WESTWIND

Federal Government Cybersecurity Supply Chain Risk Management (C-SCRM) Supplier Code of Conduct

PL-842-002
Rev A
10/23/2024

Westwind Computer Products, Inc
5655 Jefferson Street, NE, Suite B
Albuquerque, NM 87109
(505) 345-4720
www.wwcpinc.com

1.0 Introduction

At Westwind, we are dedicated to upholding the highest standards of integrity, security, and ethical conduct in our business operations, particularly as a federal government supplier in the realm of Cybersecurity Supply Chain Risk Management (C-SCRM) Level 2. Our commitment to these principles is essential for fostering trust and protecting sensitive information and resources throughout our supply chain.

This Supplier Code of Conduct outlines the expectations and responsibilities for our C-SCRM Level 3 suppliers as we work collaboratively to enhance cybersecurity resilience across the supply chain. It emphasizes our commitment to compliance with federal regulations, the importance of safeguarding information and maintaining a secure operational environment.

By adhering to this Code, our suppliers will align with our core values and contribute to a secure and efficient supply chain that supports our federal government partners. A strong commitment to ethical practices and security is vital for our shared success and protecting our nation's critical assets. We recognize that the landscape of Cybersecurity is continually evolving, and as such, our suppliers must be agile, responsive, and proactive in their efforts to mitigate risks and uphold the integrity of the supply chain.

As we navigate the complexities of cybersecurity supply chain risk management, we are committed to fostering collaboration, transparency, and mutual accountability. Together, we can build a robust framework that not only meets compliance standards but also instills confidence in our partnerships and enhances the overall security posture of our operations.

2.0 Purpose

This Supplier Code of Conduct aims to define the ethical and operational standards that our Level 3 suppliers must uphold in relation to Cybersecurity Supply Chain Risk Management (C-SCRM). This Code seeks to create a secure and responsible supply chain that prioritizes Cybersecurity, compliance, and ethical conduct, reinforcing our collective commitment to safeguarding sensitive information and resources.

3.0 Scope

This Code applies to all Level 3 suppliers engaged with our organization, including:

- **Distributors (Disti's)**: Entities that provide products or services directly to our organization.
- **OEM Direct**: Any third-party entities that provide products or services on behalf of direct suppliers.
- **Subcontractors (Teaming Partners):** Organizations involved in the supply chain that may impact Cybersecurity and overall risk management.

Level 3 encompasses Suppliers responsible for operational activities, including procurement and system-related Cybersecurity Supply Chain Risk Management (C-SCRM) activities as part of the enterprise's Software Development Life Cycle (SDLC).

A critical Level 3 activity is the development of the C-SCRM plan. This plan includes security control information, system categorization, operational status, related agreements, architecture, critical personnel, applicable laws, regulations, policies, and contingency plans. Continuous

hygiene is essential in C-SCRM; thus, the C-SCRM plan is a living document that must be maintained and regularly referenced for continuous monitoring of implemented controls. These plans should not merely satisfy compliance requirements but should demonstrate the enterprise's ongoing commitment to effectively employing them to shape, align, inform, and drive C-SCRM actions and decisions across all levels.

4.0 Reference Documents

- FAR Part 9 - Contractor Qualifications
- FAR Part 15 - Contracting by Negotiation
- FAR Part 52 - Solicitation Provisions and Contract Clauses
- Executive Order 14028 - Improving the Nation's Cybersecurity
- NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-37 - Risk Management Framework for Information Systems and Organizations
- NIST SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

5.0 Code of Conduct Principles

5.1 Compliance with C-SCRM Standards

- Suppliers must comply with all applicable federal regulations and guidelines regarding supply chain security, including NIST Special Publications and the Federal Acquisition Regulation (FAR).

5.2 Risk Assessment and Management

- Suppliers must conduct regular risk assessments, identify potential vulnerabilities, and implement effective risk mitigation strategies.

5.3 Data Security and Protection

- Suppliers must implement robust data security measures to protect sensitive information, including encryption, access controls, and incident response protocols.

5.4 Incident Reporting

- Suppliers must establish clear channels for reporting incidents, ensuring timely communication and thorough documentation of security breaches or operational disruptions.

5.3 Supply Chain Transparency

- Suppliers must provide transparency regarding their supply chain operations, including the sources of materials and components, to enable effective risk management.

5.6 Third-Party Supplier Management

- Suppliers are responsible for assessing and managing the Cybersecurity risks posed by their own suppliers, ensuring that they comply with similar C-SCRM standards.

5.7 Training and Awareness

- Suppliers must educate their employees and their employees about cybersecurity risks, best practices, and compliance requirements associated with the supply chain.

5.8 Continuous Improvement

- Suppliers are encouraged to engage in ongoing training, assessment, and enhancement of their practices in alignment with industry best practices and evolving threats.

5.9 Documentation and Audit

- Suppliers must maintain documentation of their C-SCRM practices, as well as their suppliers, and be prepared for audits or assessments conducted by the government to ensure compliance.

5.10 Compliance with Laws and Regulations

- Suppliers must comply with all applicable laws, regulations, and standards relevant to their operations and supply chain activities.

5.11 Ethical Conduct

- Suppliers must conduct their business with integrity, honesty, and transparency, avoiding conflicts of interest and unethical practices.

5.12 Labor Practices

- Suppliers must uphold workers' rights, ensuring fair wages, reasonable working hours, and safe working conditions. Child and forced labor are strictly prohibited.

5.13 Environmental Stewardship

- Suppliers are encouraged to adopt environmentally responsible practices and minimize their ecological footprint, including waste reduction and resource conservation.

6.0 Acknowledgment

By signing below, the supplier acknowledges receipt of this Supplier Code of Conduct and commits to its principles and standards.

Supplier Name: _____

Authorized Representative: _____

Title: _____

Date: _____

7.0 Revision History

Rev	Date	Sec./Para.	Summary of change	Authorized by
A	10/28/2024	N/A	Initial issue	