**VENDOR SECURITY QUESTIONNAIRE**

Metal Finishing Calculator v3.0.0

|  |  |
| --- | --- |
| **Document Version:** | 1.0 |
| **Date:** | January 30, 2026 |
| **Vendor:** | Psyrcuit LLC |
| **Product:** | Metal Finishing Calculator v3.0.0 |

|  |
| --- |
| **Response Legend:**  **N/A** = Not applicable (offline application, no network/cloud features)  **Customer Responsibility** = Control implemented by customer's IT environment  **Yes/Implemented** = Vendor provides this capability |

# 1. Company Information

|  |  |
| --- | --- |
| **Question** | **Response** |
| **1.1 Company legal name** | Psyrcuit LLC |
| **1.2 Company headquarters location** | Tucson, Arizona, USA |
| **1.3 Year company founded** | 2024 |
| **1.4 Number of employees** | 1-10 |
| **1.5 Primary business activity** | Custom software development for manufacturing industry |
| **1.6 Company website** | https://psyrcuit.com |
| **1.7 Security contact email** | security@psyrcuit.com |

# 2. Product Information

|  |  |
| --- | --- |
| **Question** | **Response** |
| **2.1 Product name and version** | Metal Finishing Calculator v3.0.0 |
| **2.2 Product deployment model** | On-premise desktop application (Windows) |
| **2.3 Is the product cloud-based?** | No - 100% offline, local installation only |
| **2.4 Does the product require internet?** | No - fully functional without any network connectivity |
| **2.5 Does the product transmit data externally?** | No - zero network transmission capability |
| **2.6 Technology stack** | Electron 40.1.0, React 18.2.0, Node.js (bundled) |
| **2.7 Supported operating systems** | Windows 10 (1903+), Windows 11 - 64-bit only |

# 3. Data Security

|  |  |
| --- | --- |
| **Question** | **Response** |
| **3.1 Where is customer data stored?** | Locally on customer's workstation only. Default: %APPDATA% or customer-specified directory. |
| **3.2 Does vendor have access to customer data?** | No - Psyrcuit has zero access to customer data. All data remains on customer premises. |
| **3.3 Is data encrypted at rest?** | Customer Responsibility - Application relies on OS-level encryption (BitLocker recommended) |
| **3.4 Is data encrypted in transit?** | *N/A - No data transmission occurs. Application is 100% offline.* |
| **3.5 Data retention policy** | Customer Responsibility - Customer controls all data retention and deletion |
| **3.6 Data backup procedures** | Customer Responsibility - Standard file backup procedures apply |
| **3.7 Data classification supported** | Application supports ITAR/CUI environments through offline architecture |
| **3.8 Can data be exported?** | Yes - PDF quotes, JSON quote files (all local, no cloud export) |

# 4. Access Control

|  |  |
| --- | --- |
| **Question** | **Response** |
| **4.1 Does the application require authentication?** | No application-level authentication. Relies on Windows user authentication. |
| **4.2 Multi-factor authentication supported?** | *N/A - No application authentication. Customer can enforce MFA at Windows login.* |
| **4.3 Role-based access control?** | Customer Responsibility - Use Windows NTFS permissions and user accounts |
| **4.4 Password policy enforcement?** | *N/A - No application passwords. Windows password policies apply.* |
| **4.5 Session timeout implemented?** | Customer Responsibility - Use Windows screen lock policies |
| **4.6 Audit logging of user actions?** | Customer Responsibility - Windows Event Logs capture file access |
| **4.7 Can access be revoked remotely?** | Customer Responsibility - Remove application or revoke Windows access |

# 5. Network Security

|  |  |
| --- | --- |
| **Question** | **Response** |
| **5.1 Does the application make network connections?** | No - Zero network connectivity. Application can be blocked in firewall with no impact. |
| **5.2 What ports does the application use?** | *N/A - No network ports opened or used* |
| **5.3 Does the application use APIs?** | *N/A - No external API calls. All processing is local.* |
| **5.4 Is a VPN required?** | *N/A - No network access required* |
| **5.5 Does the application support TLS?** | *N/A - No network transmission* |
| **5.6 Can it operate on air-gapped networks?** | Yes - Designed for air-gapped and isolated environments |
| **5.7 Firewall rules required?** | None required. Application can be fully blocked. |

# 6. Application Security

|  |  |
| --- | --- |
| **Question** | **Response** |
| **6.1 Secure development lifecycle followed?** | Yes - Code review, dependency scanning, security testing |
| **6.2 Third-party components managed?** | Yes - SBOM maintained, versions pinned, vulnerabilities monitored |
| **6.3 Input validation implemented?** | Yes - All user inputs validated and sanitized |
| **6.4 Protection against injection attacks?** | Yes - No SQL/database. All data is local JSON files. |
| **6.5 Code signing implemented?** | SHA-256 checksums provided for integrity verification |
| **6.6 Context isolation enabled?** | Yes - contextIsolation: true, sandbox: false (required for offline MAC-based licensing) |
| **6.7 Node integration disabled in renderer?** | Yes - nodeIntegration: false, contextIsolation: true |
| **6.8 Does the application support third-party add-ons or plugins?** | Yes - Optional add-on modules can extend calculator functionality. All add-ons require Ed25519 cryptographic signature verification before execution. |
| **6.9 How are add-ons verified before execution?** | Ed25519 elliptic curve signature verification with SHA-256 content hashing. Public key is hardcoded in the application binary. Private key held offline by Psyrcuit LLC exclusively. |
| **6.10 Can unsigned or tampered add-ons execute?** | No - Unsigned or signature-failed add-ons are rendered inert. UI controls are disabled. Verification occurs at installation, every application launch, and renderer load. |
| **6.11 Can the add-on system be disabled?** | The add-on system has no add-ons installed by default. Removing all add-on directories effectively disables the system. The application operates normally without add-ons. |

# 7. Incident Response

|  |  |
| --- | --- |
| **Question** | **Response** |
| **7.1 Incident response plan in place?** | Yes - Documented incident response procedures |
| **7.2 Security incident notification timeframe?** | Critical: 24 hours, High: 72 hours, via email to affected customers |
| **7.3 Has vendor experienced a data breach?** | No - No breaches. Note: Vendor has no access to customer data. |
| **7.4 How are vulnerabilities reported?** | Email security@psyrcuit.com - Response within 48 hours |
| **7.5 Vulnerability patching timeframe?** | Critical: 30 days, High: 60 days, Medium: 90 days |

# 8. Business Continuity

|  |  |
| --- | --- |
| **Question** | **Response** |
| **8.1 What happens if vendor ceases operations?** | Application continues to function indefinitely - no vendor dependency for operation |
| **8.2 Is source code escrowed?** | Available upon request for enterprise agreements |
| **8.3 Application availability SLA?** | *N/A - Local application, not a service. 100% available when installed.* |
| **8.4 Disaster recovery plan?** | Customer Responsibility - Standard workstation backup/restore procedures |
| **8.5 Data portability?** | Yes - All data stored in standard JSON format, fully portable |

# 9. Compliance & Certifications

|  |  |
| --- | --- |
| **Question** | **Response** |
| **9.1 SOC 2 certification?** | *N/A - Not applicable for offline desktop software with no data processing services* |
| **9.2 ISO 27001 certification?** | Not currently certified |
| **9.3 ITAR compatible?** | Yes - Designed for ITAR environments. No foreign data transmission. |
| **9.4 CUI compatible?** | Yes - Supports CUI environments. Data remains on customer-controlled systems. |
| **9.5 CMMC compatible?** | Yes - Inherits customer's CMMC controls. See NIST 800-171 Responsibility Matrix. |
| **9.6 GDPR applicable?** | *N/A - Vendor does not process personal data. All data under customer control.* |
| **9.7 HIPAA applicable?** | *N/A - Application not designed for healthcare data* |

# 10. Third-Party Risk

|  |  |
| --- | --- |
| **Question** | **Response** |
| **10.1 Does the application use third-party components?** | Yes - 7 components. See SBOM for complete list with versions and licenses. |
| **10.2 Are third-party components monitored for vulnerabilities?** | Yes - npm audit, NVD monitoring, security advisory subscriptions |
| **10.3 Are components from trusted sources?** | Yes - npm registry, Cloudflare CDN, jsDelivr only. See Third-Party Attestation. |
| **10.4 Does the application use subprocessors?** | No - No data leaves customer premises. No subprocessors involved. |
| **10.5 Does the application connect to external services?** | No - Zero external service connections |
| **10.6 Are third-party add-ons subject to supply chain controls?** | Yes - All add-ons require cryptographic signature from Psyrcuit LLC. Only Psyrcuit-signed add-ons can execute. Unsigned third-party code is blocked. Psyrcuit LLC is not liable for add-ons whose signature verification has been bypassed through binary modification. |

# 11. Physical Security

|  |  |
| --- | --- |
| **Question** | **Response** |
| **11.1 Where is customer data physically stored?** | Customer Responsibility - Data stored only on customer's local workstations/servers |
| **11.2 Data center security controls?** | *N/A - No vendor data centers. Application is locally installed.* |
| **11.3 Physical access controls?** | Customer Responsibility - Customer's facility security applies |
| **11.4 Media disposal procedures?** | Customer Responsibility - Standard secure deletion procedures apply |

# 12. Licensing & Updates

|  |  |
| --- | --- |
| **Question** | **Response** |
| **12.1 How is the application licensed?** | Per-computer license tied to MAC address hash. Offline validation. |
| **12.2 Does licensing require internet?** | No - License validation is 100% offline using cryptographic hash |
| **12.3 How are updates delivered?** | Manual download from Psyrcuit. No auto-update functionality. |
| **12.4 Can updates be tested before deployment?** | Yes - Customer controls when/if updates are installed |
| **12.5 Backward compatibility policy?** | Yes - Settings and quotes from v2.x migrate automatically to v3.x |

# 13. Additional Attestations

|  |
| --- |
| **Psyrcuit LLC attests that Metal Finishing Calculator:**  ✓ Contains no telemetry, analytics, or usage tracking code  ✓ Makes no network connections of any kind  ✓ Stores all data locally on customer-controlled systems  ✓ Does not collect, transmit, or process personal information  ✓ Can operate indefinitely without vendor contact  ✓ Is suitable for air-gapped, ITAR, and CUI environments  ✓ Uses only permissively-licensed third-party components (MIT, LGPL) |

# 14. Related Documentation

The following documents provide additional detail on specific security topics:

|  |  |
| --- | --- |
| **Document** | **Description** |
| **Product Security Overview** | Executive summary of security architecture |
| **Data Handling Specification** | Detailed data flow and storage documentation |
| **NIST 800-171 Responsibility Matrix** | Control-by-control responsibility mapping |
| **Configuration & Hardening Guide** | Installation and security configuration |
| **Software Bill of Materials** | Complete component inventory with licenses |
| **Third-Party Component Attestation** | Formal attestation on component sourcing |

For questions about this questionnaire: security@psyrcuit.com

Psyrcuit LLC • Tucson, Arizona • psyrcuit.com