for anomalies.
    2. **Containment**: Isolate affected systems.
    3. **Eradication**: Remove threats (e.g., malware).
    4. **Recovery**: Restore from backups.
    5. **Post-Incident:** conduct root cause analysis and lessons learned.
- **Notification**: Notify affected parties and regulators within 72 hours of confirmed breach, per legal requirements.

9. Training and Awareness

- All users must complete mandatory annual security training.
- New hires receive training within 30 days of onboarding.
- Phishing simulation conducted quarterly.
- Awareness campaigns on topics like password hygiene and social engineering.

10. Compliance and Enforcement

- **Audits**: Audits are conducted annually.
- **Violations**: Breaches of this Policy may result in disciplinary action, up to termination, and potential legal consequences.
- **Legal Compliance**: Adhere to relevant laws; designate a compliance officer if required.

11. Policy Review and Updates

- This Policy is reviewed annually or after major incidents/changes.
- Effective Date:
- Approved By:
- Contact: