DocSmith Security Whitepaper (Public)

Version: 1.0.0

Publication Date: 2026-02-14

Classification: Public Distribution

1. Executive Summary

DocSmith is an offline-first UAE WPS SIF generation utility designed for payroll operators and compliance teams. The product architecture prioritizes local execution, deterministic validation outcomes, and minimal data exposure.

This whitepaper describes the current security posture of the published product surface and extension workflow.

2. Scope

In scope

- Browser-based product surfaces served at `https://www.docsmith.tools`
- Extension-assisted local payroll preparation workflow
- Validation, generation, and export boundaries for SIF outputs
- Data handling controls in normal operator use

Out of scope

- Customer endpoint hardening and host OS security
- Bank-side or MoHRE portal security controls
- Third-party IT policy governance inside enterprise networks

3. Architecture Overview

DocSmith operational flow is structured as:

- User browser session
- Extension runtime boundary
- Local processing engine
- Generated SIF artifact

Design principle: payroll content remains in the operator-controlled environment during preparation and export.

4. Data Flow

High-level sequence:

1. Input payroll values from user-controlled source files or form entry.
2. Run local validation rules against required WPS field constraints.
3. Build deterministic SIF output in session memory.
4. Export final file to user-selected storage destination.
5. Clear temporary processing state at session close or reset action.

Control statement: Zero remote payroll transmission is a design requirement for the core generation path.

5. Data Classification and Handling

- Payroll identifiers (sensitive): processed locally for validation and file generation.
- Operational metadata (low sensitivity): used for UX and deterministic workflow state.
- Diagnostic/audit events (non-payload): no payroll row payloads are intentionally transmitted for analytics.

Retention model:

- Session state is temporary by design.
- Draft persistence behavior depends on local feature usage and browser profile context.

6. Threat Model Summary

A. Data leakage risk

Mitigation:

- Local-first processing model
- No intentional server-side payroll parsing pipeline in core workflow

B. Malicious extension/runtime manipulation

Mitigation:

- Controlled release and extension identity checks
- User verification of official listing and publisher details

C. File tampering before submission

Mitigation:

- Deterministic generator output and validation gate before export
- Operator verification using known format constraints

D. Local endpoint compromise

Mitigation:

- Shared-responsibility posture documented for enterprise and IT admins

- Recommendation for managed browser policy and endpoint controls

7. Browser Permission Governance

Each permission request is mapped to a functional need and reviewed against least-privilege expectations during release cycles.

Evaluation dimensions:

- Purpose justification
- Misuse risk surface
- Mitigation and user guidance

Enterprise rollout recommendation: validate extension policy and permission posture in a pilot group before wide deployment.

8. Security Limitations

- Product controls do not replace enterprise endpoint security controls.
- Bank-specific WPS acceptance logic may vary and is outside product control.
- Regulatory interpretation and legal compliance remain the responsibility of each employer.

9. Responsible Disclosure and Contact

Security and operations contact:

- `support@starwealthdynamics.org`

Responsible disclosure process:

1. Submit issue summary and reproducible context.
2. Include version/build details and impact description.
3. High-severity reports are triaged first and acknowledged in standard support window.

10. Assurance Statement

DocSmith aims to provide an auditable, locally executed payroll preparation workflow for UAE WPS SIF generation. Security posture and documentation are maintained as living artifacts and updated when architecture, permissions, or workflow controls change.

Disclaimer: This document is an operational security overview and not legal advice.