MAGNUM CONSTRUCTION SERVICES INC.

CONFIDENTIALITY AND DATA PROTECTION POLICY

Document Code: MCS-CL-P08 | **Revision:** 1.0 | **Effective Date:** November 1 2025

---

1. PURPOSE

To establish strict procedures for protecting confidential information, intellectual property, and personal data collected, processed, or stored by Magnum Construction Services Inc. This policy ensures compliance with applicable privacy laws (GDPR, HIPAA, and U.S. Data Protection Acts) and maintains client and employee trust.

---

2. SCOPE

Applies to all Magnum employees, contractors, subcontractors, vendors, and third-party service providers who access corporate systems, project data, or client information. Includes all formats of data: physical documents, digital files, email, cloud storage, and mobile devices.

---

3. REFERENCES

- MCS-CORP-02 Code of Ethics
- MCS-CORP-10 Records Management and Document Control Policy
- ISO 27001 Information Security Management System
- U.S. Federal Privacy Laws (CISA, HIPAA, GLBA)
- EU General Data Protection Regulation (GDPR)
- Florida Information Protection Act (FIPA)

MAGNUM
CONSTRUCTION SERVICES

4. RESPONSIBILITIES

Role	Responsibility
Executive Director	Approves policy, ensures organizational compliance, and oversees investigations of data breaches.
IT Manager / Data Protection Officer (DPO)	Implements cybersecurity controls, maintains encryption, and performs risk assessments.
HR Manager	Ensures employee training, confidentiality agreements, and disciplinary enforcement.
Project Managers	Enforce data-protection requirements at project level and monitor third-party compliance.
All Employees	Safeguard all confidential information and immediately report potential breaches or loss.

---

5. DEFINITIONS

- **Confidential Information:** Any non-public business, financial, technical, or personnel data belonging to Magnum or clients.
- **Personal Data:** Information identifying an individual (e.g., name, ID, contact details, payroll records).
- **Data Processing:** Any operation involving collection, storage, transmission, or disposal of data.
- **Data Breach:** Unauthorized access, disclosure, loss, or alteration of confidential or personal data.

MAGNUM
CONSTRUCTION SERVICES

6. POLICY REQUIREMENTS

6.1 Confidential Information Handling

- Mark all confidential documents as **"CONFIDENTIAL – MAGNUM USE ONLY."**
- Share information only on a **need-to-know** basis with authorized personnel.
- Execute **Non-Disclosure Agreements (NDAs)** with clients, vendors, and partners.
- Restrict file access through password-protected servers and SharePoint permissions.

6.2 Data Protection Controls

- All devices must use **AES-256 encryption** and **multi-factor authentication (MFA)**.
- Use company-approved storage (no personal USBs or cloud accounts).
- Backups performed daily and verified weekly by IT.
- Sensitive emails must be encrypted (Outlook S/MIME or similar).

6.3 Data Retention and Destruction

Record Type	Retention Period	Disposal Method
Corporate Contracts & Legal Files	10 Years	Secure digital archive + shred paper copies
Employee Records	7 Years after termination	Encrypted archive / certified shredding
Project Documents	As per contract requirements (min. 10 Years)	Digital deletion / document control approval
Marketing / Client Lists	5 Years max or upon request	Permanent deletion / opt-out removal

MAGNUM
CONSTRUCTION SERVICES

6.4 Incident Response / Data Breach

- Notify the **Data Protection Officer (DPO)** within 24 hours of discovery.
- Contain and investigate breach; document root cause and impacts.
- Notify affected clients, employees, and regulators within 72 hours (GDPR standard).
- Implement corrective and preventive actions (CAPA).

6.5 Third-Party and Subcontractor Access

- Third parties must sign a **Data Processing Agreement (DPA)** before access.
- Periodic audits of vendors to ensure cybersecurity and privacy compliance.
- Terminate access immediately upon contract completion.

6.6 Training and Awareness

- Mandatory Confidentiality and Data Protection training for all employees annually.
- Refresher modules for managers and system admins every six months.
- Completion records maintained in the HR Training Register (MCS-HR-F02).

---

7. ENFORCEMENT AND VIOLATIONS

- Breach of this policy may result in disciplinary action up to termination, civil liability, or criminal penalties.
- Repeated violations or gross negligence shall trigger formal investigation by the Executive Director and Legal Counsel.

---

8. REVIEW AND AUDIT

This policy shall be reviewed annually by the Data Protection Officer and Executive Director to ensure alignment with changing laws, industry standards, and client requirements.

MAGNUM
CONSTRUCTION SERVICES

9. APPROVALS

Name	Title	Signature	Date
Michael Gaya	Executive Director		
Data Protection Officer	IT Manager / Compliance		
HR Manager	Corporate Administration		