Information Security and Privacy at Airtel

Safeguarding customer privacy, and ensuring security of data across its operations, lines of business and supply chain, is a key focus area for Airtel. This is not just to ensure legal and regulatory compliance, but to reinforce the trust that our customers and other stakeholders have placed in us. To ensure that the privacy of information is maintained during the entire information lifecycle, we have implemented robust internal systems and checks. This is encapsulated in the comprehensive Bharti Airtel Information Privacy Policy, which contains management direction and guidelines to ensure privacy of personal information collected by Airtel so that information is handled in accordance with the appropriate laws, regulations and contractual obligations.

The Policy is owned by the Chief Information Security Officer and approved by the Airtel Management Board, and is embedded in the risk/compliance management system at Airtel. It is applicable to all employees of Airtel and third parties including suppliers, who have access to information of customers, employees and vendors. We have identified different stakeholders and assigned accountability for relevant clauses of the Policy that fall within their area of responsibility. We are certified against global standards such as ISO27001 and ISO22301, and have adopted the NASSCOM-DSCI Privacy Framework (DPF) to protect the privacy of personal information from unauthorized use, disclosure, modification, or misuse, which allows us to identify critical customer information and ensure adequate measures to safeguard it. To ensure compliance with the Policy, we conduct periodic internal and external audits of various functions.

Information moving within and across the boundaries of our organization is effectively monitored in real-time for any breach in company policy. Any non-compliance is immediately escalated and investigated. The Circle Information Security Council (CISC) recommends disciplinary actions against employees, partners or third parties involved in privacy breaches. Having zero tolerance towards the breach, strict actions, like separation from services and/or police complaints, are initiated against the individuals. Non-compliance of any third party with the privacy practices followed at Airtel is ground for disciplinary actions up to and including termination of the contract. As per the policy, the Third party is required to establish a procedure to ensure that the associates are made aware of their personal liability of personal information and that any deviation to the policy may lead to the associate's services being discontinued/ terminated.

Airtel has also established an efficient Fraud Management Program driven by revenue assurance and fraud management experts, which makes use of highly sophisticated and evolved tools and processes to detect and prevent the occurrence of fraud. Airtel associates with Law Enforcement Agencies (LEA) to support investigations by provision of customer information and complying with all requests as per regulatory norms.

We work with industry, government, law enforcement and community organizations to help our customers understand and manage the risks associated with the online world. We support a range of government initiatives to raise awareness, and provide online education and guidance. Some of the measures undertaken in the last few years include:

- Working with CERT-In to resolve cyber incidents and malware infections
- Upgrading technology constantly to reduce threat exposures

• Associating with Law Enforcement Agencies (LEA) to support investigations

• Actively participating in multiple national level working groups and numerous international forums on internet safety and cyber security