**DATA HANDLING SPECIFICATION**

Metal Finishing Calculator v3.0.0

|  |  |
| --- | --- |
| **Document Version:** | 1.0 |
| **Date:** | January 30, 2026 |
| **Prepared By:** | Psyrcuit LLC |
| **Audience:** | IT Security, Data Governance Teams |

# 1. Purpose

This document provides a comprehensive specification of how Metal Finishing Calculator handles data throughout its lifecycle. It is designed to demonstrate that the application poses zero data exfiltration risk, as all data remains exclusively within the customer's local environment with no transmission capabilities.

# 2. Data Classification Matrix

The following table classifies all data types processed by the application:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Type** | **Classification** | **Storage Location** | **Retention** | **Deletion** |
| **Quote Files** | Customer-determined | Customer directory | Customer controls | Customer deletes |
| **Settings/Config** | Non-sensitive | AppData or Shared Hub | Indefinite | Customer deletes |
| **License Key** | Non-sensitive | Settings file | With settings | With settings |
| **PDF Exports** | Customer-determined | Customer directory | Customer controls | Customer deletes |
| **Backup Files** | Non-sensitive | Settings subfolder | Customer controls | Customer deletes |

**Note:** Quote files and PDF exports may contain CUI if customers include controlled technical data in part descriptions. The application does not evaluate content classification—this remains the customer's responsibility.

# 3. Data Flow Architecture

The application's data flow is entirely contained within the customer's local environment:

|  |
| --- |
| **DATA FLOW DIAGRAM**  ┌─────────────────────────────────────────────────────────────┐  │ CUSTOMER'S LOCAL ENVIRONMENT │  │ │  │ [User Input] ──► [MFC Application] ──► [Local Files] │  │ │ │  │ ▼ │  │ [PDF Generation] │  │ │ │  │ ▼ │  │ [Local PDF File] │  │ │  └─────────────────────────────────────────────────────────────┘  ╔═══════════════════════════════════════════════════════════╗  ║ ✓ NO arrows exit the customer boundary ║  ║ ✓ NO network connections ║  ║ ✓ NO cloud services ║  ║ ✓ NO external APIs ║  ╚═══════════════════════════════════════════════════════════╝ |

# 4. Storage Locations

All storage locations are within the customer's file system and fully configurable:

|  |  |  |
| --- | --- | --- |
| **Storage Type** | **Default Location** | **Configurable** |
| **Settings** | %APPDATA%\Metal-Finishing-Calculator\ | Yes - via Shared Hub |
| **Quotes** | User-specified directory | Yes - first-run setup |
| **PDF Exports** | User-specified directory | Yes - per export |
| **Backups** | Settings directory\backup\ | Yes - follows settings |
| **Shared Hub** | Network path (optional) | Yes - customer specifies |

# 5. Data at Rest

All persistent data is stored in human-readable JSON format. The application relies on the customer's existing security infrastructure for protection:

|  |  |
| --- | --- |
| **Aspect** | **Implementation** |
| **File Format** | JSON (human-readable, auditable) |
| **Encryption** | Relies on customer's disk encryption (BitLocker, etc.) |
| **Access Control** | Relies on customer's file system permissions (NTFS ACLs) |
| **Backup** | Customer's existing backup procedures apply automatically |
| **Integrity** | JSON validation on load; corrupt files rejected gracefully |

# 6. Data in Transit

|  |
| --- |
| **NOT APPLICABLE**  Metal Finishing Calculator performs zero data transmission.  There is no network code in the application.  All data remains on the local file system at all times. |

# 7. Data Retention & Disposal

The application does not enforce any data retention policies. Customers maintain complete control:

|  |  |
| --- | --- |
| **Aspect** | **Details** |
| **Retention Policy** | None enforced by application - customer determines |
| **Deletion Method** | Standard OS file deletion (Explorer, command line, etc.) |
| **Remote Wipe** | Not applicable - no remote access capability exists |
| **Residual Data** | None - files are standard JSON, no hidden caches |
| **Uninstallation** | Delete application folder and AppData directory |

# 8. Shared Hub Feature (Optional)

The Shared Hub feature enables settings sharing across multiple computers within the customer's network. This is an optional configuration for multi-estimator environments:

|  |  |
| --- | --- |
| **Aspect** | **Details** |
| **Purpose** | Share process definitions, fee structures, and templates across computers |
| **Location** | Customer-specified network folder (e.g., \\server\MFC-Hub) |
| **Data Boundary** | Remains within customer's internal network - no external access |
| **Access Control** | Customer sets folder permissions via standard network share ACLs |
| **Psyrcuit Access** | None - Psyrcuit has no ability to access customer shared hubs |
| **Encryption** | Relies on customer's network encryption policies |

## Shared Hub Directory Structure

|  |
| --- |
| **\\server\MFC-Hub\**  ├── Settings\  │ ├── mfc\_settings\_[ComputerID1].json  │ ├── mfc\_settings\_[ComputerID2].json  │ └── backup\  ├── Quotes\  ├── Templates\  └── Backups\ |

# 9. Vendor Data Access Statement

|  |
| --- |
| **Psyrcuit LLC hereby attests that:**  1. We have NO access to customer data under any circumstances.  2. We have NO mechanism to receive, view, or collect customer information.  3. We have NO remote access capability to customer systems or files.  4. We have NO telemetry, analytics, or usage tracking of any kind.  5. The application is architecturally incapable of transmitting data. |

# 10. Add-On Data Access

## 10.1 Data Access Matrix

Add-on modules operate within a restricted data access model. The following matrix defines permitted and prohibited data operations:

|  |  |
| --- | --- |
| **Data Category** | Access Level |
| **Active quote fields (dimensions, quantities, pricing)** | READ/WRITE – Via defined IPC API only |
| **Application settings (process configs, rates)** | READ ONLY – Cannot modify settings |
| **Other users’ quote files** | BLOCKED – No filesystem access |
| **System files and OS resources** | BLOCKED – Sandboxed renderer process |
| **Network endpoints** | BLOCKED – No outbound connections |
| **Customer PII or contact data** | BLOCKED – No access to data outside active quote |
| **License keys or credentials** | BLOCKED – Stored in main process only |

## 10.2 Data Isolation Controls

Add-ons execute in isolated renderer contexts with contextIsolation: true and nodeIntegration: false. Data exchange between add-ons and the main application occurs exclusively through the preload bridge’s defined IPC channels. Add-ons cannot access data belonging to other add-ons.

## 10.3 Cryptographic Authorization

Data access is gated by cryptographic signature verification. Only add-ons bearing a valid Ed25519 signature from Psyrcuit LLC can interact with the IPC data channels. Unsigned or tampered add-ons are rendered inert with all interactive controls disabled, preventing any data access.

## 10.4 Liability

**WARNING: Psyrcuit LLC is not responsible for data handling behavior of any add-on whose cryptographic signature verification has been bypassed through modification of the application binary. Unauthorized modifications void all data handling guarantees described in this specification.**

For data handling inquiries, contact: security@psyrcuit.com

Psyrcuit LLC • Tucson, Arizona • psyrcuit.com