Cybersecurity Policy
Version 1.0

Approved by
Board of Directors in their meeting held on August 05, 2025

CYBERSECURITY POLICY

1 Introduction

Bharti Telecom Limited ("Company") and its IT service provider, with this policy shall strive for the preservation of the Confidentiality, integrity and availability of Company's information assets pertaining to customer's data, for safe & secure computing environment in order to build adequate trust & confidence in electronic transactions.

2 Scope

a) This policy applies to all employees, contractors, consultants and third-party users (internal and external) accessing Company's information systems from within or outside.

b) This policy covers the usage of all of the Company's information technology and communication resources, including but not limited to:

i) All computer-related equipment like PCs, workstations, telecom equipment, databases, printers, servers, shared computer resources etc. & all networks & hardware to this equipment is connected.
ii) All software including purchased or licensed business software
applications, in-house applications, vendor/supplier provided applications. Computer operating systems, firmware and anyother software residing on Company owned equipment.

3. Purpose

- To safeguard the cyber facing information infrastructure of the Company various types of cyber threats
- All the third-party vendors are to be managed as per the Company Third Party Security Policy.
- Company shall co-ordinate with external agencies during and after the cyber crisis as per the *Company Cyber Crisis Management Plan (CCMP)*.
- An indicative but not exhaustive list of requirements to be put in place by Company to achieve the baseline cyber security framework given in the policy. This may be evaluated periodically to integrate risks that arise due to newer threats, products or processes.

4. Roles and Responsibilities

Head information Technology Cell/Dept:

- Head of IT Cell/Department will be responsible for bringing to the notice of the Board/IT sub-committee of the board about the vulnerabilities and cyber security risk the Company is exposed to.
- Head of IT Cell/Department by virtue of his role, may ensure inter alia, current /emerging cyber threats to business and the Company's preparedness in these aspects are invariable discussed in such committee(s).
- Head of IT Cell/Department shall manage, monitor and drive cyber security related projects.
- Should co-ordinate the activities pertaining to Cyber Security Incident Response Teams within the Company.
- Shall develop and get an independent assessment of Cyber Security including its coverage at least on a quarterly basis.
- Shall have a robust working relationship with Company's Top Management. Head of IT Cell/Department may be a member of (or invited to) committees on operational risk where IT/IS risk is also discussed.

- Head of IT Cell/Department shall be adequately staffed with technically competent people. If necessary through recruitment of specialist officers commensurate with the business volume, extent of technology adoption and complexity.
- Shall be an invitee to the IT committee and IT steering committee.

Information Technology Cell/Department:

- To provide IT products support and services to the divisions and functions in accordance with the cyber security requirements of the Company.
- Provide alternative solutions on industry practice to satisfy increased protection requirements.
- Provide relevant support to other on meeting cyber security objectives and plans.
- Provide periodic metrics to evaluate the cyber security posture of the Company on a quarterly basis.
- Coordinate all activities necessary for compliance to the cyber security policy
- Oversee the execution of the cyber security planning at the functional level
- Maintain and update the relevant document.

Human Resources

- Ensure that all personnel are made aware of their information / Cyber security responsibilities
- Assign relevant information/Cyber security trainings to staff
- Provide guidance and support on the procedures that ensure compliance with applicable HR policies and employment regulations
- Address security requirements for all personnel before, during and at termination or change of employment which include trigger access to system, email and physical access at time on-board/off boarding of employee

5 Policy

5.1 Implementation Approach

Successful implementation of the Cyber Security Policy requires continuous commitment, governance and action by various stake holders who are collectively responsible for the Company's approach to cyber security. Company shall develop and maintain or hire professional cybersecurity workforce. Company has implemented various controls/measures to address various cyber security threats . Company will adopt new innovative cyber security technology and solutions as required from time to time to protect ban information assets.

- Cyber Crisis Management Plan of the Company should cover effective measure prevent cyber attacks and to promptly detect any cyber intrusion so as to respond / recover / and contain the fall out.
- Respective Officers /Management of IT Dept. Controlling Cyber facing applications must take following steps to make progress against the Cyber Security Objective.
- Identify & Safeguard Company's Cyber facing information Infrastructure.
- Identify & prepare a list of the Cyber facing information infrastructure Assess the threat to Cyber facing information infrastructure.
- Identify the Gap and the cyber security controls
- Implement cyber security controls / standards or suggest management action plan to mitigate risk.
- Analyze cyber security trends and threats to provide timely reports to management
- Always make the use of trustworthy technology products and services
- Continuously monitor the security posture of cyber facing IT & information infrastructure.

Respond, resolve and recover from cyber incidents:
In case the cyber facing infrastructure, the asset owner suspects any incidents then:

- Do the preliminary assessment of the incident
- If any cyber-attack is observed, report the matter immediately to the competent authority in accordance with the Company's cyber crisis Management plan.
- Take immediate remedial steps to stop/reduce the cyber infections within cyber facing information infrastructure as per CCMP.
- Take action to correct and recover from cyber security incidents and system failures
- Establish mechanisms and procedures to facilitate timely information sharing and action among stakeholders as per the CCMP.
- Enhance and maintain situational awareness capabilities.
- Establish and continuously enhance incident response capabilities
- Ensure preparedness by conducting cyber security exercises and drills.

5.2 Cybersecurity Awareness & Training

Company shall take the steps to enhance cyber security awareness amongst the staff using trainings, posters, mails etc. on continuous basis.
Staff of IT Dept. Handling cyber facing applications must take periodic trainings to make themselves aware of new cyber threats and measures

5.3 Reporting and Performance Measurement

- Performance of Cyber Security implemented by the Company should be monitored continuously and based on the assessment future cyber security requirements should be identified.
- Regular assessment should be carried out for identifying potential threats in cyber security.
- Report about the Cyber Security Incident should be put before the Board and return thereof should be to be submitted to RBI on due date.
- Cyber incidents shall be reported to company by outsourced vendor immediately, so that the incident is reported by the Company to the RBI/CERT within 6 hours of detection of incident.

5.4 Cybersecurity Domains

Inventory Management of IT Assets

- Company should maintain an up-to-date inventory of IT assets. IT assets include systems and network, including disaster recovery systems and networks with their supporting facilities but limited to information, software, physical, service and people indicating their criticality.
- Any remote administration connections authorized by Company should use strong authentication (typically two-factor authentication) as well as corresponding encryption methods (such as ssh, ssl and vpn) to secure communication traversing the network.
- Company should ascertain the risk related to critical information stored, transmitted, processed and accessed.

Preventing Access of unauthorized software

- Company should maintain central inventory of all software(s).
- Company should develop mechanism to control installation of unauthorized software in the Company.
- Company should track use of authorized / unauthorized software (if any) in the Company.
- Company should define procedures for granting and approving exceptions which at minimum should cover justification of exceptions, duration of exception and authority for approving.
- Company shall white list authorized application/software/ libraries etc.

Environmental Controls

- A cyber risk profile based on activities at various locations such as Administrative offices, branches, data centre and disaster recovery site, should be documented and maintained which help risk based decision and implementation of cyber security controls.
- Company should ensure that physical access to information processing areas and their supporting infrastructure (communications, power, and environmental) are controlled to prevent, detect, and minimize the effects of unintended access to these areas (e.g., unauthorized information access, or disruption of information processing itself).

- Company shall evaluate the cyber security risks and take up cyber insurance of an appropriate value from time to time. The need will be assessed on a yearly basis.

Network Management and Security

- Network security architecture should be documented at Company level. Network security architecture should be updated as and when there are major changes inCompany's environment or at least annually.
- Security architecture and standard security management principles should be applied in network devices configuration, vulnerability and patch management and change in routing table or setting of network devices.
- Access to network's device should be restricted to only Company's authorized network staff and appropriate access control mechanism that support individual accountability and access restriction.
- Company should install network security devices, such as firewalls as well as intrusion detection and prevention systems, to protect its IT infrastructure from security exposures originating from internal and external sources.

Secure Configuration

- Document and apply baseline security requirements/ configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically
- Periodically evaluate critical device (such as firewall, network switches, security devices, etc.) configurations and patch levels for all systems in the Company's network including in Data Centers, in third party hosted sites, shared-infrastructure locations.
- Company should document minimum baseline security standards (MBSS) for IT platforms.
- The MBSS should be tested before any major release on an IT platform.
- The MBSS should be reviewed at least once annually and before major upgrade.

Anti Virus and Patch Management

- Follow a documented risk-based strategy for inventorying IT components that need to be patched, identification of patches and applying patches so as to minimize the number of vulnerable systems and the time window of vulnerability/exposure.
- Implement and update antivirus protection for all servers and applicable end points preferably through a centralized system
- Put in place systems and processes to identify, track, manage and monitor the status of patches to operating system and application software running at end-user devices directly connected to the internet and in respect of Server operating Systems/ Databases /Applications/ Middleware, etc
- Periodically conduct VA/PT of internet facing web/mobile applications, servers & network components throughout their lifecycle (pre- implementation, post Implementation, after changes etc.)

- Periodically conduct Application security testing of web/mobile applications throughout -their lifecycle (ore-implementation, post implementation, after changes) in environment closely resembling or replica of production environment.
- Company should implement security controls to provide robust defence against the Installation spread and execution of malicious code at multiple points in the enterprise
- Mechanisms such as-web security, anti-malware and continuous monitoring to detect advanced threats such as ransom ware, cyber extortion, data destruction, DDOS should be implemented.
- Anti-Virus should be installed on all end points, servers and centrally, managed for policy configuration management, virus definition updates.
- Company should implement and maintain preventive, detective and corrective measures across the enterprise to protect information systems and technology from malware.
- Anti-Malware packages for operating systems should be deployed and definitions should be periodically updated.
- Malware protection should be installed on all web-gateways, exchange servers and centrally managed for policy implementation.
- Company should implement white listing of internet websites/systems.

User Access Control and Management

- Provide secure access to the Company's assets/ services from within/outside Company's network by protecting data/ information at and in-transit.
- Carefully protect customer access credentials such as logon user id, authentication information and tokens, access profiles, etc. against leakage/attacks
- Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a need to know basis and for specific duration when it is required following an established process.
- Implement appropriate (e.g. centralized) systems and controls to allow, manage, log and monitor privileged/supervisor/administrative access to critical systems (servers/OS/DB, applications, network devices etc.)
- Implement controls to minimize invalid logon counts, deactivate dormant accounts.
- Monitor any abnormal change in pattern of logon.

Secure Mail and Messaging System

- Implement effective systems and procedures to ensure that e-mails are used as an efficient mode of business communication.
- Ensure that e-mail service and operations remain secure, efficient while communicating within intranet as well as through internet.
- Email specific server controls should be documented.
- Security of email communication should be enhanced by use of disclaimer, hashes or encryption.
- Company should control permissible attachment types in email systems.

Removable Media

- By default, access to removable media, drives {USB ports, CD / DVD ROM drives, floppy drives) should be disabled.
- Critical and sensitive information stored in removable media should be sanitized before disposal. Removable media should be disposed of securely and safely when no longer required.
- Company should deploy governing mechanism for use of personally owned and official mobile devices.
- Company should deploy mechanism to scan removable media for malwares, before granting any read /write access.
- Company should implement centralized policies through active directory or endpoint management systems to restrict use of removable media.

- Exceptions for granting write access to removable media should be granted after approval of Head of IT and regular recertification process should be established, tracked and documented.

User \ Employee \ Management Awareness

- Company should deploy mechanism to protect data at rest and in transmit by implementing secure access controls to the Company's network.
- Company should deploy mechanism in place to protect customer access credentials against data leakages.
- Company should provide access rights on a need to know basis for specific duration.
- Users should not be granted administrative rights on end-user workstations /laptops.
- Company should implement centralized authentication and authorization system for accessing IT assets including but not limited to applications, operating systems, databases, network and security devices/systems, point of connectivity.

Customer Education and Awareness

- Customer education and awareness program should be designed and implemented.
- Customers should be encouraged to report any phishing mails/websites, etc.
- Customers shall be educated on the downside risks involved in sharing of their login credentials to any third party and the consequences arising of such situations.
- Communication medium such as E-mail, SMS, banner, advertisements, Audio-Visual at branch offices should be used to improve customer cyber security awareness.

Backup and Restoration

- Periodic backup of the important data should be taken and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files).

Vendor and Outsourcing Risk Management

- Company shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment
- Among others, Company shall regularly conduct effective due diligence, oversight and management of third party vendors/service providers & partners.
- Establish appropriate framework, policies and procedures supported by baseline system security configuration standards to evaluate, assess, approve, review, control and monitor the risks and materiality of all its vendor/outsourcing activities shall be put in place
- Company shall ensure and demonstrate that the service provider adheres to all regulatory and legal requirements of the country. Company may necessarily enter into agreement with the service provider that amongst others provides for right of audit by the Company and inspection by the regulators of the country.
- For more information refer to *Company IT Outsourcing Policy.*

Vulnerability Assessment and Penetration Testing

- The Company should periodically conduct vulnerability assessment and penetration testing (VA/PT) for all the critical systems.
- Vulnerabilities identified should be remediated in a timely manner.
- Penetration testing of public facing systems and critical applications should be carried out by professionally qualified teams.
- Concerned Asset owners/team leaders should ensure that necessary remedial measures are implemented to close the findings detected by penetration testing.
- VA/PT findings and follow up actions should be closely monitored by senior management as well as Information Security/ IT audit team.
- The Company should periodically & actively participate in external cyber drills.

Incident Response arid Cyber Crisis Management

- Company should adhere to incident response procedures to respond consistently to attacks, minimize all loss, leakage or disruption during an attack.
- Learning's from information security incidents should be documented and communicated to stakeholders. This information shall be used in improving the processes and systems to reduce recurrence and/or future impact of the security incident.
- Employees and third parties shall report any observed or suspected information security weaknesses in systems or services through proper communication channels.
- Company should develop recovery strategies to ensure critical application systems are resumed within the agreed Recovery Time Objectives (RTO).
- Management responsibilities should be assigned to ensure a quick, effective, and orderly response to information and cyber security incidents.

6. Compliance

All the users, including employees, staff, contractors, third parties and other agents who have access to Company's information and/ or information assets should comply with this policy. Periodic changes to this policy should be updated on the Company HRMS and users should be notified in this regard by an alert mail from the Information Security Department.

- Any violation of the clauses of this Policy should be considered as an act constituting misconduct and should be treated accordingly.
- Disciplinary action should be taken as per the HR Policy

7. Policy Review

This policy (including all sub-policies and provisions) shall be reviewed at the time of any major change(s) in the existing business environment affecting policies and procedures or at least once every year, whichever is earlier. This document shall be reviewed by the CIO and approved by the by Board and IT Strategy Committee.