



TREPOL 2900

Source Code Security Policy

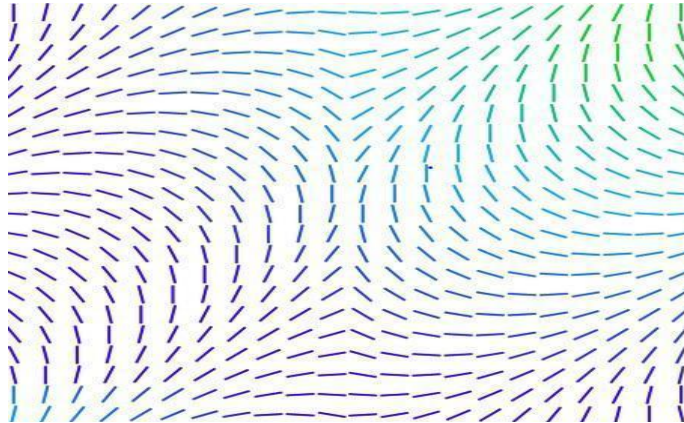


Table of Contents

1. Purpose	4
2. Scope	4
3. Target Audience	4
4. Roles and Responsibilities	4
5. Compliance	6
5.1 Enforcement and Management	7
5.2 Monitoring and Review of Policy	7
5.3 Policy Approval	7
5.4 Exceptions	7
5.5 Document Location	7
5.6 Document Updates	7
6. Policy	8
6.1 Source Code and Artifact Repositories	8
6.2 Source Code Access Controls	8
6.2.1 Access to Software Developers	8
6.2.2 Read-Write Access Compensating Controls	8
6.2.2.1 Code Review	9
6.2.2.2 SOC Monitoring	9
6.2.3 Access Control Lists	9
6.3 Source Code Security Controls	9
6.3.1 Engineering Endpoints	9
6.3.1.1 Lab Systems Exception	10
6.3.1.2 Unmanaged Antivirus Protection Exception	10
6.3.1.3 Malware Check-In Restriction	10
6.3.2 Managing and Controlling Source Code	10
6.3.2.1 Trellix Restricted Data Classification of Source Code	10
6.3.2.2 Trellix Confidential – Internal Data Classification of Source Code	11
6.4 Source Code Outside a Repository	11
6.4.1 Emailing Source Code	11
6.4.2 Remote Access	11
6.4.3 Removable Media	11
6.4.4 Cloud Storage	11
6.4.5 Strong Encryption	12
6.4.6 Off Premises	12
6.4.7 Third-Party Developers	12
6.4.8 Tool Vendor Escalation	12
6.4.9 Mobile Device Requirements	12

6.4.10 Global Export Compliance	13
6.4.11 High Risk Countries Exception	13
6.4.12 Source Code Developed in High Risk Countries	13
6.5 Non-Developer Access to Source Code	13
6.6 Third-Party Access to Source Code	14
6.6.1 Distribution Policy	14
6.6.2 Litigation Exception	14
6.6.3 Third-Party Assessments	14
6.6.4 Certification Artifacts	14
6.7 Contributing to Open-Source Libraries	14
6.8 Reporting Policy Violations	15
7. References	15
8. Definitions and Acronyms	15
9. Revision History	17
10. Approvals	18