Trellix

TREPOL 1200

Acceptable Use Policy

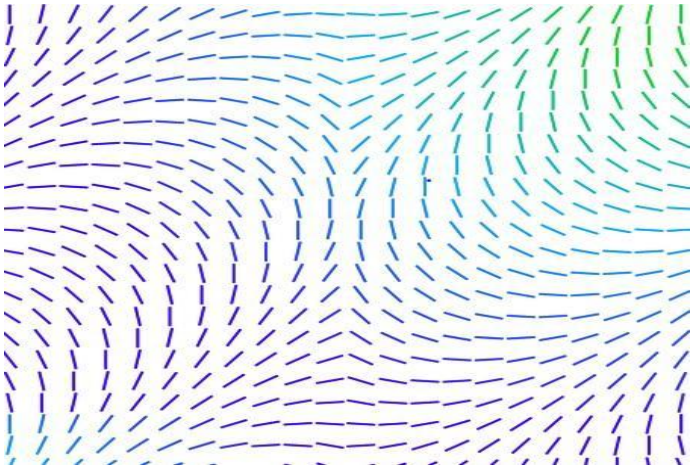

Table of Contents

1. Purpose **4**
2. Scope **4**
3. Target Audience **4**
4. Roles and Responsibilities **4**
5. Policy & Compliance **5**
5.1 Policy Statement 5
5.2 Compliance 6
5.3 Enforcement & Management 6
5.4 Monitoring & Review of Policy 6
5.5 Policy Approval 6
5.6 Exceptions 6
5.7 Document Location 6
6. Trellix's Right to Monitor **6**
7. Appropriate Use of Resources **7**
7.1 Access 7
7.1.1 Principles of "Need-to-Know" & "Least Privilege" 7
7.1.2 Access to Company Data 8
7.1.3 User Access 8
7.1.4 Protecting Passwords 8
7.2 Network Aware Devices 8
7.2.1 Trellix Owned Devices 9
7.2.2 Device Security Protection 9
7.2.3 Contractor Devices 9
7.2.4 Vendor Systems & Connections 9
7.2.5 Unauthorized Network Devices 9
7.2.6 IT Consumables 9
7.3 Software 10
7.4 Storage 10
7.4.1 Use of Removable Media 10
7.5 Messaging 11
7.5.1 Using Instant Messaging (IM) Software on Trellix Devices 11
7.5.2 Use of Email 11
7.5.3 SPAM & Malicious Email Reporting 12
7.5.4 Commercial Emails 12
7.5.4.1 Anti-SPAM Legislation 12
7.5.4.2 Right to Intercept for Unsolicited Bulk Email Prevention 12
7.5.4.3 Consequences of Non-Compliance 12

7.5.4.4 Third Party Use of @Trellix..... 12
7.5.4.5 Using Trellix Resources to Send Unsolicited Emails..... 13
7.5.5 Use of Voice Mail..... 13
7.6 Social Media..... 13
7.7 Electronic Recordings..... 13
7.8 Personal Use of Trellix Resources..... 14
7.9 Working While Mobile..... 14
7.9.1 Remote Access..... 14
7.9.2 Working in Public Places..... 14
7.9.3 Working from Small Office Home Office (SOHO) or Other Off-Site Locations 15
7.10 Inappropriate Use of Information Systems, Data, & Assets..... 15
7.11 Clean Desk & Clear Screen..... 16
7.12 Cloud Computing Services..... 16
8. References..... 17
9. Definitions & Acronyms..... 17
10. Revision History..... 19
11. Approvals..... 20