Cybersecurity and Information Security Policy

DMCI Holdings recognizes the critical importance of cybersecurity and information security in safeguarding our business, employees, customers, and partners. This policy outlines the governance processes and best practices to ensure the protection of our information technology (IT) infrastructure, data, and systems from threats, disruptions, and disasters.

It is applicable to all directors, officers, employees, contractors and suppliers who interact with our information technology resources.

Governance and Responsibility

The Company and its subsidiaries will maintain an IT risk management team responsible for identifying and assessing all IT-related risks. This team should include representatives from IT, cybersecurity, legal, compliance, and other relevant departments.

The Chief Strategy and Sustainability Officer shall be responsible for the overall management and implementation of this policy. They will lead the IT risk management team, coordinate security measures and report to senior management on security issues and improvements.

Risk Management and Assessment

Regular risk assessments will be conducted to identify and prioritize potential threats and vulnerabilities. Mitigation strategies will be implemented based on these assessments.

Vendors handling sensitive data or providing critical services shall undergo security assessments before engagement and will be monitored regularly for compliance.

Information Security Measures

Information security measures include strict access controls based on a "need-to-know" basis and unique login credentials. We enforce a strong password policy and implement Multi-Factor Authentication (MFA) for critical systems. Sensitive data is encrypted during transmission and at rest.

Our network security utilizes firewalls, intrusion detection systems, and other protective measures. Regular security testing will be enforced, as well as the timely application of security patches to address known vulnerabilities. These measures ensure the protection of our IT infrastructure and data, enhancing cybersecurity and safeguarding our business, employees, customers, and partners.

Employees should promptly report any security incidents or vulnerabilities to the IT department.

Incident Response and Disaster Recovery
A detailed incident response plan will be maintained, outlining the steps to be taken in the event of a security breach or incident.

All security incidents, whether suspected or confirmed, must be reported immediately to the IT department, who will follow the incident response plan.

Regular data backups will be performed, and a disaster recovery plan will be in place to ensure business continuity in the event of a catastrophic event.

Training and Awareness
All employees will undergo periodic cybersecurity training to stay informed about emerging threats and best security practices. Employees will be educated on identifying and reporting phishing attempts to prevent data breaches.

Compliance and Audit
Regular audits will be conducted to assess compliance with this policy and relevant regulations.

We will comply with all applicable laws, regulations, and industry standards concerning information security.

Continuous Improvement
This policy will be reviewed periodically and updated to reflect the evolving threat landscape and business requirements. After each security incident, a post-incident review will be conducted to identify lessons learned and improve security measures.

Reporting Concerns
The active involvement of all employees is crucial in maintaining a safe and secure environment. If you become aware of any suspicious or potentially harmful activities, incidents, vulnerabilities or violations to this policy, we encourage you to report such activities to the hotline below:

Helpdesk and Reporting Hotline:
Chief Strategy and Sustainability Officer
Tel (632) 888 3000
Fax (632) 816 7362
Email: dmciholdings@dmcinet.com