

CYBERSECURITY & CUI PROTECTION POLICY

STRAVIK Construction Group · Controlled Document

Document No.	Revision	Effective Date	Document Owner	Status
STV-LEG-POL-018	00 (Initial Issue)	2026-10-24	President	Issued for review / pending approval

Management system alignment: This document is aligned with ISO 9001:2015, ISO 14001:2015 and ISO 45001:2018 requirements as applicable. STRAVIK Construction Group does not claim third-party certification to these standards. Florida Certified General Contractor License No. **[FL LICENSE NO.]**.

REVISION HISTORY

Rev.	Date	Description of Change	Prepared By	Approved By
00	2026-10-24	Initial issue for STRAVIK Construction Group	[PREPARED BY]	Michael Gaya, President

1. PURPOSE

To protect STRAVIK information systems and Controlled Unclassified Information (CUI) received on federal contracts, aligned with NIST SP 800-171 (no certification or assessment score claimed).

2. SCOPE

Applies to STRAVIK Construction Group and its subcontractors and suppliers on federally funded or federally assisted contracts, and as otherwise required by contract or law.

3. REFERENCES

- NIST SP 800-171 Rev. 2/3 — Protecting CUI in Nonfederal Systems
- DFARS 252.204-7012 / -7019 / -7020 and CMMC (where contractually required)
- FAR 52.204-21 Basic Safeguarding
- 32 CFR Part 2002 (CUI Program)

4. POLICY

- CUI is stored, processed and transmitted only on STRAVIK-approved systems listed in the System Security Plan (**[SYSTEM SECURITY PLAN]**).
- Access is limited to authorized users with a need to know; multi-factor authentication is required for remote and privileged access.
- Devices use full-disk encryption, current patches, endpoint protection and screen locks.
- CUI is marked and handled per the CUI Registry; transmitted only via encrypted channels.

5. NIST 800-171 CONTROL FAMILIES

Family	STRAVIK Implementation
Access Control / Identification & Authentication	Role-based access, unique accounts, MFA
Awareness & Training	Annual security awareness training; CUI handling training
Audit & Accountability	Logging enabled and reviewed: [LOG REVIEW PROCESS]
Configuration Management	Baseline configurations, change control
Incident Response	Report incidents to [IT MANAGER] immediately; DoD reporting within 72 hours where DFARS 7012 applies
Media Protection	Encrypt removable media; sanitize before disposal
Personnel / Physical Security	Screening; office access control; visitor escort
Risk / Security Assessment	Annual self-assessment; Plan of Action & Milestones (POA&M)
System & Communications Protection	Firewalls, encryption in transit, network segmentation

6. INCIDENTS

Suspected compromise, lost devices or phishing are reported immediately to **[IT MANAGER]** at **[PHONE / EMAIL]**.

RESPONSIBILITIES

Role	Responsibility
President	Approves this document and assigns resources; signs certifications.
[COMPLIANCE OFFICER]	Administers the program, monitors compliance and maintains records.
Project Managers	Flow down requirements to subcontracts and purchase orders; monitor field compliance.
Subcontractors / Suppliers	Comply with flowed-down requirements and provide required documentation.

DOCUMENT CONTROL

- Controlled under the Records Management & Document Control Policy (STV-GOV-POL-011) and the Document Control Procedure (STV-GOV-PRO-015).
- Reviewed at least annually, or after an incident, audit finding, regulatory change or significant change in operations.
- Records generated under this document are retained per the retention schedule in STV-GOV-POL-011.

APPROVAL

Role	Name	Title	Signature	Date
Prepared By	[PREPARED BY]	[TITLE]		
Reviewed By	[QUALITY / HSE MANAGER]	[TITLE]		
Approved By	Michael Gaya	President		

This document is reviewed at least annually, or upon significant organizational, legal or operational change, and re-issued under document control per STV-GOV-POL-011.