



Information Security Policy

Table of Contents

1. Purpose	4
2. Scope	4
3. Target Audience	4
4. Roles & Responsibilities	4
5. Compliance	5
5.1 Enforcement & Management	5
5.2 Monitoring & Review of Policy	5
5.3 Policy Approval	6
5.4 Exceptions	6
5.5 Document Location	6
6. Policy	6
6.1 Operational Objectives	7
6.2 Information Security Framework Overview	8
6.2.1 Information Security Policies	8
6.2.2 Distinct from Standards	8
6.2.3 Distinct from Guidelines	8
6.2.4 Distinct from Procedures	9
6.3 Policy Risk Management & Residual Risks	9
6.4 Company Policy Statements	9
6.4.1 Information Security Policy	9
6.4.2 Information Security Risk Management Policy	10
6.4.3 Acceptable Use Policy	10
6.4.4 Global Mobility Services Policy	10
6.4.5 Access Control Policy	10
6.4.6 Information Classification & Handling Policy	10
6.4.7 Information Systems Acquisition, Development & Maintenance Policy	10
6.4.8 Communications & Operations Management Policy	11
6.4.9 Incident Response Policy	11
6.4.10 Physical Security Policy	11
6.4.11 Personnel Security Policy	11
6.4.12 Business Continuity Policy	11
6.4.13 Data Retention Policy	11
6.4.14 Cryptographic Policy	11
6.4.15 Information Security Audit Monitoring & Logging Policy	12
6.4.16 Crisis Management Policy	12
6.4.17 Cloud Security Policy	12
6.4.18 Software Supply Chain Risk Management Policy	12

6.4.19 Third Party Supplier Information Security Policy	12
6.4.20 Source Code Security Policy	12
6.4.21 Malware Handling Policy	13
6.4.22 Artificial Intelligence Use Policy	13
6.4.23 Internal Use of AI Tools Policy	13
6.4.24 Insider Risk Policy	13
7. Definitions & Acronyms	13
8. References	14
9. Revision History	14
10. Approvals	14