# NIST SP 800-218 Secure Software Development Framework (SSDF) Attestation Document

## Contents



## 1. Introduction

This document serves as an attestation of Exponam, LLC's adherence to the guidelines set forth in NIST Special Publication (SP) 800-218, "Securing the Software Development Lifecycle: A Framework for Secure Software Development." The purpose of this attestation is to confirm our commitment to the secure development of software, consistent with industry standards and government recommendations for secure software practices.

## 2. Scope of the Attestation

This attestation applies to all software development activities within Exponam, LLC, including both in-house and third-party software products developed or managed by the organization. The following attests to the incorporation of security practices as outlined in the NIST SP 800-218 framework throughout our software development lifecycle (SDLC).

# 3. Overview of NIST SP 800-218

NIST SP 800-218 provides a detailed framework for integrating security into the SDLC and is designed to promote secure coding practices, vulnerability management, incident response, and other key security activities. The main components of the framework include:

- **Security Planning**: Identifying security requirements early in development.
- **Secure Coding Practices**: Following secure coding guidelines to avoid common vulnerabilities.
- **Testing and Validation**: Ensuring the security of the software through continuous testing and validation.
- **Vulnerability Management**: Identifying and addressing security weaknesses in software.
- **Software Integrity**: Protecting the software's integrity through proper authentication and access control measures.

# 4. Statement of Compliance

Exponam, LLC hereby attests that it complies with the practices outlined in NIST SP 800-218 for secure software development, as reflected in our policies and procedures. Specifically, we have integrated the following practices:

1. **Secure Software Development Practices**:
    - We maintain secure coding standards across all software development teams.
    - All software is reviewed and tested for security risks before deployment.
2. **Use of Secure Development Tools**:
    - Development tools and technologies are aligned with NIST's security guidelines.
3. **Ongoing Risk Assessments**:
    - We conduct regular risk assessments throughout the software development lifecycle to identify and mitigate security threats.
4. **Vulnerability Management**:
    - Vulnerability assessments and penetration testing are conducted on a continuous basis, and remediation is promptly addressed.
5. **Incident Response and Monitoring**:

- Our software development process includes monitoring for security incidents, with established incident response protocols in place.

6. **Compliance with the Secure Software Development Framework (SSDF)**:
    - Exponam, LLC is fully committed to complying with all the applicable requirements set forth in NIST SP 800-218.

# 5. Supporting Materials

To further substantiate our adherence to NIST SP 800-218, we have attached the following supporting documentation:

1. **Information Security Policy**: This policy encompasses Exponam, LLC's security framework, including the Information Security Management System (ISMS), risk management processes, control procedures, and other critical security measures. The key sections of the policy include:
    - Information security management system objectives and manual
    - Risk management strategies and risk treatment plans
    - Control policies covering access control, password policy, encryption, and incident management
    - Business continuity planning and disaster recovery procedures
    - Incident monitoring and continuous improvement processes
2. **Acceptable Information Technology Resource Use Policy**: This policy outlines the acceptable use of IT resources within Exponam, LLC, including:
    - Access, authentication, and authorization procedures
    - Electronic communication practices
    - Consequences of policy violations and procedures for reporting violations
    - Training programs to ensure all employees are aware of their roles and responsibilities in maintaining security

# 6. Attestation Declaration

By signing this document, Exponam, LLC confirms that it has:

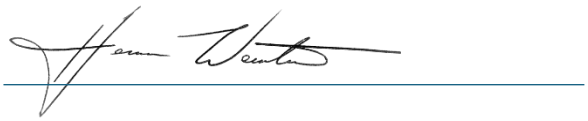
- Implemented and continues to follow secure software development practices as outlined in NIST SP 800-218.

- Ensured that all relevant personnel are trained in and adhere to the security policies and procedures mentioned in our Information Security Policy and Acceptable IT Resource Use Policy.
- Conducted internal audits and assessments to verify compliance with the framework and have taken corrective actions where needed.

This attestation is made in good faith and with the understanding that Exponam, LLC remains committed to ensuring secure software development practices throughout our SDLC.

## 7. Certification and Signature

**Signed by:**



- **Name:** Herman Weintraub
- **Title:** Co-founder, CEO
- **Organization Name:** Exponam, LLC
- **Date:** August 1, 2024

## 8. Conclusion

Exponam, LLC is committed to securing the software we develop, ensuring that our practices align with NIST SP 800-218 standards for secure software development. We continuously improve our practices to meet evolving security challenges and provide assurance that our software development processes meet high standards of security and compliance.