



Software Supply Chain Risk Management Policy

Table of Contents

1. Purpose	3
2. Scope	3
3. Target Audience	3
4. Roles and Responsibilities	3
5. Policy & Compliance	4
5.1 Compliance	4
5.2 Enforcement & Management	5
5.3 Monitoring & Review of Policy	5
5.4 Policy Approval	5
5.5 Exceptions	5
5.6 Document Location	5
6. Policy	5
6.1 Supply Chain Management & Supplier Governance	5
6.2 Authenticity & Provenance	6
6.3 Supplier Governance	6
6.4 Secure Design & Engineering	7
6.5 Product Offering Lifecycle Management & Organization	7
6.6 Protect IP & Product (Supplier) Offering Assets	7
6.7 Secure Coding & Manufacturing Practices	8
6.8 Asset Management	9
6.9 Respond to Vulnerabilities	9
6.10 Detect Vulnerabilities	10
6.11 Identify Cyber Threats	10
6.12 Respond & Recover	11
6.13 Physical Security In-Transit	11
6.14 Awareness & Training (Security-Specific)	11
6.15 Supply Chain Integrity	11
6.16 Supply Chain Resilience	12
6.17 Diversity of Supply Base	12
7. References	12
8. Definitions & Acronyms	13
9. Revision History	13
10. Approvals	14