Security and Data Handling at Plavidian

A customer overview of how your data is protected | Prepared July 29, 2026 | Current version always available at plavidian.com/security

Campaigns, government offices, nonprofits, and commercial mailers hand us voter files, constituent data, and customer lists. This document states plainly how that data is handled. Every claim describes practice that exists today, verified before it was written down; where we have not verified something, we say nothing rather than round up.

NIST SP 800-171
Assessed 104/110, DoD methodology

CMMC Level 1
All 15 requirements met, pass/fail

DFARS 252.204-7012
Safeguarding and reporting ready

Encrypted End to End
TLS 1.2+ in transit, AES-256 at rest

MFA on Every Staff Account
Mandatory two-step, no exceptions

Camera-Verified Production
Chain of custody on verified jobs

How your data is protected

- **Encrypted in transit and at rest.** Traffic to Plavidian Connect uses TLS 1.2 or higher, and customer files and database records are encrypted at rest with 256-bit AES on Microsoft Azure in United States regions.
- **Individual accounts, two-step verification.** Access requires an individual account; there are no shared logins. Every Plavidian staff account requires a second factor from an authenticator app, mandatory and not able to be switched off. Passwords are stored as salted PBKDF2-HMAC-SHA256 hashes.
- **Sessions that end themselves.** Idle sessions sign out automatically, repeated failed sign-ins lock the account, and sign-in activity is recorded with time and source address.
- **Files that cannot attack you.** Every list and report we generate neutralizes spreadsheet formula injection, the application does not intentionally execute uploaded macros, scripts, or active document content, and uploaded files are malware-scanned in our own Azure tenant. Customer files remain within Plavidian's controlled production environment and its contracted cloud infrastructure, and are not submitted to unrelated third-party scanning, enrichment, analytics, or AI services.
- **Documented chain of custody.** The Plavidian Assurance Report documents what was produced on a job and how the run reconciled to your list. When camera verification runs, every piece read is part of that record.
- **Defined retention, then removal.** Job-tied data, including uploaded files, mailing lists, and per-piece camera scan records, is retained five years from job completion, then deleted.
- **A defined AI boundary.** Customer mailing lists, job files, and artwork are never sent to any AI service.

Our security framework: NIST SP 800-171

Plavidian's security program is built on NIST Special Publication 800-171, the standard developed by the National Institute of Standards and Technology to protect sensitive government information (Controlled Unclassified Information) held on nonfederal systems. Its 110 requirements cover access control, authentication, audit logging, configuration management, incident response, personnel and physical security, risk assessment, and the protection of communications and stored information. It is a government-defined, prescriptive standard with a published assessment methodology, not a commercial checklist, and we apply it to political, nonprofit, government, and commercial customer work alike.

Where we stand, in numbers. On July 29, 2026, Plavidian Connect was self-assessed against all 110 requirements and scored under the Department of Defense Assessment Methodology: **104 of a possible 110, with 108 of 110 requirements implemented**. The two remaining requirements sit at the methodology's defined partial-credit positions, each with a corrective action and target date in our Plan of Action and Milestones. The assessment is documented in the summary format required for posting to the DoD's Supplier Performance Risk System, and our exercised Incident Response Plan carries the reporting duties DFARS 252.204-7012 requires.

CMMC Level 1. CMMC Level 1 is pass/fail against the 15 basic safeguarding requirements of FAR 52.204-21, with no plan of action permitted at that level. Our assessment covers every one, all implemented, and neither open item is a Level 1 requirement: Plavidian meets Level 1 outright, with the formal SPRS self-assessment and affirmation filed when covered work requires them.

If your organization asks for SOC 2

We are asked about SOC 2 regularly, and the honest answer has two parts. First: **Plavidian does not hold a SOC 2 report.** SOC 2 is most commonly associated with commercial technology and outsourced service providers. Plavidian has instead chosen to align its security program with NIST SP 800-171, a U.S. government framework specifically developed to protect sensitive government information in nonfederal systems. We chose to build on NIST SP 800-171 because, for the data our customers actually give us, it is in important respects the more demanding yardstick.

NIST SP 800-171 (our framework)	SOC 2
Developed by the U.S. government through NIST, specifically to protect sensitive government information	Developed by the AICPA for general service-organization assurance
110 defined, prescriptive requirements; every organization is measured against the same list	Controls are selected within the scope of a particular examination, and scope can vary among organizations
Published government scoring methodology; our result is a number (104/110) with open items and dates disclosed	Result is an auditor's opinion on the controls within scope
Self-assessed by Plavidian; documented, not independently audited	Independent CPA attestation
Built for environments entrusted with sensitive government data, which is the standard we hold voter and donor files to	May cover security, availability, processing integrity, confidentiality, and privacy as scoped

Where the government framework goes further than a typical commercial scoping, we follow it: prescriptive multifactor and audit requirements, incident response that must be exercised rather than merely written, personnel screening, physical protection of printed material, and media destruction, all assessed against a fixed 110-item list rather than a negotiated scope. Where SOC 2 offers something we do not have, independent attestation, we say so plainly rather than blur the difference. If your vendor process requires a completed security questionnaire, send it: we complete questionnaires against our System Security Plan rather than from memory.

What we do not claim

No certifications we do not hold, and no words like comprehensive or military-grade. Our published security page changes the same day practice changes, or the claim comes down.

Documentation available to you

- **Public:** the full security and data handling statement at plavidian.com/security, and the NIST SP 800-171 explainer at plavidian.com/nist-800-171.
- **Under NDA:** the System Security Plan (version-dated, with cryptographic inventory), the Plan of Action and Milestones, and the July 29, 2026 assessment worksheet.
- **On request:** your completed security questionnaire, and the Plavidian Assurance Report on your own jobs.

Questions before you send a file, or a questionnaire to complete: **info@plavidian.com** | 760-666-3130