



TREPOL 2700

Software Supply Chain Risk Management Policy

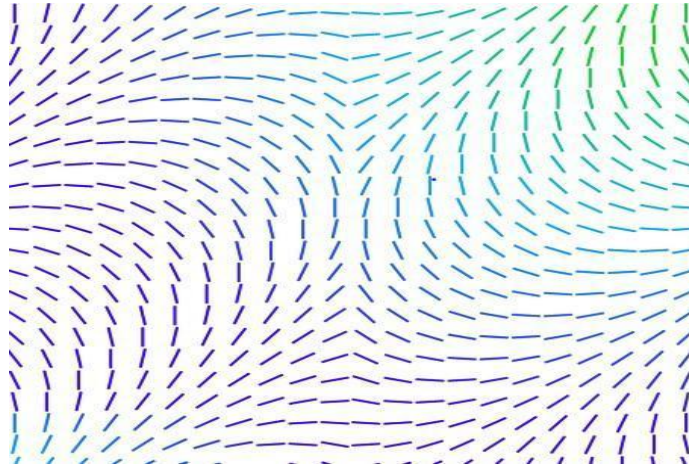


Table of Contents

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

- 7. **References**..... 14
- 8. **Definitions and Acronyms**..... 15
- 9. **Revision History**..... 15
- 10. **Approvals**..... 16

1. Revision History

redacted

2. Approvals