

DocSmith Security Whitepaper (Public)

Product: DocSmith SIF Generator (Browser Extension)

Version: 1.0

Applies to: Extension v1.0.2 (Chrome Web Store; Edge Add-ons)

Date (GST): 2026-02-09

Owner: Axis (Security Architecture)

Generated: 2026-02-09 04:59 UTC

1. Executive Summary

DocSmith SIF Generator is a local-first UAE WPS Salary Information File (SIF) generation and validation tool delivered primarily as a browser extension. The security posture is designed to minimize data exposure by keeping payroll processing on the user's machine, avoiding accounts and backend services for core functionality.

This document describes the current security model, data handling behavior, and limitations as of the version listed above. It is intended for customers, evaluators, and regulators.

2. Scope

In scope

- Browser extension used to generate and validate WPS SIF files.
- Local validation and deterministic SIF generation logic.
- Input formats: Excel/CSV uploads and internal data objects derived from user-provided files.
- Output: .SIF files and validation reports.

Out of scope

- Licensing/payment services (not implemented in the extension release covered here).
- External integrations, cloud storage, or sync.
- Customer endpoint security (device management, OS hardening), network perimeter, or email security.
- Third-party platforms (Chrome Web Store / Edge Add-ons) beyond distribution and update delivery.

3. Security Objectives

- Minimize sensitive data exposure (local-first processing).
- Ensure deterministic, reproducible SIF outputs.
- Provide explainable validation errors and auditability for correctness.
- Maintain a minimal browser permission and network footprint.

4. Architecture Overview (Current Design)

- Distribution: MV3 browser extension (Chrome/Edge).
- UI surfaces: toolbar action popup; side panel when supported (Edge may fall back to opening a tab as accepted v1 behavior).
- Background: service worker for extension lifecycle.
- Processing: in-browser and in-memory during user sessions.
- Outputs: SIF files and validation reports saved by the user via browser download/save flows.

5. Data Classification

Typical payroll inputs and outputs include sensitive personal and payroll data such as:

- Employee names, internal identifiers, and payroll reference fields.
- Bank account identifiers (e.g., IBAN) and salary amounts.
- Salary payment schedules and totals.

Recommended handling classification: Confidential / Restricted (customer policy applies).
Customers should treat generated SIF files as sensitive payroll artifacts.

6. Data Flow, Storage, and Retention

Data flow (high level)

- Input: user selects an Excel/CSV file (or equivalent) from their local system.
- Processing: parsing, normalization, validation, and SIF generation occur locally in the browser context.
- Output: generated .SIF file and validation report are produced for the user to save.

Retention (as of extension v1.0.2)

- Core SIF processing is designed to be in-memory and user-driven.
- The release covered by this document does not require server-side storage to function.

- Generated outputs are saved by the user; retention and access control of those files are customer responsibilities.

7. Browser Permissions and Network Access

Permissions

- No host permissions are required for core SIF processing.
- The extension's design intent is least-privilege: only capabilities necessary for local file processing and UI are used.

Network access

- Core functionality does not require contacting external services.
- Any external URLs shown in the UI are informational links that are user-initiated navigation, not payroll-data transfer.

8. Threat Model Summary (High-Level)

Key threats

- Malformed or inconsistent input leading to incorrect SIF output.
- Local device compromise or unauthorized local access to uploaded input files or generated outputs.
- Supply-chain risk via extension distribution/update channels.
- Misinterpretation of extension store review as a compliance or security audit.

Mitigations (current)

- Strict validation rules, cross-record consistency checks, and deterministic formatting rules.
- Local-first processing (no backend dependency for core generation/validation).
- Clear disclosure of limitations and evidence expectations per release.
- Use official distribution channels and verify publisher identity where supported.

9. Assurance and Evidence Expectations

The assurance goal is correctness + auditability of outputs:

- Deterministic output: identical input should produce identical SIF output.
- Validation evidence: a validation suite, fixtures, and sample artifacts maintained per release.

- Release evidence: record version, changes, and known limitations before public publication.

10. Limitations and Disclosures

- No independent third-party security audit completed as of this version.
- Extension store review is not a compliance or security audit.
- Side panel behavior differs across browsers; Edge may fall back to opening a tab (accepted v1 behavior).
- This document describes current behavior; future features (licensing, cloud sync, integrations) require a new review and updated whitepaper.

11. Vulnerability Reporting

Contact: security@starwealthdynamics.org Response goal: acknowledge within 3 business days; triage within 7 days.

12. Change Log

- 2026-02-09: Published v1.0 (public) based on draft v0.1; expanded scope language and clarified data handling, permissions, and limitations.