TATA CAPITAL

CYBER SECURITY POLICY

Version 1.1

INTERNAL

TABLE OF CONTENTS

1. Document Summary

Revision History		
Version No	Date	Approved By
V 1.0	March 21, 2018	Board of Directors
V 1.1	October 30, 2019	Board of Directors

Change History				
Author	Reviewer	Version No	Review Date	Change Description
IS	CISO	1.0	1/4/2018	Drafted as per Master Directions
IS	CISO	1.1	5/8/2019	Annual Review, Version update, Inclusion of NHB circular number, No Change in policy content.

Key Details	
Issuing Authority	CISO
Approving Authority	Board of Directors
Review Frequency	At least once a year or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness
Classification	Internal Circulation
Mode of circulation	PDF document with view only rights
Coverage	TCL and its Subsidiaries
Location of the read only document	Tata Capital Intranet
Master Direction Circular Clause	DNBS.PPD. No.04/66.15.001/2016-17 dated June 08, 2017 Clause 3.2,3.3,3.4,3.5,3.6,3.6 NHB/ND/DR5/ Policy Circular No.90/2017-18 dated June 15, 2018

2. Policy Background

As a part of Cyber Security Governance, the organisation has developed a Cyber Security Policy to address the various aspects of the Cyber security.

Tata Capital group entities are regulated by namely RBI/ NHB/ SEBI/ IRDA. The regulator also mandates a need for a Cyber Security Policy. This policy is framed based on the guidelines from the regulator as well as the best practices.

This Cyber Security Policy is distinct from the Information Security Policy

3. Group Structure

Tata Capital Limited ("Company" or "TCL"), the flagship financial services company of the Tata Group, is a subsidiary of Tata Sons Limited and is registered with the Reserve Bank of India ("RBI") as a Systemically Important Non-Deposit Accepting Core Investment Company ("CIC"). TCL and its subsidiaries (collectively referred to as "Tata Capital") are engaged in a wide array of services/products in the financial services sector. The list of subsidiary companies is as listed in Annexure A.

The Board of Directors, as well as the regulators of these legal entities are different.

4. Policy Statement: (ID.GV.1)

The organization shall take all necessary steps to protect information and information infrastructure in internet/cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation from relevant external bodies both Private, Public and the Government.

The objective of this Policy is to proactively identify the Cyber threats and the risks manifested in information infrastructure and manage, mitigate, avoid, transfer or accept the risks as per the risk appetite of the organisation.

5. Applicability of the policies

The policy is applicable to the parent as well as all the subsidiary companies (refer Annexure A). There will be two sets of policies, which will be similar in nature, based on the regulator (RBI, NHB, etc).

However, this policy shall be approved by the Board of each of these legal entities to comply with the Regulatory requirements.

6. Scope of Policy

Cyber Security Policy is applicable to all cyber facing Information/ Data/ Information Processing facilities and IT assets of the Organisation which is available to or accessible by the organisation's Employees, vendors, contractors, consultants, temporary staff and other individuals even if, affiliated with Third Parties and are utilising the Organisation's network.

All automated information assets and services that are utilized by the Company's Network are covered by this policy. It applies equally to network servers, Wi-Fi devices, firewalls, routers, switches, hubs, other peripheral equipment, workstations, desktops and laptops and all types of software within the company's LAN and WAN environment.

7. Interrelation with Information Security Policy

The Organisation has a separate Board approved policy for Information Security.

This policy is in addition to Information Security policy. There are certain overlaps in terms of people, processes and technology as well as the implementation.

Information security policy is designed to protect Information and Information Systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide Confidentiality, Integrity, Availability, Authenticity.

Cyber Security Policy is designed to Prevent, Detect, Respond and Recovery in an effective manner, from Cyber Attacks arising out of the various threat vectors, with sole objective of building Organisational Resilience.

8. Components of the policy

The various components of the policy shall cover the following structure as defined below

a. Governance
b. Legal Requirements & Assurance Framework
c. Cyber Security Risk management
d. Identify & Protect (Including Vulnerability Management)
e. Cyber Crisis management plan
f. Cyber Security Preparedness indicators
g. Skilled Personnel
h. Cyber Security Awareness
i. Security Operations Centre
j. Cyber Liability Insurance

9. Governance

TCL shall have the governance structure as follows:

- The Board
- Cyber Security Committee
- Individual Team/ Role other than Cyber Crisis Management
- Cyber Crisis Management Team

9.1 Board

The board is responsible for effective evaluation, directing and monitoring the overall Cyber Security program of the Organisation. In addition, the Board also shall periodically

- Approve the Policy for the first time. Any subsequent modifications to the policy shall be approved by the Information/ Cyber Security Group. However, the board will have to be apprised of any major changes done to the policy.
- Approve the necessary budgets on an annual basis for the various Cyber Security activities across the Technical Controls as well as Human Resources Training and Education

9.2 Cyber Security Committee

- TCL has constituted an Information Security (IS) Committee as per the Information Security Policy. The members of the IS committee will be the members of the Cyber Security Committee as well.

9.3 Department Roles and Responsibilities (ID.GV.2)

9.3.1 All Users

All personnel (including staff, outsourced personnel, vendors as well as any other third party) shall take all necessary precautions to protect company's network related information and systems under their control.

9.3.2 Information Security Department

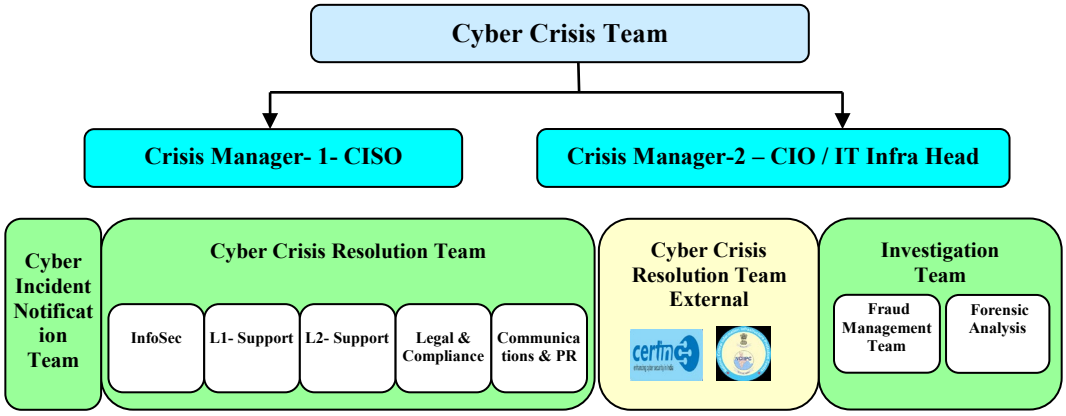
The IS department shall be responsible for the reporting of the incidents to the regulator jointly in consultation with CISO/ IT/ RISK

9.3.3 IS Audit Department

The IS Audit Department will be responsible for the Audit of the Cyber Security Policy and its related implementation to ensure that the necessary controls are in place.

9.3.4 Cyber Crisis Management Team

The various teams and their composition with respect to the CCMP (Cyber Crisis Management Plan) is as below. The detailed roles and responsibilities of the Team as well as members are elaborated in the CCMP.



10. Legal Requirements & Assurance Frameworks (ID.GV.3):

10.1 NIST CSF Framework

In order to implement the Cyber Security policy, there needs to be a framework which is supposed to be used by the organization.

The Organisation shall adopt the "Framework for Improving Critical Infrastructure Cyber Security" (herein referred to as CSF) Ver 1.0 published by the National Institute of Standards & Technology (NIST)

The CSF will be adopted after necessary localization as the context of the Framework is United States. The organization may use a phased approach for the implementation of the CSF.

The CSF' Core functions as depicted in Table -1 will be adopted in totality with supplemental procedures defined for each of these core functions and their sub categories.

The organization shall not use the 'Tiered' approach as well as the 'Profile' mentioned in the Framework.

The organization shall prepare an additional mapping of those controls in existence and any additional controls will only be documented and implemented as envisaged in the CSF.

10.2 RBI/ SEBI/ NHB/ IRDA

The organisation is regulated by various agencies and all relevant notifications related to the Cyber security will form part and parcel of the overall CSF to be implemented across the organization.

10.3 Information Technology Act 2000

The Information Technology Act is the overarching Act in India with respect to Cyber law in India. The Organisation shall adopt the same and necessary controls as defined related to Cyber security shall be engrained in the policy.

10.4 NCIIPC

The organisation has been identified as Critical Information Infrastructure by the GOI and all necessary reporting and compliances as defined in the specific rules and regulations will form part this Policy.

11. Cyber Security Risk Management (ID.GV.4)

The Risk Assessment and the Risk Management of Cyber Security Risk is covered in the NIST Framework assurance framework as below:

Risk Assessment (ID.RA): The organization understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

The results of the Annual Risk Assessment shall be placed before the ORMC for the review.

The Risk assessment process shall be common across Information Risk as well as Cyber Security Risks

12. Identify and protect (including Vulnerability Management)

The functions of Identify and Protect is documented through the Information Security Policy and procedures while the prevent, detect, respond and recover are specifically covered in the Cyber Crisis Management plan.

The vulnerability management is part of multiple functions in NIST as below:

- ID.RA-1: Asset vulnerabilities are identified and documented
- ID.RA-2: Threat and vulnerability information Cyber Threat Intelligence is received from information sharing forums and sources
- ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- PR.IP-12: A vulnerability management plan is developed and implemented
- DE.CM-8: Vulnerability scans are performed
- RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

The organization shall implement a robust vulnerability management mechanism and shall use the existing system/ process adopted and implemented for Information Security.

13. Cyber Crisis Management Plan

The Organisation shall implement a Cyber Crisis Management Plan which will encompass coordination with internal stake holders as well as external stake holder's like Cert-in, RBI/ NHB/ SEBI/ IRDA/ NCIIPC etc.

CCMP shall address the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment which is a function as defined in the CSF

This plan will form a part of the respond and recover function of the CSF.

There shall be a Cyber Incident Management designed as follows which shall be part of the detailed CCMP.

13.1 Incident Management

The organization shall implement a robust Cyber Security Incident management mechanism in place. The organization shall use the existing Incident management system/ process adopted and implemented for Information security.

The incident management process will be covered as a part of the Respond and Recover Function of the CSF

13.2 Reporting

The organisation shall implement a mechanism of Reporting the Cyber Security Incidents to the following authorities.

- RBI, NHB, NCIIPC, Cert-in, Law enforcement agencies etc.

This is not an exhaustive list. The organization shall add any other entities reporting based on the statutory requirements over a period of time.

The organization shall implement a CCMP in line with the above guidelines

14. Cyber Security Preparedness Indicators

The Organisation shall develop Cyber Security Preparedness indicators in a phased manner.

These indicators will be placed before the ORMC for their information and necessary action as necessary budgetary approvals may be required for the Indicators to be above the satisfactory level.

The Organisation shall adopt the C2M2 Framework developed by the Department of Energy as the Cyber Security Preparedness indicators which includes the necessary maturity Levels.

15. Skilled Personnel

The Organisation shall ensure that the Cyber security function is adequately resourced with necessary requisite skills in terms of the staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc.

16. Cyber Security Awareness

The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

The Organisation shall conduct periodic awareness sessions for the

- Board, All employees, Contract Employees

This training will be conducted along with the Information Security training.

17. Security Operations Centre (SOC)

A separate outsourced SOC shall be established to proactively address risks faced by Cyber threats. This is necessary as the organization may not have the necessary skill-set and maturity levels to manage the activities in-house.

The sole objective of outsourcing the SOC is that the skill sets of the outsource agency is far more superior to that of the Organisation and they have necessary wherewithal to be updated on the monitoring of the Cyber Risks.

18. Cyber Liability Insurance

The organisation based on the Risk assessment conducted and on the recommendation of the Cyber Security Committee shall insure the Cyber Security Risk through necessary Cyber Liability Insurance.

Annexure A- Legal Entity

Sr No	Group /Company Name	CIN	Nature of Business	Regulator
1	Tata Capital Limited (TCL)	U65990MH1991PLC060670	NBFC	RBI
2	Tata Capital Financial Services Limited (TCFSL)	U67100MH2010PLC210201	NBFC	RBI
3	Tata Cleantech Capital Limited (TCCL)	U65923MH2011PLC222430	NBFC	RBI
4	Tata Capital Housing Finance Limited (TCHFL)	U67190MH2008PLC187552	HFC	NHB
5	Tata Securities Limited	U67120MH1994PLC080918	Depository Participant, Investment Banking, MF distribution	SEBI
6	Tata Capital Pte. Ltd.		Fund management, advising on corporate finance, dealings in securities and investments in debt papers	Monetary Authority of Singapore
7	Tata Capital Plc.		Regulated services, intermediary providing fund marketing services to TCAPL.	Financial Conduct Authority, UK
8	Tata Capital Advisors Pte. Ltd. (TCAPL)		Fund Management	
9	Tata Capital Markets Pte. Ltd. (TCPL)		Capital Market Services	Monetary Authority of Singapore

Annexure B – Reference Document

Internal Document	
Sr No	Description
1	CCMP
2	Information Security Policy

External Document		
Sr No	Name /Ref No	Description
1	DNBS.PPD.No.04/66.15.001/2016-17 dated June 08 ,2017	Master Direction - Information Technology Framework for the NBFC Sector
2	NHB/ND/DR5/ Policy Circular No.90/2017-18 dated June 15, 2018	Guidelines of the National Housing Bank (“NHB”)

Annexure C - Acronyms

Acronyms	Expansion
CCMP	Cyber Crisis Management Plan
CIC	Core investment Company
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
CSF	Framework for Improving Critical Infrastructure Cyber Security
CTO	Chief Technology Officer
IT	Information Technology
IRDA	Insurance Regulatory Development Authority
NCIIPC	National Critical Information Infrastructure Protection Centre
NHB	National Housing Board
PFRDA	Pension Fund Regulatory Development Authority
RBI	Reserve Bank of India
SEBI	Securities & Exchange Board of India
SOC	Security Operations Centre