**INCIDENT RESPONSE POLICY**

Metal Finishing Calculator

|  |  |
| --- | --- |
| **Document Number:** | MFC-IRP-001 |
| **Version:** | 1.0 |
| **Effective Date:** | January 30, 2026 |
| **Last Review:** | January 30, 2026 |
| **Owner:** | Psyrcuit LLC |

# 1. Purpose & Scope

This policy defines Psyrcuit LLC's procedures for identifying, responding to, and communicating security incidents affecting Metal Finishing Calculator. Due to the application's offline architecture, incident scope is limited to:

|  |
| --- |
| • Vulnerabilities discovered in application code or bundled components  • Security issues in third-party dependencies (React, Electron, etc.)  • Malicious tampering of distributed application files  • Compromise of Psyrcuit's build or distribution systems |

|  |
| --- |
| **Note:** Because Metal Finishing Calculator is 100% offline with no network connectivity, data breaches involving customer data are not possible through the application. Psyrcuit has no access to customer data. |

# 2. Severity Classification

|  |  |  |
| --- | --- | --- |
| **Severity** | **Definition** | **Example** |
| **Critical** | Active exploitation or vulnerability enabling remote code execution, data exfiltration, or complete system compromise | Malicious code in distributed binary; RCE in Electron/Chromium affecting MFC |
| **High** | Significant vulnerability with clear path to exploitation but no evidence of active exploitation | Privilege escalation; bypass of Electron sandbox; critical dependency CVE |
| **Medium** | Moderate vulnerability requiring specific conditions or user interaction | XSS requiring user to load malicious file; medium-severity dependency CVE |
| **Low** | Minor issue with minimal security impact | Information disclosure of non-sensitive data; minor dependency update |

# 3. Response Procedures

## 3.1 Detection & Reporting

|  |  |
| --- | --- |
| **Internal Discovery:** | Security issues found during development, testing, or dependency monitoring are logged immediately in the internal tracking system. |
| **External Reports:** | Customers and researchers report vulnerabilities to security@psyrcuit.com. Acknowledgment within 48 hours. |
| **Dependency Alerts:** | Automated monitoring via npm audit and NVD subscriptions. Alerts reviewed within 24 hours. |

## 3.2 Response Timeline

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Acknowledgment** | **Patch Target** | **Customer Notification** |
| **Critical** | 4 hours | 24-72 hours | Within 24 hours of confirmation |
| **High** | 24 hours | 7-14 days | Within 72 hours of confirmation |
| **Medium** | 48 hours | 30-60 days | With next scheduled release |
| **Low** | 72 hours | 90 days | In release notes |

# 4. Customer Communication

When a security incident affects customers, Psyrcuit will:

|  |  |
| --- | --- |
| **1.** | Send email notification to all registered customers with active support agreements |
| **2.** | Provide description of the vulnerability (without exploitation details) |
| **3.** | Include affected versions and whether customer's version is impacted |
| **4.** | Provide mitigation steps if a patch is not yet available |
| **5.** | Deliver patched version with installation instructions |
| **6.** | Publish security advisory on psyrcuit.com (after customers have had time to patch) |

# 5. Contact Information

|  |
| --- |
| **Security Incident Reporting**  **Email:** security@psyrcuit.com  **Response:** Acknowledgment within 48 hours (24 hours for Critical)  **Please include:** Product version, description of issue, steps to reproduce (if applicable), your contact information |

*This policy is reviewed annually and updated as needed.*

Psyrcuit LLC • Tucson, Arizona • psyrcuit.com