

## Information Security Asset Classification Policy

- Any asset which has a business value is to be considered as an information asset. This will include, but not be restricted to; information in digital and non digital format, portable media, network infrastructure devices (servers, routers, switches, modems, tape drives, storage devices, load balancers, ids, ips, firewalls), applications, services, desktops , laptops and mobile computing and communication devices, utilities such as power generation, conditioning and distribution equipment and air-conditioning equipment amongst others.
- Valuation of information assets shall take into account the Business Impact Parameters such as (Financial, Operational, Regulatory/Compliance, Competitive and Legal); should they be compromised in any manner.
- A score shall be assigned for each of the Business Impact Parameters against Business Impact Criteria such as HIGH, MEDIUM and LOW comprising point scale of 5, 2 and 0.5 respectively, to arrive at the Risk Impact Class.
- Risk Impact Class shall be categorised as CRITICAL, SIGNIFICANT, MODERATE AND NEGLIGIBLE. The Risk Impact Class (RIC) will lead to the classification of the Information Asset.
- All Information generated or in existence shall be clearly identified and an Information Asset Classification (IAC) template shall be drawn up by respective Department Implementer (DI). The IAC shall only be effective after approval from the authorized signatories.
- Labelling methods in pursuant to the classification modality shall be adopted.
- Retention Limits shall be defined for every category of the identified information asset in consonance with the requisite business, regulatory and legal requirements.
- The term 'owner' for an information asset is an individual or department which has a management approval and hence responsibility for controlling the production, development, maintenance, use and security of an asset. Owners shall set the security requirements for information assets and shall be responsible for communicating those requirements to all the custodians.
- Custodians shall be those who are the authorized employees/departments who shall have the custody of the Information Asset.
- There shall be a formal review mechanism to ensure that the listing of all Information Assets along with their valuation and classification is current, accurate and relevant.
- In order to measure the effectiveness of the process of the maintenance of the inventory of the Information Assets, stakeholders shall be evaluated against the metrics which have been defined. Corresponding actions and records shall form as supporting elements of the compliance process.
- Any exception shall be managed through a formal process.

**Date :** November 1, 2017



**T V Narendran**  
CEO & Managing Director

