**Information Security Policy**

HCL Software is a division of HCL Technologies that develops and delivers a next generation portfolio of enterprise grade software-based offerings with flexible consumption models, spanning traditional on-premises software, Cloud based PaaS, SaaS and bundled managed services.

HCL Software is committed to protecting the critical information assets by implementing and maintaining an Information Security Management System (ISMS) to help ensure that its applicable information security objectives are met, and the ISMS is able to adapt to internal and external changes.

The goal of the ISMS is to protect HCL Software and its customers information assets from threats identified, whether internal or external, deliberate or accidental.

The objectives of Information Security are:

- Maintain the confidentiality of the information such that only authorized persons have access
- Ensure the integrity of information
• Arrange for the availability of information such that only authorized persons can access the information, assets and systems whenever required

The HCL SW aligns with the ISO/IEC 27001:2013 as a base security standard and extends to other security standards, for example ISO 27017, ISO 27018, SOC 2 Type II, PCI and HIPAA.

HCL SW has an established information security governance structure to effectively and efficiently manage the ISMS, inclusive of:

• Identification of information assets
• Management of risks to an acceptable level through the design, implementation, and maintenance of risk treatment plans
• Communication of information security objectives and performance in achieving these objectives
• Development of security awareness programs and training as appropriate
• Compliance with local laws and regulations and contractual obligations as relevant to Information Security

This Information Security Policy is supported by specific internal policies in the following aspects of Security Management ...

• **Risk Management** – Risks are
managed in a standard lifecycle with status reported to senior management at regular intervals

- **Human Resource** – Includes controls around culture, mandatory annual trainings, communication, performance evaluation process and termination process.

- **Physical and Environmental Security** – Includes building perimeter security as well as secure protection mechanisms for internal offices, infrastructure, data center / server rooms.

- **Supplier Management** – Includes vendor risk assessment and formal agreements with details of any SLAs required on the supplied product or service.

- **Information Security Aspects of Business Continuity** - Includes details used to support backup, business recovery and continuity.

- **Internal Audit & Compliance** – A dedicated team to manage Internal Audit and management of compliance.

- **Asset Management** – A formally managed register for all assets in HCL Software’s environments. Each asset has a structured set of attributes as its definition.

- **Access Controls** -
Includes the definition of unique user ID’s and formal password controls.

- **Cryptography** – encryption standards are applied.

- **Communication Controls [Networks and Firewalls]** – Includes details of the protection levels set and the restricted controls for such vital resources.

- **System Acquisition, Development, Maintenance** – Systems acquisition, development and maintenance of products and environments is managed per policy.

- **Information Security Incident Management** – Security incidents are captured and managed in a structured lifecycle.

- **Security Readiness Standard, Provisioning and De-provisioning** – A minimum security standard is in place for all devices being provisioned to or de-provisioned from its infrastructure.

- **Patch Management** – Patches are applied to a timeframe based on the severity of the vulnerability.

- **Security Monitoring and Logging** – Logs are collected and reviewed by the dedicated Security Operation Center (SOC) team to identify alerts of unauthorized activity.

- **Vulnerability Scanning / Penetration Testing** – Independent Penetration Testing is conducted a minimum of once per year.

- **Health Check of Environments / Devices** – This is based on the CIS Benchmark controls.