Cybersecurity and Data Privacy Policy

CONTENTS

Document Change Log

Version	Description	Updated on	Reviewed by	Reviewed by	Approved by
V3	Data Privacy Policy	04-Dec-2024	AGM-IT	General Manager (SAP)	Senior Vice President (F&A)
V4	Data Privacy and Cyber Security Policy	31st January, 2025	IT Head	Chitra Menon	Chitra Menon

1. PURPOSE

To protect personal, sensitive, and confidential data handled by the organization and ensure compliance with data protection laws, and policy for access to internet for users.

2. SCOPE

Applies to all employees, vendors, and third parties who access or manage data through company IT systems.

3. POLICY

3.1. Data Collection and Consent

- Collect only the data necessary for business operations.
- Obtain explicit consent where required.

3.2. Data Access and Control

- Implement role-based access controls (RBAC).
- Access to personal or sensitive data must be logged and monitored.
- Users must not share credentials or unauthorized access.

3.3. Data Storage and Protection

- Store data only in secure, approved systems.
- Use encryption, firewalls, and endpoint protection for security.
- Perform regular backups and secure them appropriately.

3.4. Data Sharing and Third Parties

- Share data only with authorized internal teams or approved vendors.
- Execute NDAs or data processing agreements with third parties.

3.5. Data Retention and Disposal

- Retain data only as long as necessary.
- Securely delete or anonymize data after the retention period expires.

3.6. Data Breach Response

- Any suspected or actual data breach must be reported immediately to IT Security.
- The breach response plan must be activated within 24 hours.

3.7. User Responsibilities

- Employees must complete mandatory privacy training annually.
- Unauthorized access, disclosure, or misuse of data may lead to disciplinary or legal action.

3.8. Compliance

- The organization is committed to complying with all applicable data protection laws (e.g., GDPR, DPDP Act 2023). Regular audits will be conducted to ensure adherence.

Internet access will be allowed to all domain users of BPTP. All personal mailing sites like Gmail/yahoo mail, Social media like twitter/ Facebook and unrequired sites will be blocked by default. These web sites will be allowed if officially required.

IT will ensure that none of the business sites are being affected because of blocking of these sites.

Internet access policy have been created for above-mentioned sites, either these sites will be accessible or not accessible.

3.9. AVP and above Internet Policy

- It will have extra internet access and rest all other users will have default access. Internet access can be provided or modify as per the company's requirement.

3.10. WhatsApp and Webmail Access Policy

- If any user requires special internet browsing access or WhatsApp access, they must obtain Management approval.

3.11. Shopping Access Policy

- Online shopping internet sites will be provided to purchasing and other users whom are involved in purchasing or comparing prices.

3.12. Guest Access Internet Policy:-

- Provision will be there for wireless (Wifi) users and request to give Wifi access to be generated by BPTP employee (Sponsoring Employee) through email only with start & end date for which the access will be live. In the case of start and end date, time is not mentioned the access will be generated for same day only.

3.13. Permitted Use of Internet and BPTP Network

- The Network is the property of BPTP Limited and is to be used for legitimate business purposes. Users are provided access to the computer network and the internet to assist them in the performance of their jobs. All Users have a responsibility to use BPTP network and the internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet may result in disciplinary action.

3.14. Prohibited Activities

- BPTP's computer network will not be used to disseminate, view or store commercial or personal advertisements, solicitations, sexual content, promotions, destructive code (e.g., viruses, Trojan horse programs, etc.) or any other unauthorized materials. Further, at all times users are responsible for the

professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.

3.15. Illegal Copying:

- Users should not illegally copy material protected under copyright law or make that material available to others for copying. Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. Users should not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the respective HOD.

3.16. Communication of Trade Secrets:

- Unless expressly authorized to do so, users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to BPTP. Unauthorized dissemination of such material may result in severe disciplinary action.

Usage of BPTP Computer Resources

3.17. Accessing the Internet

- To ensure security, avoid the spread of viruses & malware, and to maintain BPTP's Internet Usage Policies or Acceptable Use Policies, employees may only access the Internet through a computer attached to BPTP's network and approved Internet firewall or another security device(s).

3.18. Frivolous use

- Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups or other social media, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

3.19. Virus Detection

- Files obtained from sources outside BPTP, including disks/USB drives brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to an e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage BPTP's

computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks/USB drives from non-Company sources, without first scanning the material with Company-approved virus checking software. If the user suspects that a virus has been introduced into BPTP's network, the user shall notify IT department immediately.

3.20. No Expectation of Privacy

- Employees are given computers and internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, post, send or receive using the BPTP's computer equipment. The computer network is the property of BPTP Limited and may be used only for Company purposes.

3.21. Monitoring of computer and Internet usage

- BPTP Limited has the right to monitor and logs and archive any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat, and newsgroups, monitoring file downloads, and all communications sent and received by users via Email, IM & Chat & Social Networking.

4. GOVERNANCE AND REVIEW

- **Policy Owner:** IT and Legal/Compliance Teams
- **Review:** Management shall review this policy periodically and the amendments required, if any, shall be made and communicated accordingly.

5. APPROVING AUTHORITY

- **Approved by:** IT Head

  Chitra Menon

- **Effective Date: 31st January 2025**

6. APPENDIX

Definitions

Term	Definition
BRSR	India's mandatory ESG disclosure framework aligned with SEBI guidelines for sustainability reporting.

Term	Definition
CERT-In	Indian Computer Emergency Response Team, the nodal agency for responding to cybersecurity threats.
Confidential Information	Any non-public information, proprietary data, trade secrets, and business operations details.
Consent	Freely given, specific, informed agreement to process personal data.
Cybersecurity	The practice of protecting systems, networks, and programs from digital attacks.
Data Breach	Unauthorized access, disclosure, alteration, or destruction of data.
Data Subject	An individual whose personal data is collected or processed.
Designated Persons	Employees and insiders identified under SEBI regulations for compliance with insider trading norms.
DPDP Act	The Digital Personal Data Protection Act, 2023 (India).
ESG	Environmental, Social, and Governance, a set of standards measuring a company's impact and ethical behaviour.
GRESB	A global ESG benchmark assessing environmental, social, and governance performance of real estate assets, including standing and development projects.
IT Act	The Information Technology Act, 2000, and its rules, which govern electronic data and cybersecurity in India.
Personal Data	Information relating to an identified or identifiable individual, including name, contact details, etc.
POSH Act	The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013.
SEBI	Securities and Exchange Board of India.
Sensitive Personal Data	Includes financial data, health information, biometric data, etc., as defined by Indian law.
UPSI	Unpublished Price Sensitive Information, information that could materially affect the stock price of the Company if made public.