FORTIFY SOLUTIONS

Document Title	**:** Quality & Governance Policy
Document No.	**:** FS-GOV-QGP-04-01
Version	**:** 1.0
Approval Date	**:** 01-08-2025
Next Review Date	**:** Annually or sooner as required

Quality & Governance Policy

1. Purpose

This policy establishes **Fortify Solutions'** commitment to delivering services of the highest quality while ensuring robust governance, risk management, and compliance with legal, ethical, and information security standards. The policy provides a foundation for all operations, helping to ensure that our services are reliable, secure, compliant, and aligned with stakeholder expectations.

2. Scope

This policy applies to:

- σ All **Fortify Solutions** activities: **Consulting, Penetration Testing (VAPT), Compliance Advisory, Corporate and Professional Training, and GRC (Governance Risk & Compliance) Advisory**.
- σ All employees, contractors, vendors, and partners performing work for or on behalf of Fortify Solutions.
- σ All information assets (client data, company internal data), physical assets, and operations (digital, physical, remote).

3. Governance Commitments

Fortify Solutions commits to:

a) **Leadership & Accountability**

- σ Top management clearly demonstrates commitment to quality, security, risk management, and ethical governance.
- σ Roles & responsibilities are defined for Leadership team.

b) **Quality Assurance**

- σ Meet or exceed client expectations.
- σ Maintain documented processes, SOPs, and controls to ensure consistency.
- σ Monitor client satisfaction, timely delivery, and quality of deliverables.

c) **Information Security**

- σ Protect confidentiality, integrity, and availability of all sensitive information.

- σ Enforce access controls, data classification, secure handling, incident response, and encryption as per policy.
- σ Ensure continuous compliance with ISO 27001, applicable privacy laws (DPDP, GDPR, and other as applicable).

d) **Risk Management**

- σ Identify, evaluate, and treat business and operational risks proactively.
- σ Maintain a Risk Register and review it regularly.
- σ Incorporate risk considerations in planning, projects, vendor management, and security practices.

e) **Compliance**

- σ Adhere to all relevant legal, contractual, regulatory obligations (including privacy, intellectual property, anti-corruption).
- σ Uphold ethical practices, transparency, and fairness in dealings with clients, employees, and third parties.
- σ Enable whistleblower mechanisms and fair investigations of complaints.

f) **Continuous Improvement**

- σ Use audits, feedback, incident investigations, and management reviews to identify improvement opportunities.
- σ Set measurable objectives (quality, security, client satisfaction, risk reduction).
- σ Review this policy and associated processes at least annually (or sooner as required).

g) **Awareness & Culture**

- σ Ensure all staff are trained in their responsibilities under this policy.
- σ Promote a culture of accountability, integrity, and respect.
- σ Encourage reporting of issues, concerns, or non-conformities without fear of retaliation.

4. Roles & Responsibilities

Role	Responsibilities
Managing Director / CEO	Endorse and support implementation; allocate resources; ensure policy effectiveness.
Quality Manager	Oversee quality systems, monitor objectives, audit performance, client satisfaction.
ISMS / Information Security Manager	Implement security controls, incident response; ensure compliance with ISO 27001 & privacy laws.
Risk & Compliance Officer	Manage risk register; conduct compliance reviews; monitor legal/regulatory obligations.
Department Heads / Project Managers	Ensure policy adherence in everyday operations; escalate issues; report performance.
All Employees / Contractors	Abide by policy, follow supporting policies/procedures; report issues.

5. Policy Enforcement & Non-Compliance

- σ Non-compliance with this policy or subordinate policies (Quality, Security, Ethics) may lead to disciplinary action, up to termination, depending on severity.
- σ Any violation regarding data privacy, corruption, security breach, or other serious misconduct will be investigated promptly.

6. Monitoring, Review & Reporting

- σ Performance will be measured using Key Performance Indicators (KPIs) such as: customer satisfaction, delivery timeliness, number of security incidents, vendor compliance, and others as deemed fit and serve the purpose.
- σ Internal audits will assess compliance with this policy and associated policies.
- σ Management Review Meetings will include policy performance, major incidents, risk trends, and others as deemed fit and serve the purpose.
- σ Policy to be reviewed at least once per year or more often when changes occur in business, technology, law, or risk environment.

7. References

- σ ISO 9001:2015 – Quality Management System standards

- ISO/IEC 27001:2022 – Information Security Management System standards
- Indian DPDP Act 2023 & General Data Protection Regulation (GDPR), where applicable
- **Fortify Solutions'** supporting policies: Access Control, Data Classification & Handling, Incident Response, Risk Management, Vendor Management, Code of Conduct.

8. Definitions

- **GRC (Governance, Risk & Compliance)** – The integrated framework for **Fortify Solutions** to govern operations, manage risk, and ensure compliance.
- **Quality** – Meeting or exceeding client requirements and internal standards.
- **Information Security** – Protecting data from unauthorized access or harm.
- **Risk** – Uncertainty that could impact achievement of objectives.
- **Compliance** – Adherence to laws, contracts, standards.

Signed: _____

Date: _____