TATA COMMUNICATIONS
TRANSFORMATION SERVICES

INFORMATION SECURITY POLICY

Tata Communications Transformation Services Limited (TCTSL) is committed to provide a trustworthy environment to safeguard business, customer and employee's data/information/information systems through its well-defined information security framework aligned to ISO 27001:2013.

TCTS shall implement and maintain best practices and procedural controls to identify and protect information/ information systems thereby ensuring confidentiality, integrity, and availability (CIA) as per the ISO standards.

All TCTS's Information assets must conform to TCTS's information security policies standards and procedures as outlined below:

Protection of TCTS's information assets - Including but not limited to hardware, software, electronic data or information (in any form) and personnel.

Protection of client's information assets - Unless any specific requirements have been documented and/ or contracted by a client, all clients' information assets will be managed following the applicable TCTS's information security policies, standards, and procedures.

TCTS's ownership of information - Any information not identified as the property of other parties, will be considered as property of TCTS, provided TCTS asset is used for storage or transmission of such information.

Information Rights Management - All employees must adhere to the IRM/Data classifications to protect documents containing sensitive information from unauthorized access. IRM protects files from unauthorized copying, viewing, printing, forwarding, deleting, and editing.

Generative model/AL/ML usage - AI Model (Generative Model, Artificial Intelligence and Large Language Model) shall be used solely for legitimate business purposes and in accordance with company- policies and applicable laws.

All AI model implementations shall use only licensed, and Company approved tools.

Use of freeware and tools that have not been evaluated, authorized, or approved by the company in accordance with this Policy are not permitted. Users shall refrain from using corporate email ids to register with opensource / freeware tools.

Asset disposal - To provides a rigorous and consistent process to ensure IT assets that are deemed "end of life" or to be recycled, are securely wiped off any data before it is redistributed or taken out of the TCTS premises in adherence to the IT policy.

User monitoring and privacy - All actions occurring on or over TCTS's information assets shall be monitored without notice. Users of TCTS's information assets should have no expectation of privacy in their actions, processes, communications, or files unless such privacy granted by a separate agreement.

Violation consequences - Violation of the information security policies, standards, or procedures may lead to security policies, standards or procedures may lead to disciplinary action as per the HR policies of Tata Communications Transformation Service Limited up to but not limited to termination of employment.

TCTS is committed to satisfy the applicable requirements and continually improve its information security management system. We will communicate this policy to all our employees and ensure appropriate training provided to raise awareness on information security.

Agnel Navin

Agnel Navin
CEO
1st April 2024

Version	Description	Date of issue
1	Initial Policy	10th Jul 2007
2	Updated as per ISO 27001:2013	17th Oct 2014
3	BYOD policy withdrawal	01st Feb 2020
4	Updated Information Rights Management	03rd Nov 2021
5	Updated AI model usage guidelines	14th Jun 2023