Electronic Payments and Services Pvt. Ltd

POLICY MANUAL

Version 3.1

DECEMBER - 2022

Contents

SECTION- 1

I. Corporate Vision

To be a leader in providing Technology Solution for Retail Banking and Payment system space by building a strong bond with our customers, our stakeholders and our employees.

II. Corporate Philosophy

1. Managerial Ethics: Our Business ethics are based on integrity and commitment towards achieving organization goals. Our code of ethics is enshrined in the values of good Humanity and Governance.

2. Leadership: Will encourage and foster leadership with a vision to focus on leveraging opportunities and meeting challenges.

3. Customer satisfaction: The Company is committed to benchmark our success with customer satisfaction by attaining, delivering and maintaining the highest standards of Quality and Cost-effective services.

4. Passion for excellence: The Company shall strive for excellence with passion in all its business with focused approach.

5. Concern for environment: The Company is committed to preserve and protect the country's ecological environment and heritage.

SECTION- 2

I. Code of Conduct

The EPS Code of Conduct outlines four key elements that guide professional activities, decisions, and procedures within EPS: integrity, transparency, respect and professionalism.

The EPS Code of Conduct contributes to the welfare of all EPS's stakeholders like clients, employees, shareholders, partners and others with whom we do business, as well as the communities and environments in which EPS operates.

The EPS Code of Conduct serves as an umbrella for several policies and procedures within EPS, which form an integral part of the Code.

All EPS employees receive the Code of Conduct when they start at EPS as a part of the Personnel Guide during the Induction Process. The Management Board will review the EPS Code of Conduct on a regular basis and execute necessary changes as per the compliance and regulations. The Code of Conduct and related policies are also available on EPS's website – www.electronicpay.in

EPS expects employees to:

1. Be aware and behave according to the Code of Conduct and policies in the Personnel Guide.
2. Set an example for others; and
3. Speak out when they feel that the business principles are threatened or compromised.

Situations may occur that have not been foreseen in the existing policies or procedures. If this occurs, each employee will have to find the best manner of acting, based on own insights and estimation of the situation.

If an employee requires advice on the application of the Code of Conduct, he/she can contact the AVP-HR & Head-Risk & Governance Team

Please find below a further explanation of the key elements of the Code of Conduct and (most of) the related policies.

Every employee is the brand ambassador of the Company and custodian of the Company values

The Core Values of EPS lie in the word "STRIVE"and everything that EPS does is guided by these core values:

S-Service

T-Trust

R-Relationship

I-Integrity

V-Value People

E-Excellence

A. INTEGRITY

Integrity is essential to everything we do at EPS. In this way we will uphold the reputation of EPS and indirectly of the banking sector in general. EPS expects employees to fulfil their role with integrity and care and carefully consider the interests of clients, colleagues and all our other stakeholders.

General Guidelines on Integrity

The general rules on integrity for EPS employees expect that they:

- Comply with the (local) laws and never allow a customer/s or colleague to disrupt the law and regulations.
- Refrain from doing business with persons, companies or institutions if such business is related to activities that are prohibited or can be considered unethical.
- Report (suspicion of) fraud or Anti-Money Laundering or other dishonest behavior immediately.
- Be Committed, Honest , Disciplined and Resilient

Confidentiality

We expect employees to treat all information, which is not intended to be disclosed for business reasons, as confidential. Examples of this are client information, commercial information, financial information, and personal information.

The employee is at any time and any place expected to act with care in handling digital and hard copy information and in the use of private computers. Especially if information is used outside EPS office the employee is responsible for maintaining the confidentiality and accuracy of the data.

With regard to guide for social media usage at EPS, a social media policy is in place. Information published via social media about EPS affects our public image and can have consequences for our business as well as our clients and stakeholders.

Internal policy on Information Handling and the Use of email, intranet and social media are available for employees on SharePoint

Insider Trading Policy

This policy shall be applicable to all insiders of the company, including the Directors, Promoters and employees of the company, EPS expects its employees must keep all information and secrets that relate to EPS's present and future business operations strictly confidential. It is prohibited to misuse or disclose to any third party any information about EPS's business operations or information about specific projects.

Anti-Bribery and Corruption

Bribery in any form or kind is prohibited by EPS. Employees are not allowed to either accept or ask for any personal benefits or payments that are not accounted for, nor offer such benefits or payments themself. Any contacts that might lead to or could create an appearance of a mixing of business interests with private interests should be always avoided.

Business Gifts

In contact with business relations the employee should remain independent and honest. For that reason, employees are not allowed to receive or give (business) gifts or favors from or to third parties because of their role or position within EPS, if this could create an appearance of unwanted influence. Gifts or similar benefits may only be offered to, or accepted from, a third party if they are modest in value and if they are consistent with reasonable hospitality given in the ordinary course of business.

Safeguarding Corporate Assets

Safeguarding EPS assets, both tangible and intangible (such as intellectual property rights) is vital to the success of EPS's goals and objectives. Employees have a duty to use EPS's assets only for legitimate business purposes and to protect them from loss or unauthorized use. Under no circumstances may EPS's assets be used for unlawful or improper purposes.

B. TRANSPARENCY

EPS attaches much value to transparent and open communication with all its stakeholders, employees, clients, partners and shareholders and society. Therefore, we ask employees to act transparently and to be open, of course considering the confidentiality of business information.

Outside Positions

To avoid any potential conflict of interest or reputational issue, employees are not allowed to accept and execute any paid outside positions without prior permission of management. The same applies for any unpaid activity in which EPS may be involved in any form or in an activity that might harm the interests or reputation of EPS. Exceptions can only be allowed after prior approval from the Managing Director and President HR and Administration.

Personal Relationships at Work

EPS recognizes that personal relationships may exist or develop between employees. However, where personal relationships exist or develop, we ask our employees to disclose the relationship to management as soon as possible. Open communication and transparency are very important.

Career Moves to Partners or Clients

In general EPS supports but does not actively stimulate potential career moves of its employees towards clients or partners. Due to the potential conflict of interest during the orientation and transition period towards the future employer, such a process should be as transparent as possible.

The employee is expected to notify his manager immediately when entering a discussion with a client or partner of EPS, suggesting prospective employment or the willingness to consider a potential offer. The following step is that management will disengage the employee from any on-going business with that client or partner, in order to prevent any situation of possible conflict of interest.

To safeguard both EPS and the employee from reputational damage occurring from such situation of conflict of interest, be it real or presumed, the period between the initial notification and the actual starting date of a new employment shall be equal to or more than such employee's notice period under employment documents. By a special written approval of the respective Head of Department and President – HR and Administration, an exception can be made to shorten the notice period.

Conflict of Interest

To operate in a fair and open manner, it is important that every employee of EPS shall avoid any situation or interest which might interfere with their judgment concerning their responsibilities to EPS and its clientele.

Should such a conflict of interest arise, it must be reported immediately by the person subject to the conflict to AVP-HR and the Head-Risk & Governance

team

C. **RESPECT**

EPS values differences and is committed to maintain a work environment that is respectful of each other's differences. We expect our employees to treat their colleagues, customers, suppliers or other stakeholders with dignity and respect.

EPS supports and respects the principles set out in the Universal Declaration of Human Rights - and serves as guiding principles within EPS and the integration into all its business engagements.

EPS is an advocate of equal opportunities and will not tolerate unlawful discrimination, harassment or bullying. Discrimination means unequal treatment because of race, sex, disability, religion, or sexual orientation.

Non-Discrimination and Equal Opportunities

EPS tries actively to achieve a truly diverse workforce (e.g., on gender, nationality, and age) within every department. EPS treats its employees in a manner that does not discriminate with regard to gender, nationality, religion, race, age, disability, sexual orientation, political opinion, or ethnic origin.

EPS promotes the ideal that all employees shall be treated with equal respect and dignity.

EPS does not engage child labor nor other forms of compulsory or forced labor, in conformity with prevailing Labour Laws and Rules notified by State and Central Government.

.

Undesirable Behavior or Communication-Details are incorporated in the policy manual.

EPS follows a strict procedure for complaints on undesirable behavior / communication involving sexual harassment, violence/aggression and bullying. A safe and healthy working environment shall be provided for all employees.

Any act of violence or threats to any employees are never acceptable at EPS and must be reported to the AVP-HR immediately, as soon as such situations should occur. Non-adherence of the Code of Conduct or Law shall be treated as serious disobedience by the Company and adherence of employees in reporting any violent, unethical, or illegal acts in a timely manner is essential.

To maintain high standards of professional behaviour and promote transparent structure and effective communication EPS has implemented the **Whistle Blower** and **Prevention of Sexual Harassment of Women at Workplace** Policies in the organisation. The Policies are aimed at providing guidance and protection with regards to raising concerns or complaints of any untoward incident or violation. **Above referred policies** are applicable not only to all employee of EPS but also includes vendors' employees, service providers and customers interacting with EPS.

- **Whistle Blower Policy**

In order to ensure ethical behaviour; the Company considers it proper to provide for a channel to its various stakeholders, which will ensure prompt reporting of any untoward event of concern without any fear. Keeping in view, the Company has implemented the "Whistle Blower Policy".

Examples of activities expected to be reported under Whistle Blower Policy are as following - Fraud, Breach of Confidentiality, Kickbacks, Bribery, Falsification or Manipulation of Expenses, Violation of ethical Code of Conduct, Discrimination, Harassment, Failure to comply with legal and regulatory obligations or any act which leads to unethical business practices.

Reporting of any untoward act or similar concern, shall be addressed to below mentioned Company's Vigilance Officer (Whistle blower) through Email or written communication on the below:

Mr. Mani Mamallan
Chairman and Managing Director
mdoffice@electronicpay.in

All complaints addressed to Vigilance Officer shall be handled in complete confidential manner and complainant will not be disclosed during and after the investigation process.

- **Prevention of Sexual Harassment of Women at Workplace**

Keeping in line with EPS' commitment to provide a safe and conducive work environment to all its employees, it is imperative to prevent and eliminate all forms of sexual harassments at the workplace.

The policy is formulated in pursuance of the Vishakha Guidelines, 1997 as set of guidelines promulgated by the Supreme Court in 1997, letter superseded as the Sexual Harassment of Women at Workplace (Prevention, Prohibition &Redressal) Act, 2013. In furtherance to the policy, the Company has duly have constituted an Internal Committee chaired by VP-Corporate Affairs.(IC)

In case of a concern, the aggrieved person can report or raise complaint to the committee or any of the committee member in writing.

For raising complaints through emails, complaints can be mailed to ic@electronicpay.in (All complaints and concerns addressed to IC shall be dealt with in strict confidence.)

All Forms of Sexual Harassment Prohibited-

Company does not tolerate sexual harassment, a form of unlawful discrimination. Any act, Incident or attempt of unwelcome sexual advances, requests for sexual favors and other verbal or physical conduct or gesture of a sexual nature shall amount to constitute sexual harassment, when:

- Submission to such conduct is made, explicitly or implicitly, as a condition of an individual's employment or advancement.
- Refusal to accept such conduct is used as a ground for employment decisions adversely affecting such individual; or

- Such unreasonable conduct interferes with an individual's work performance or creates an intimidating, hostile, or offensive working environment.

Do's

- It is the duty of the employees to keep the Company informed about any consensual relationship at workplace, which may result in conflict of interest while discharging official duties by them.
- All employees shall behave professionally towards each other at all times, includes, during subsistence of a consensual relationship or there after
- The employees at all times shall respect all persons' dignity and shall refrain from engaging into any unprofessional or inappropriate behavior and shall not engage in any other conduct towards any person that could violate the Sexual Harassment of Women at Workplace policy

  The Company shall not be held responsible at any time, for any unacceptable behavior, unruly or untoward behavior by any of the employees ,irrespective whether such employees are observed or informed to be in a consensual relationship.

D. PROFESSIONALISM

EPS provides its clients and partners with high-quality products, services, and knowledge. EPS strives to keep the quality at a high level and to offer all services in an efficient, responsible, and sustainable manner.

EPS promotes and develops rigorous ethical and professional standards to encourage and build on best industry practices. EPS strives to provide a solid

foundation on which the banking industry can build the human capital on which the sustainable, customer-driven banking industry we all wish to see is based. Over time, this will support a strong culture of ethical and professional development across our industry.

General Guidelines on Professional Behavior

In line with the Code of Conduct, employees are expected to:

- Perform their duties with objectivity and professional care.
- Serve in the interest of all stakeholders in a lawful manner.
- Gain and maintain appropriate knowledge, skills and competences in their fields of expertise.
- Undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge, and competences; and
- Support the professional knowledge of colleagues, clients, and partners in enhancing their understanding whenever necessary or appropriate.

Safety

Employees should carefully follow all necessary safety measure within EPS and during business trips.

***EPS attaches great value to compliance with the Code of Conduct. Disciplinary measures will be taken against those persons who are responsible for any violation of the Code of Conduct.

DISCLOSURE OF EMPLOYMENT OF IMMEDIATE FAMILY MEMBER

1. Each employee of **Electronic Payment and Services Private Limited** is required to disclose information of any immediate or distant relative working in the Organization. With a view to keep the company informed/ updated regarding details of any immediate /

distant relative, each employee shall complete this form and submit to HR Department from time to time.

2. For the purpose of clarity, Relative would mean and include wife or husband, son or daughter, parents, siblings, or any other person related to any of them by blood or marriage irrespective of whether they are dependents or not.

   Having read and understood the above, I confirm that: (select only one of the following options)

   Is any of your relative(s) [immediate or distant] working in the

   same organization:

   No

   YES

   If Yes, please provide below details of related employee: -

   Name(s): _____

   Nature of relationship: _____

   Location of work: _____

   Department(s): _____

   Date of Joining: _____

3. In addition to above, I further confirm below: -

   A. That I am not a Politically Exposed Person (PEP). **No**

B. I am a Politically Exposed Person **YES**

If yes,

Details of Political exposure to be provided: _____

4. I understand and I am aware of Anti Money Laundering Policy (AML policy) applicable to employees of the Company and further confirm that I shall adhered to, the AML Policy at all times during my employment.

5. I understand and I am aware of Information and Technology Policy (IT policy) applicable to employees of the Company and further confirm that I shall adhere to the IT policy at all times during my employment.

Name (in blocks): _____

Employee Id: _____

Signature: _____

Date: _____

The following declaration is a moral and ethical conduct declaration in the EPS Code of Conduct, and it acts as a guideline for the actions of all of EPS's employees:

Declaration:

"I declare that I will perform my duties at EPS with integrity and care.

- I will carefully consider all the interests involved in the company, i.e. those of the clients, the shareholders, the employees and the society in

which the company operates.

- I will give paramount importance to the client's interests and inform the client to the best of my ability.
- I will comply with the laws, regulations and code of conduct applicable to me at EPS.
- I will observe secrecy, confidentiality in respect of matters entrusted to me.
- I will not abuse any knowledge gained at EPS and its clientele. I will act in an open and assessable manner and I know my responsibility towards society.
- I will endeavor to maintain and promote confidence in the ATM & Payments, Banking and Retail sector.

In this way, I will uphold the reputation of EPS.

Employee Name: Employee ID:

Employee Signature: Date:

Declaration:

"I declare that I will perform my duties at EPS with integrity and care.

- I will carefully consider all the interests involved in the company, i.e., those of the Clients, the Shareholders, the Employees, and the society in which the company operates.
- I will give paramount importance to the client's interests and inform the client to the best of my ability.
- I will comply with the laws, regulations, and code of conduct applicable to me at EPS.
- I will observe secrecy in respect of matters entrusted to me.
- I will not abuse any knowledge gained at EPS and its clientele. I will act in an open and assessable manner and I know my responsibility towards society.
- I will endeavor to maintain and promote confidence in the ATM &

Payments, Banking and Retail sector.

In this way, I will uphold the reputation of EPS.

Employee Name: Employee Code:

Employee Signature: Date:

II. Anti- Bribery Policy

1. Purpose

- Electronic Payment and Services Private Limited (the "Company") has adopted an Anti-Bribery and Corruption Policy (the "Policy").
- The purpose of this Policy is to safeguard and promote legitimate business throughout the organization and to prevent and prohibit corruption, bribery, and similar acts in connection with the organization. This document sets out the processes and procedures to be followed to be in adherence to the Anti-Bribery and Corruption Policy of the Company

2. Compliance Officer

The Company has designated Mr. B. R. Nath as the Anti-Bribery and Anti Corruption Compliance Officer ("Compliance Officer")

3. Communication

The Company will communicate the Policy and its approach for the implementation of the Policy to its employees and vendors.

4. **Responsibility of Employee**

- Gifts or Favors: - Policy is applicable to all gifts and hospitalities which may be received from, or offered to, any customers, suppliers, and other business contacts of the Company. No employee shall accept small gifts of impersonal items, favors or hospitality and gifts of a promotional nature from any existing or potential customers or suppliers. No gifts shall be accepted by any employee, however under any exceptional cases, if gift amounting maximum up to INR 2500/- is accepted by an employee, the same shall be approved by his/her reporting manager in advance. In case any employee accepts Gift exceeding aforesaid amount of INR 2500/- from any of customer, suppliers, and other business contracts of the Company, then such deviation shall be duly informed to the management of the Company. The reporting manager shall immediately report any approvals granted towards acceptance of Gifts or Favor by any of his/ her team members, to the Compliance Officer for information and record purposes. Employees shall not accept gifts that, by their nature have the potential to cause reputational damage or embarrassment to the Company. These shall include any gifts in form of cash, cash convertible gifts or any payment, favor or inducement that might improperly influence an official transaction.

- Bribery: - The Company or its employees (in matters related to their engagement with the Company) shall not pay and shall not accept bribes, either directly or via third parties, in any circumstance. Breach or attempted breach of this principle by an employee shall be regarded as an act of gross misconduct. Employees shall never offer or accept any bribe or inducement, which may influence or appear to influence their actions. No employee shall misuse his or her position within the Company or the information he or she gathers during the course of his or her official duties to further his or her private interests or those of anyone else. In case of doubt of what constitutes a bribe or an instance of corruption, employees shall seek necessary guidance from their reporting manager or the Compliance Officer.

- Facilitation Payments: - Payment of 'Speed Money' or 'Fast Money' to expedite or 'facilitate' either routine or non-routine matters is against the values of the Company. This shall include any payment made to an external party in relation to a matter or issue to facilitate a favorable outcome in a business.

- Dealing: - If an employee is aware of any such transaction, he or she shall bring it to the notice of the Compliance Officer immediately.

5. Reporting and Compliance

- Any complaint, suspicion, or concern of any employee ("Reporter") that arises on the discovery of any corrupt practice or bribery or similar malpractice shall be raised to the Compliance Officer immediately. Such reporting to the Compliance Officer shall be obligatory for and binding on all employees, whether the act in question has occurred in the past or is about to occur in the future.

- The Compliance Officer may order further investigation on the matter and take any actions necessary to facilitate speedy and accurate investigation.

- Any serious instances of corruption or bribery or similar acts shall be liable to be probed and be subjected to appropriate disciplinary action. If the said act amounts to a serious offence then the Company shall have discretionary powers to take appropriate steps, including registering a complaint with the appropriate regulatory or legal authority depending upon the intensity and nature of the act.

- Due care and caution shall be exercised in case of any transactions under probe that are being entered into by the Reporter himself or herself.

- Whistleblowing: - No employee shall suffer demotion, penalty, or other adverse consequence for refusing to pay or accept a bribe even if such a

refusal has resulted or may result in an unfavorable business outcome for the Company. The Company regards the reporting of any instance of bribery or attempted bribery as a legitimate example of 'whistle blowing' and affirms that no employee shall suffer demotion, penalty, or any other adverse consequence for such reporting. Employees shall be kept informed of the Whistle blower Policy and their responsibilities under the same.

6. Third Party Vendors

The Company requires screening procedures to be carried out on those of its suppliers, agents, advisers, contractors, intermediaries, and other representatives who supply material goods and services to it ("Third Party Vendors", or TPVs) to protect the Company from the risk of it being associated with illegal or corrupt payments (or of payments purportedly being made on its behalf) and to ensure that the highest ethical standards are maintained. No TPV can enter into an agreement with any external party on behalf of the Company, unless formally agreed otherwise. Any instance of a TPV an employee of a TPV being asked to act as a principal for the Company for any dealing shall be considered as a misconduct and call for disciplinary action. The Company requires that TPVs are made aware of its Anti-Bribery and Corruption Principles.

7. Responsibility of Reporting Manager or Head of Business Unit or Head of Department ("Managers")

Employees who are reporting managers of any other employees ("Managers") have additional primary responsibility to assess the risk of bribery and corruption occurring and to implement appropriate preventative measures. They shall continuously monitor gifts and entertainments received or given by the employees and ensure compliance with this Policy. They may take support from the Compliance Officer or other Managers, on tracking all identified risks, identifying their mitigating measures, and on the implementation and supervision of this Policy in general, thereby, maintaining high standards of internal control and risk containment measures.

8. Training and awareness

An ongoing employee awareness programmes are a key enabler to convey awareness of this Policy, relevant legislations, employee obligations and expectations. Awareness is developed through periodic training and frequent communications. The Human Resources Department shall design requisite awareness programmes to ensure adequate understanding of the Policy amongst employees.

9. Governance Framework

- The Compliance Officer shall have the responsibility of implementation, monitoring and reviewing the Anti-Bribery and Corruption Policy and placing the same to the Board of Directors annually for review and any required amendments.

- The Compliance Officer shall have the responsibility to review reports of bribery or corruption received and refer relevant matters for inquiry or investigation, as appropriate, in consultation with the top management, or the process laid in this regard, and for further reporting to regulatory authorities, as may be required and for further attendant actions.

- The Compliance Officer shall conduct incisive scrutiny of reports received by him or her from various Managers and identify potential bribery or corruption risks.

- The Compliance Officer shall also ensure that the audit functions of the Company, including concurrent audits are designed to expose bribery or corruption prone areas.

- Periodic review of the whistle blower guidelines shall be undertaken in order to promote the culture of openness in the Company and to enable employees to disclose improper practices and suspicious actions to the management.

10. Governance Framework – Review and Reporting

- **Information to Senior Management**

The Compliance Officer will keep the senior management of the Company informed of the steps taken to implement the Principles and Procedures of this Policy, and of the conclusions of any reviews and of any material findings arising out of the work of implementation of this Policy.

- **Review**

The Compliance Officer will monitor, review and report to the Board of Directors on the effectiveness of and adherence to the Policy, its Principles, Procedures and the steps taken by the Company to implement them.

- **Reporting**

Where relevant, the Agenda for the Board Meetings of shall include a report on the workings and effectiveness of this Policy including the number of reports of bribery and corruption received and a summary of investigations conducted. The Compliance Officer shall convey the directions and guidance given by the Board of Directors to the employees of the Company and other functional departments for carrying out necessary actions, and obtain action taken reports from them and place them for the information of the Board of Directors.

11. Authority to change and amend Process and Procedure.

The policy will be reviewed on a 2-yearly basis. If there is a change in the business environment, it will be reviewed as and when required.

The Compliance Officer shall communicate any changes in process and procedure in the implementation of the Anti-Bribery and Corruption Policy.

III. Anti-Money Laundering Policy

Electronic Payment and Services Private Limited embraces the highest standards of honesty, ethics, and integrity as core business values, and will do business only in lawful and ethical ways. The Company is subject to the Prevention of Money Laundering Act 2002 ("PMLA"), or as relevant, to various international anti-money laundering laws.

It is the policy of the Company to avoid money laundering and any activity that facilitates money laundering or the funding of terrorists or criminal activity.

Money Laundering is the process by which illegal funds and assets are converted into legitimate funds and assets. Money laundering is being employed by launderers worldwide to conceal criminal activity associated with it such as drugs or arms trafficking, terrorism and extortion. All crimes that produce a financial benefit give rise to money laundering. Generally, money laundering occurs in three stages:

- Placement: Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

- Layering: Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

- Integration: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

The integrity of the capital marketplace depends heavily on the perception that it functions within a framework of high legal, professional, and ethical standards.

1. Objectives

The objectives of this policy are:

- To have a proper due diligence process before engaging with various service providers, consultants, vendors, investors at the time of accepting investment in the Company (collectively known as "Business and Investment Entities").
- To monitor and report suspicious transactions.
- To discourage and identify money laundering or terrorist financing activities.
- To take adequate and appropriate measures to follow the spirit of the PMLA.
- To develop employee awareness and vigilance to guard against money laundering and terrorist financing.

2. The Program

The objective of having an AML or CFT Program is to have in place adequate policy, practice and procedure that help to prevent money-laundering activities. Such procedures would include the following:

1. Appointment of Compliance Officer.
2. Due Diligence, including:
   a. Acceptance and Identification
   b. Categorization
3. Transaction monitoring to identify and Report Suspicious Transactions (STR)
4. Record keeping and retention of records

5. Internal Control Measures

6. Co-operating with law enforcement agencies in their efforts to trace the money laundering transactions and persons involved in such activities

7. Clear communication to the employees to ensure strict adherence to due diligence requirements

1. AML or CFT Compliance Officer Designation and Duties

As required under the Prevention of Money Laundering Act 2002, the Company has designated Mr. B. R. Nath as the AML or CFT Compliance Officer. The Compliance Officer will ensure that:

- This AML or CFT Policy is implemented effectively by the Company
- The identification and assessment of potentially suspicious transactions are done on a regular basis.
- The Company regularly updates changes or additions to the AML or CFT provisions as necessary.
- Coordinate AML or CFT training for appropriate personnel as required and advise employees to report any suspicious transactions to the concerned parties in a timely manner.
- Seek approval from the Board of Directors in deciding whether to establish relationship with Business and Investment Entities, where money laundering risks are perceived.
- Evaluate, in consultation with others, whether to delegate portions of AML compliance to third parties.
- The Company responds promptly to any request for information, including KYC related information, made by the regulators, statutory authorities, and investors of the Company.

Reliance on Third Parties

While evaluating whether to delegate portions of AML compliance to third parties: -

1. The Company shall obtain the necessary information to establish
   - Identity of the third party
   - Identity of the ultimate beneficial owner in case the third party is not an individual
2. Copies of the documentary evidence should be made available to the Company upon request.
3. The Company shall ensure that the third party is a regulated or supervised entity and has similar KYC compliance measures in place.

2. Due Diligence

a. Acceptance and Identification

Considering the potential risks posed by a money launderer, it is essential to make reasonable efforts to determine the true identity of Business and Investment Entities. For Business and Investment Entities with whom the aggregate transaction value in a single financial year is above INR 1 Crore Only.

- All KYC documentation must be completed before signing any firm documentation for a new business or investment relationship.
- Any discrepancies, anomalies or non-compliance issues must be mentioned.
- At the time of due diligence and KYC documentation, in spite of appropriate measures or KYC policies, if
  - information provided is suspected to be non-genuine, or

- There is perceived non-cooperation in providing the information, decision-making authorities within the Company will be appropriately informed and the Company will not move ahead with further process.

The submission of all documents required under this policy is a pre-requisite.

- In respect of cross border correspondent banking, the Company shall additionally
- gather sufficient information about the correspondent or respondent bank to understand fully the nature of its business and to determine, from publicly available information, its reputation, and the quality of supervision.
- if necessary, seek information whether it has been subjected to a money laundering or terrorist financing investigation or regulatory action.
- obtain approval from the Board of Directors before establishing new correspondent relationships where money laundering risks are perceived.
- clearly understand the respective responsibilities of each institution
- The Company shall not engage or continue correspondent banking relationship with a Shell Bank i.e., a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group. The Company shall not keep anonymous accounts or accounts created in obviously fictitious names.

- Beneficial Owner: -

A. Where the client is a person other than an individual or trust, i.e., company, partnerships or unincorporated association or body of individuals, the beneficial owner is identified as follows.

1. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest i.e., ownership of or entitlement to:

a) More than 25% of shares or capital or profits of the juridical person, where the juridical person is a company.

b) More than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

c) More than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

2. In cases where there exists doubt as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means such as through voting rights, agreement, arrangements or in any other manner.

3. Where no natural person is identified under above clauses, the identity of the relevant natural person who holds the position of senior managing official.

B. Where the client is a trust, beneficial owners of the client are identified and reasonable measures are taken to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

C. Where the client or the owner of the controlling interest is a company listed on a stock exchange or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

D. Procedures include identifying the natural persons with a controlling interest and identifying the natural persons who comprise the mind and

management of the legal person or arrangement. Where the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements, the relevant information or data may be obtained from a public register, from the customer or from other reliable sources.

- Politically Exposed Persons ("PEP"): PEPs are individuals who are or have been entrusted with prominent public functions, e.g., heads of states or of governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations, important political party officials, etc.

- The Company has put in place necessary procedures to determine whether their existing or potential promoters or directors of Business and Investment Entities is or are a PEP.

- Such procedures include seeking additional information from clients, accessing publicly available information etc.

- The Company takes reasonable measures to establish the source of wealth and the source of funds of PEPs.

  ✓ The source of wealth refers to the origin of the PEP's total assets. This information will usually give an indication as to the volume of wealth the PEP would be expected to have, and a picture of how the PEP acquired such wealth. Although the Company may not have specific information about assets not deposited or processed by them, it may be possible to gather general information from commercial databases or other open sources.

  ✓ The Company ensures that the level and type of transactions are consistent with its knowledge of the PEP's source of wealth and source of funds.

  ✓ Deviation of facts regarding the PEP vis-à-vis general understanding may require further assessment of the situation. Outcome of the assessment could include a decision whether to enter into or continue

with the relationship or whether further steps would be necessary, such as termination of the business relationship and filing STRs to the Financial Intelligence Unit ("FIU").

- ✓ Failure to voluntarily disclose information by any PEP is also considered a red flag.

- In case there is a money laundering-through-PEP risk with any of the Business and Investment Entities, a specific approval of the Board is sought with respect to establishing or maintaining the business relationship.

b. Categorization

The Company transacts with Business and Investment Entities based on the risk they are likely to pose. For this purpose, The Company has categorized Business and Investment Entities and they are under low risk and high-risk category based on appropriate Due Diligence and KYC process.

LOW RISK

Low risk entities are those who are likely to pose low or nil risk. Individuals and entities whose identities and sources of wealth can be easily identified, and their bank accounts by and large conform to the known profile may be categorized as low risk. They can include the following:

- Salaried Individuals
- Corporate which have provided financial details as requested by the Company
- Government employees and government owned companies
- Businessman whose identity and source of wealth is easily identified and who complies with necessary KYC disclosures

- Individuals or corporates who do not fall in the above-mentioned points and who provide necessary information as per KYC norms and exhibit transparency

- Individuals or corporates who have been introduced by brokers or branch managers and they have known them personally

HIGH RISK

- High net-worth individuals whose identity and source of wealth is difficult to identify

- Trusts, charities, NGOs, and organizations receiving donations

- Politically Exposed Persons (PEPs)

- Those with dubious reputation as per public information available, etc.

- Clients in high-risk countries as announced by appropriate authority from time to time

List of High-Risk Countries - http://www.fatf-gafi.org to be referred for the latest list of high-risk countries and monitored jurisdictions.

3. Transaction monitoring to identify and report suspicious transaction.

Screening of transactions by the Company includes focusing on the accounts and business transactions of the Business and Investment Entities and holding various discussions with finance or accounts teams regarding transactions and seeking clarifications, if necessary.

Suspicions transaction means a transaction which, to a person acting in good faith -

a) Gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence, regardless of the value involved.

b) Appears to be made in circumstances of unusual or unjustified complexity; or

c) Appears to have no economic rationale or bonafide purpose; or

d) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

Broad categories of reason for suspicion and examples of suspicious transactions are as follows.

a) False identification documents

b) Identification documents which could not be verified within reasonable time

c) Doubt over the real beneficiary of the account

d) Suspicious background or links with known criminals

e) Unusual or unjustified complexity

f) No economic rationale or bonafide purpose

g) Source of funds are doubtful

h) Investment proceeds transferred to a third party

i) Suspicious off market transactions

j) Large sums being transferred from overseas for making payments

Such matters, if dubious, are reported to the Compliance Officer of the Company and a suitable action including decision on reporting to Financial Intelligence Unit - India (FIU-IND) shall be taken in consultation with the Board.

Confidential Reporting of AML or CFT Non-Compliance to Compliance Officer

Employees will report any violations of the firm's AML or CFT compliance program to the AML or CFT Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to an appropriate member of senior management. Such reports will be confidential, and the employee will suffer no retaliation for making them.

Confidential Reporting of Suspicious Transactions ("STR") to FIU-IND

In cases where a money laundering practice is identified that warrants a reporting to FIU-IND, reporting of transactions at account level or transaction level shall be done using the formats prescribed by FIU-IND (http://fiuindia.gov.in). Guidance with respect to Reporting of Suspicious transactions to FIU-IND is included. Furthermore, Employees should be prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report (STR) or related information is being filed with the FIU-IND.

4. Record Keeping and retention of records.

All relevant documents relating to Business and Investment Entities with whom the aggregate transaction value in a single financial year is above INR 1 Crore Only should be maintained for at least for 8 years from the end of the financial year in which the latest transaction with such entities has taken place. The Board may consider revising this provision to maintain all the records for an extended period, if necessary.

5. Internal controls and foreign branches and subsidiaries

The Company has put in place the following:

a. Procedures and checks (including but not limited to having separate maker and checker, payment authority limited to senior personnel, minimum cash impress, periodic physical verification of fixed assets etc.) to ensure that the internal controls and policies, including AML or CFT policy, are operating and effective

b. Background checks and verifications at the time of recruiting new employees.

c. Creating general awareness amongst employees regarding the AML or CFT norms and recent changes

The Company will ensure that foreign branches and majority owned subsidiaries which the Company may have in future are governed by this AML or CFT Policy, as may be amended to be compliant with their country specific requirements.

6. Monitoring of Investment related Transactions

The Company pays special attention to all complex transactions and all unusual patterns which have no apparent economic or visible lawful purpose for making investment in Business and Investment Entities. The Company monitors any debt that is offered by promoters or directors to it and vice versa for any reason that is beyond the obvious.

7. Review of Policy

The aforesaid AML or CFT Policy is reviewed on a 2 yearly basis or as and when required with regard to testing its adequacy to meet the compliance requirements for the Business and Investment Entities. The Compliance Officer is the authority to give directions to undertake additions, changes, modifications etc. as required.

8. Sharing AML or CFT Information with Regulators

The Company will respond to any request from any regulatory body ("Regulator") about accounts or transactions by promptly searching its records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization, to the Regulator. Upon receiving an information request, the Compliance Officer is to be responsible regarding the request and similar requests in the future.

Further, the Company will not disclose the fact that any Regulator has requested or obtained information from it, except to the extent necessary to comply with the information request. The Company will maintain procedures to protect the security and confidentiality of requests from Regulators. It will direct any questions it has about the request to the requesting Regulator.

Unless otherwise stated in the information request, the Company will not be required to treat the information request as continuing in nature.

The Company will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities. The Company will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the firm's other books and records.

How to Raise a Question or Concern

The Company's employees have a responsibility to help detect, prevent, and report instances of money laundering. The Company encourages its employees and anyone doing business on its behalf to raise any questions they may have about this policy or its application to the Company's operations and to report any suspected violations of this policy to appropriate personnel as soon as possible.

If there are questions regarding this policy, or to report a concern, please contact the Compliance Officer, Mr. B. R. Nath via e-mail at br.nath@electronicpay.in

IV. Whistle Blower Policy

1. PREAMBLE

Section 177 (9) of the Companies Act, 2013 requires every listed company and such classes of companies as prescribed by the Companies (Meetings of Board and its Powers) Rules, 2014 ("Rules") to establish a vigil mechanism for the directors and employees to report genuine concerns in such manner as may be prescribed.

Electronic Payment And Services (P) Ltd. ("The Company") had adopted a Code of Conduct for Employees ("The Code"), which lays down the principles and standards that should govern their actions. Any actual or potential violation of the Code, howsoever insignificant or perceived as such, is a matter of serious Protected Disclosure for the Company and should be brought to the attention of the concerned. A vigil mechanism shall provide for adequate safeguards against victimization of persons who can also use such mechanism for reporting genuine concerns including above.

It also makes provision for direct access to Mr. Mani Mamallan, Managing Director of the Company in appropriate or exceptional cases.
Under these circumstances, the Company, being a company which falls within the class of companies required by the Rules to form such policy, proposes to formulate a Whistle Blower Policy or Vigil Mechanism.

The Board of directors have nominated Mr. Mani Mamallan, Managing Director to play the role of audit committee for the purpose of vigil mechanism, to whom other directors and employees may report their concerns.

2. DEFINITIONS

A. "Alleged Wrongful Conduct" shall mean any violation of law, infringement of the Company's rules, misappropriation of monies, actual or suspected fraud, substantial and specific danger to public health and safety or abuse of authority.

B. "Board" means the Board of Directors of the Company.

C. "Code" means the Code of Conduct for Employees adopted by the Company, as defined above.

D. "Employee" means all the present employees and whole time directors of the Company (whether working in India or abroad), including advisors, consultants and contractors.

E. "Protected Disclosure" means a disclosure, made by an employee or group of employees of the Company, through a written communication, in good faith, which discloses or demonstrates information about an unethical or improper activity with respect to or relating to the Company. It should be factual and not speculative or in the nature of an interpretation or conclusion and should contain as much specific information as possible to allow for proper assessment of the nature and extent of the concern.

F. "Policy" means this Whistle Blower Policy.

G. "Subject" means a person or group of persons against or in relation to whom a Protected Disclosure is made or evidence gathered during the course of an investigation.

H. "Vigilance and Ethics Officer" means an officer appointed to maintain records regarding the Protected Disclosure thereof, placing the same before Mr. Mani Mamallan, Managing Director for its disposal and informing the result thereof.

3. OBJECTIVES

- To enable Employees voice concerns in a responsible and effective manner.
- To provide a platform for Employees to disclose information internally, without fear of reprisal or victimization, where such Employee has a reason to believe that the information shows serious malpractice, impropriety, abuse or wrongdoing within the Company.
- To enable disclosure of information, independently of line management (although in relatively minor instances the immediate Superior would be the appropriate person to be informed).
- To ensure that no Employee of the Company feels she or he is at a disadvantage while raising legitimate concerns.
- Provide an opportunity of being heard to the persons involved especially to the Subject.

4. APPLICABILITY

All Employees of the Company. As per the definition of Employee, this would include all the present employees and whole time directors of the Company (whether working in India or abroad), including advisors, consultants and contractors.

5. PROCESS OWNER

The Head of HR will be the process owner for this Policy.

6. DISQUALIFICATIONS

A. While it will be ensured that genuine Whistle Blowers are accorded complete protection from any kind of unfair treatment as herein set out, any abuse of this protection will warrant disciplinary action.

B. Protection under this Policy would not mean protection from disciplinary action arising out of false or bogus allegations made by a Whistle Blower knowing it to be false or bogus or with a mala fide intention.

C. Whistle Blowers, who make any Protected Disclosures, which have been subsequently found to be mala fide, frivolous or malicious, shall be liable to be prosecuted under the Code.

7. POLICY and PROCEDURE

Constituents of Malpractice, Impropriety, Abuse or Wrongdoing:
Malpractice, impropriety, abuse and wrongdoing (hereinafter referred to as "Concern") can include a whole variety of issues and some are listed below. However, this is not a comprehensive list but is intended to illustrate the sort of issues, which may be raised under this Policy.

- Any unlawful act, whether criminal (e.g. theft) or a breach of the civil law (e.g. slander or libel).
- Breach of the Code or of any Policy or manual or rule adopted by the Company.
- Health and safety risks, including risks to the public as well as other Employees (e.g. faulty electrical equipment).

Fraud and corruption (e.g. to solicit or receive any gift or reward as a bribe).

- Any instance of failure to comply with legal or statutory obligation either for and on behalf of the Company or in any personal capacity in the course of discharging duties of the Company.
- Any instance of financial malpractice of any sort.
- Abuse of power (e.g. sullying or harassment).
- Any other unethical or improper conduct.
- Any actions taken to conceal any of the above.

- Pilferage of confidential or propriety information.
- Wastage or misappropriation of the Company's funds or assets.

8. DISCLOSURE OF THE PROTECTED DISCLOSURE

- It is acceptable for the Employee to discuss her or his Protected Disclosure with a colleague. The Employee may find it more comforting to raise the matter if there are two (or more) Employees who share the same Concerns.
- An Employee intending to make any disclosure of a Protected Disclosure is required to disclose all relevant information.

  The Protected Disclosure should be submitted in a closed and secured envelope and should be super scribed as "Protected Disclosure under the Whistle blower Policy". Alternatively, the same can also be sent through email with the subject "Protected Disclosure under the Whistle blower Policy". If the Protected Disclosure is not super scribed and closed as mentioned above, it will not be possible for the Vigilance and Ethics Officer to protect the Whistle Blower and the Protected Disclosure will be dealt with as if a normal disclosure.

- The Vigilance and Ethics Officer and the alternate shall be nominated by the Board.
- The Protected Disclosure shall be disclosed through e-mail or fax to the Director nominated by the Board, Mr. Mani Mamallan. The e-mail address, telephone and fax number details are set out in the Employee Handbook.

9. INVESTIGATION OF THE PROTECTED DISCLOSURE

The Protected Disclosure shall be investigated by the Director nominated by the Board, Mr. Mani Mamallan or Vigilance and Ethics Officer either by himself or through any other person as deemed necessary by the Director so appointed

or Vigilance and Ethics Officer. A copy of the Protected Disclosure disclosed shall be furnished to the Board, in complete confidentiality, for information.

10. DECISION FOR THE PROTECTED DISCLOSURE

A preliminary decision vis-à-vis the Protected Disclosure disclosed at business shall be taken to the Board with a full investigation report by the Director so appointed by Board and Vigilance and Ethics Officer.

11. RULES FOR INVESTIGATION and DECISION BY THE BOARD

The Board in consultation the Management Committee shall frame and circulate such rules as may be deemed necessary to enable a fair conduct of inquiry and investigation as well as decision.

12. PROCEDURE FOR HANDLING PROTECTED DISCLOSURE

Once any Protected Disclosure has been made by an Employee, the Director so appointed by Board and Vigilance and Ethics Officer to whom such disclosure has been made shall pursue the following steps:

- Acknowledge receipt of the Protected Disclosure within 5 working days. The receipt shall set out the details of the Concern.
- Close the matter (where possible) within 60 days.
- Obtain full details and clarifications of the Protected Disclosure.
- Consider the involvement of the Company's Auditors or the Police or any other external investigation agency or person.
- Fully investigate the allegation with the assistance where ever appropriate, of other individuals or bodies.

- Prepare a detailed written report and submit the same to the Board, as the case may be, not later than 30 days from the date of disclosure of Concern.
- Give the Employee as much feedback as it can.
- The Company may not be able to inform the Employee the precise action it takes where this would violate a duty of confidence owed by the Company to someone else.
- The Company will take steps to minimize any difficulties, which the Employee may experience as a result of raising the Concern. Thus, if the Employee is required to give evidence in criminal or disciplinary proceedings the Company will arrange for the Employee to receive advice about the procedure.

13. PROCEDURE TO BE PURSUED BY THE BOARD

- The Board will, based on the findings in the written report submitted by the Vigilance and Ethics Officer and after conducting further investigation as it may deem fit, come to a final decision in the matter (where possible) not later than 30 days from the date of receipt of the written report.
- If the Protected Disclosure is shown to be justified, then the Board shall invoke the disciplinary or other appropriate action against the concerned as per Organization's procedures.
- A copy of the decision in writing shall be sent to the Vigilance and Ethics Officer who shall also place the same before a meeting of the Board held as soon as practicable after the date of such a final decision.

14. APPEAL AGAINST THE DECISION OF THE BOARD

If the Whistle Blower or the person complained against is not satisfied with the decision of the Board, then either of the Parties may appeal against this decision by sending a report to the Board explaining why this is the case. The Protected

Disclosure will be re-investigated, if the Board decides there is good reason to do so.

15. ANONYMOUS ALLEGATIONS

This Policy encourages Employee to put her or his name to any disclosures she or he makes in writing.

In case an anonymous Protected Disclosure carries references to verifiable facts and figures, these would be verified and if found true, the Protected Disclosure will be taken up and investigated. However, it may be difficult for the Director so appointed and Vigilance and Ethics Officer to access full details and make a proper assessment of the Concern.

16. MAINTAINING CONFIDENTIALITY OF THE PROTECTED DISCLOSURE AS WELL AS THE DISCLOSURE

The Employee making the disclosure of Protected Disclosure as well as any of the persons to whom the Protected Disclosure has been disclosed or any of the persons who will be investigating or deciding on the investigation, shall not make public the Protected Disclosure disclosed except with the prior written permission of the Board. However, this restriction shall not be applicable if any Employee is called upon to disclose this issue by any judicial process and in accordance with the laws of land.

17. ASSURANCES UNDER THE POLICY

- In making a disclosure the employee shall exercise due care to ensure the accuracy of the information. If an employee raises a genuine Protected Disclosure under this Policy, she or he will not be at risk of losing her or his job due to raising the Protected Disclosure nor will she or he suffer from any form of retaliation as a result.
- The Company will not tolerate any harassment or victimization (including informal pressures) against the disclosing employee and will

take appropriate action to protect the employee when she or he raises a Protected Disclosure in good faith.

- The identity of the employee will not be revealed unless the employee himself has made either the details of the Protected Disclosure public or disclosed his identity to any other office or authority. However, it is possible that the Company will be unable to resolve the Protected Disclosure, raised without revealing the Employee's identity (e.g. required for conducting an effective investigation or when evidence is needed in a Court).
- If this occurs the Company will discuss the matter with the Employee at the earliest opportunity.

18. COMPLAINTS OF RETALIATION AS A RESULT OF DISCLOSURE

- If an Employee believes that she or he has been victimized in the form of an adverse personnel action for disclosing Protected Disclosure under this Policy she or he may file a written complaint with the Director so appointed and Vigilance and Ethics Officer.

For the purposes of this Policy an adverse personnel action shall include:

- a disciplinary action
- a suspension
- a decision not to promote
- a decision not to grant a salary increase
- a decision not to hire
- a separation
- an involuntary demotion
- rejection during probation
- a performance evaluation in which the Employee's performance is generally evaluated as unsatisfactory
- an involuntary resignation an involuntary retirement

- an involuntary reassignment to a position with demonstrably less responsibility or status as compared to the one held prior to the reassignment
- an unfavorable change in the general terms and conditions of employment

19. COMMUNICATION

A Whistle Blower Policy cannot be effective unless it is properly communicated to Employees. Employees shall be informed of this Policy by publishing it on the Company's notice board and the website of the Company.

20. RETENTION OF DOCUMENTS

All Protected Disclosures in writing or documented along with the results of investigation relating thereto, shall be retained by the Company for a period of 10 years or such other period as specified by any other law in force, whichever is more.

21. ADMINISTRATION AND REVIEW OF THE POLICY

The Board of Directors shall be responsible for the administration, interpretation, application and review of this Policy. The Board also shall be empowered to bring about necessary changes to this Policy, if required at any stage. The policy will be reviewed on a 2 yearly basis. If there is a change in the business environment, it will be reviewed as and when required.

22. AMENDMENT

The Company reserves its right to amend or modify this Policy in whole or in part, at any time without assigning any reason whatsoever. However, no such amendment or modification will be binding on the Employees and Directors unless the same is notified to them in writing.

23. REPORTING

The reporting of Whistle Blower complaints to the Risk and Governance Committee and the Board of Directors shall be done on Quarterly basis by email / presentation.

V. Prevention of Sexual Harassment Policy

THE PREVENTION OF SEXUAL HARASSMENT OF WOMEN AT WORKPLACE (PREVENTION, PROHIBITION AND REDRESSAL) ACT, 2013 AND CENTRAL RULES, 2013-Act came into force from 23rd April 2020.

Electronic Payment and Services Private Limited. has had a policy on prevention of sexual harassment at the workplace. The policy incorporates the recent legislation of Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.

POLICY ON PREVENTION OF SEXUAL HARASSMENT AT THE

WORKPLACE PHILOSOPHY:

We as a Company respect the dignity of all employees working for the Company irrespective of their gender or hierarchy and we expect responsible conduct and behavior on the part of all our employees at all levels. Providing for a safe and congenial work environment to all employees is an integral part of the Company's employment policy.

OBJECTIVE or PURPOSE:

This policy has been framed with a view to:

- Promote a workplace based on equality and respect.
- Provide a safe and congenial work environment.
- Awareness and sensitization about sexual harassment at the workplace.
- Prevent sexual harassment.

• Provide formal and informal mechanism for redressal in case of complaint of sexual harassment at the workplace.
• Define the implications and outcome of sexual harassment.
• Ensure protection against retaliation to complainants, witnesses, committee members and other employees involved in prevention and complaint resolution.

SCOPE:

This policy shall be applicable to all Female employees of Electronic Payment and Services Private Limited. and its subsidiaries including any associate engaged on fixed term contract, short term engagement, temporary, apprentice, trainees, contract persons and visitors on our premises. It shall also include any unwelcome behavior of a sexual nature mentioned in the policy by any Vendor or Supplier or Contractor including their agents, supervisors, managers and their employees to any of our employees on our premises.

DEFINITIONS:

a. Sexual Harassment:

Sexual harassment includes such unwelcome sexually determined behavior (whether direct or by implication) such as: a. Physical contact and sexual advances; b. Demand or request for sexual favors; c. sexually - colored remarks; d. Showing pornography; and e. any other unwelcome physical, verbal or non- verbal or written conduct of a sexual nature.

"Unwelcome sexually determined behavior" includes but is not limited to: • Subjecting another person to an unwelcome act of physical intimacy including grabbing, brushing, touching, including sexual flirtations, advances or propositions. • Making any unwelcome remark with sexual connotations like sexually explicit, remarks, cracking jokes or using sentences with sexual connotations or making sexist remarks etc. •

showing any sexually explicit visual material in the form of pictures or cartoons or pin-ups or calendars or screen-savers on computers or any offensive written or electronic material or including pornographic. • Engaging in any other unwelcome conduct of a sexual nature, verbal or even nonverbal, staring to make the other person uncomfortable, making offensive gestures, etc. • Sending unwelcome communication of a sexual nature, through e-mail, letter, mobile technology or any other form of written or electronic communication, exhibiting conduct of a sexual nature. • Making an unwelcome demand or request whether directly or by implication for sexual favors and making it a condition of employment or payment of wages or increments or promotion or preferential treatment or threat to detrimental treatment in employment or threat to current or future employment status or similar act.

Prevention of Sexual Harassment at Workplace • Where a Supervisor requests sexual favors from a junior (or any other person) in exchange for actual or promised job benefits such as favorable reviews, salary increases, promotions, increased benefits or continued employment or threatens to terminate any such person for non-co-operation. • Where a boss or other senior person intrudes into the private life of employees or persistently asks them out. • Where any employee(s) make(s) sexual epithet, jokes, written or oral references to sexual conduct, and gossip regarding one's sex life, comments on an individual's body, comments about an individual's sexual activity, deficiencies or prowess in an attempt to humiliate or make another person uncomfortable. • Behavior which creates an environment that is intimidating, hostile, offensive, humiliating for women employee. Workplace: Any place where working relationship and employer-employee relationship between the company and the person exists. This includes our premises (including transit houses and guest houses) and any place visited by the employee arising out of or during the course of employment including transportation provided by the employer for undertaking such a journey.

b. Definition of an Aggrieved Woman: In relation to workplace, a woman of any age whether employed or not, who alleges to have been subjected to any act of sexual harassment by the Respondent.

c. Definition of a Respondent: Against whom the aggrieved woman has made a complaint

d. Definition of an Internal Committee: The "Internal Committee" Internal Committee means an Internal Committee (sec 2(h).It has to be constituted under Section 4 by the Employer in every workplace. It is a statutory requirement

- Mandates a Presiding Officer, who shall be only women
- At least two members from among the employees who are committed to the cause of women or who have experience in social work or have legal knowledge. These members can be of either gender.
- One member from the Non-Governmental organizations or associations who are committed to the cause of women or familiar with the issues of sexual harassment. The member can be of either gender, but preference can be given to women.
- Thus there can only one Presiding Officer and only one outside member from NGO or any other associations.
- However, there is no limit for nominating members from among the employees in the organization.
- But at least 50 percent of such nominated members shall be women only.

GRIEVANCE REDRESSAL MACHINERY:

Given that this policy highlights a preventive focus, there is a need to distinguish between an informal and formal process.

PROCEDURE FOR INFORMAL GRIEVANCE REDRESSAL:

Informal processes normally involve an intermediary means for resolving a problem. In the case of Sexual Harassment, at first instance, the person (i.e. HOD, SBU Head or HR Head Woman representative of the location) may be the point of first contact for anyone seeking informal support or intervention to stop unwelcome behavior.

Benefits of an informal process are:

• It is consistent with the preventive approach.

• It helps to diffuse a minor incident without diluting as also escalating the problem.

• Often people just want unwelcome behavior to stop without drawing undue attention; an informal process makes this option more possible.

• It involves employees to share in the responsibility of eliminating unwelcome behavior at work. A sense of restraint and responsibility on the part of all concerned is critical for the effective functioning of these guidelines.

The preventive or informal process that can be adopted is as follows:

1. Convey to the person who is the cause of distress, about what that person's actions, words, behavior is doing and convey in no uncertain terms that such behavior is not appreciated. What is important is the "Way" a particular behavior, action or word is perceived; "Intent" is of no consequence.

2. The second step would be to approach someone within the company – preferably your Superior or HR Representative. The Superior or HR Representative would then try and counsel or talk it over with a view towards closing the matter amicably.

3. In any case all such incidents along with the resolution, needs to be reported to the Head of HR who will then provide a short report to the Internal Committee and the matter will be closed.

4. However, in the event of it not being resolved, then it would need to

be escalated to the Internal Committee.

PROCEDURE FOR FORMAL GRIEVANCE REDRESSAL:

In the event of the complaint not being resolved through informal mechanism, then it would need to be escalated to the Internal Committee for redressal.

1. The aggrieved woman may make, in writing, a complaint of sexual harassment at the workplace to the Internal Committee, within a period of three months from the date of incident and in case of a series of incidents, within a period of three months from the date of the last incident. The complaint can also be routed through the women representatives at respective locations. The Internal Committee will render reasonable assistance to women for making the complaints in writing. This time limit may further be extended for 3 months if the internal committee is satisfied that there were circumstances that prevented the woman from filing a complaint within the specified timeline.

2. A member of the Internal Committee would then hold an investigation and give a report to the Internal Committee

3. If a member of the Internal Committee is accused, then the member needs to step down during the investigation.

4. The Committee, before initiating the inquiry at the request of the aggrieved woman, will take steps to settle the matter between her and the respondent through mutual settlement (conciliation) wherever such settlement has been arrived, the internal committee shall record it and send the same to the President HR to take action as per recommendation. Once such settlement has been arrived at no further enquiry shall be conducted by the Internal Committee, however, a woman can further refer the same to Internal Committee for redressal if the terms of settlement have not been complied. The Committee, while investigating the complaint referred to it, will call upon both the parties separately, listen, look

at proof (if any), verify documents produced by the parties, allow the parties to produce witnesses and to put forth their say. Both the parties during the course of enquiry are given an opportunity of being heard. At the end of the investigation, the senior member of the Committee shall prepare a report of findings on the complaint and submit it to the Presiding Officer. The findings of the report should be made available to the respondent and aggrieved woman within 10 working days from the date of completion of enquiry. The Presiding officer of the Committee shall ensure that the complaint is attended to within 10 working days after receiving it and that the investigations are completed within 30 working days. The final resolution of complaint should happen within 90 days from the date of complaint.

During the pendency of an inquiry, on a written request made by the aggrieved woman, the committee may recommend to the HR, to

i. Transfer the aggrieved woman or person accused to any other location of work.
ii. Grant leave to the aggrieved woman up to the period of 3 months (over and above the entitled leave).
iii. Grant such other relief to the aggrieved woman as may be prescribed

5. The Presiding officer after studying the report and discussion with the Committee members shall submit her recommendation to the President-HR within 10 days of completing the inquiry.

6. The implementation of the recommendation of Internal Committee by President-HR should be done within 30 days of receipt of such recommendation.

7. Pursuant to a finding of Sexual Harassment by the Committee against any person accused of the same, the Committee may initiate any one or more of the following actions:
    - Actions in accordance with misconduct mentioned in service rules or appointment letter

- Issue a verbal warning
- Issue a warning in writing
- Issue a suspension
- Deprive of increment or promotion
- To deduct, notwithstanding anything in the service rules applicable, from the salary or wages of the accused person the sum as it may consider appropriate to be paid to the aggrieved woman
- Order dismissal depending upon the severity and sensitivity of the incident
- Financial Penalty (In accordance with the mental, physical trauma, loss of career opportunity, medical expenses) in lump sum or in instalments.

In case the Internal Committee on conclusion of the enquiry finds that the allegation was malicious or has made the complaints knowing it to be false, or has produced any forged or misleading document, it will recommend action to be taken by President –HR against the woman who has made the complaint. In all such cases the malicious intent on the part of the woman must be established before any action is recommended.

8. The Internal Committee will protect the identity of all individuals involved during the process, including the aggrieved woman and respondent and contents of complaints and enquiry proceedings.

Guidelines for members of Grievance Redressal Machinery:

- Believe in the reality of the complaint lodged.
- Empathize with the complainant. Do not function like a criminal court.
- Remember that it may be difficult for an employee to talk about anything 'sexual'. Hence there can be a long-time interval between the harassment and the actual complaint.
- Handle complaints in a confidential manner and within 30 working days.

- Submit annual report on sexual harassment cases, if any and actions taken to address the same, to the President –HR and MD
- Maintain all the data related to sexual harassment cases in the company
- Provide safety for the complainant and his or her supporters, if such a need be felt and that the committee can recommend action against persons indulging in intimidation of the complainant or witness to a complaint.
- Discard pre-determined notions of how an accused should look or behave or dress. Be aware of stereotypes.
- Do not insist on detailed description of harassment. This could increase the complainant's trauma.
- Most sexual crimes are committed in private; hence there may not be any eyewitnesses.
- Since this is a human rights issue, balance of probabilities is a sufficient measure of proof.
- Help the complainant regain his or her self-respect.
- Make 'discreet' enquiries as to whether other employees have experienced similar problems.
- Document results of any sexual harassment complaint or investigation. Not only the results, but also document any corrective action that the employee or supervisor was asked to take.
- Inform all employees that it is their obligation to report sexual harassment that they either experience or witness.
- The inability to substantiate a complaint or provide adequate proof need not attract action against the woman. Mechanisms to strengthen implementation of Policy.
- Communication of policy and making it available on website for employees to refer.

- Display constitution of Internal Committee.
- Making it a part of the Corporate Induction.
- Inclusion of the number of cases reported and resolution in the Annual Report.
- Appropriate Government can call upon companies or inspect records related to Policy on sexual harassment and its implementation.

1. **Internal Committee**:

   It has to be constituted under Section 4 by the Employer in every workplace. It is a statutory requirement under the sexual harassment of women at workplace (Prevention, Prohibition and Redressal) Act, 2013 and Central rules, 2013.

Scope:

All female employees on the roles and off role employees also

Objective:

To provide protection against sexual harassment of women at workplace and for the prevention and redressal of complaints of sexual harassment and for matters connected therewith or incidental thereto

Who, how and when –can make a complaint:

- Any aggrieved woman may make complaint of sexual harassment at workplace to the IC within a period of three months from the date of the incident, in case series of incidents have taken place then, within a period of 3 months from the date of last incident.
- Legal heirs or relative or friend or co-worker or officer of Woman Commission or any person having knowledge of incident with written

consent of the woman may make the complaint on behalf of aggrieved woman

- Complaint should be made in writing to the IC.

Procedure:

1. The Internal Committee may before initiating an inquiry under Section 11 and at the request of the aggrieved woman take steps to settle the matter between her and the respondent through conciliation:
   - No monetary settlement shall be made as a basis of conciliation.
   - If conciliation is success, and settlement arrived at, the IC shall record the settlement so arrived and forward the same to the Employer to take action as specified in the recommendations.
   - The IC shall provide the copies of the settlement as recorded to the aggrieved woman and the respondent.
   - No further inquiry shall be conducted by the IC, when a settlement is arrived at under Sec 10(1).

2. The Internal Committee, where the respondent is an employee, will proceed to make inquiry into the complaint in accordance with the provisions of the service rules applicable to the respondent and where no such rules exist, in such manner as may be prescribed

3. IC shall follow the provisions in accordance with the provisions under certified standing orders or service rules of the establishment

4. Complainant shall file 6 copies of complaint along with supporting documents, names and addresses of witnesses
5. Within 7 working days the committee shall send copy of the complaint to the Respondent

6. Within 10 days, the Respondent shall file reply

7. IC has the right to terminate the inquiry proceedings if the complainant fails, without sufficient cause to attend the inquiry for 3 consecutive hearings

8. IC has the right to give an ex-parte decision if the Respondent fails, without sufficient cause, to attend the inquiry for 3 consecutive hearings

9. However before terminating the inquiry or placing ex-parte a notice of 15 days in writing shall be given

10. Inquiry should be completed within 90 days (S 11(4))

11. Three members of IC including Chairperson constitute the quorum

12. If the Respondent pleads not guilty:

- Ask complainant or her representative, if any, to examine witness, if any, in the presence of the accused.
- Documents, if any, will have to be introduced at the appropriate stage and explained in the presence of the accused.
- Accused to cross-examine witnesses immediately after examination-in-chief
- Complainant to examine herself
- Respondent to cross-examine.
- The proper procedure is to lead 'evidence' against the accused employee; give him an opportunity to cross-examine the said witnesses and explain the document which appear against him. Depending on the seriousness of the issue ask the accused whether he wants to give any further explanation on when the issue has gone against him.
- Employer shall take action upon the recommendations of IC within 60 days of the receipt of Report

IC Committee members:

- VP – Corporate Affairs (Presiding officer)
- COO
- AVP – Finance & Accounts
- AVP-HR
- VP-Revenue
- VP – Business Development
- External Member

Reporting of any grievance relating to sexual harassment shall be addressed to below mentioned presiding officer of the Internal Committee through email or written communication on the below:

Ms. Pradnya Bagade
VP – Corporate Affairs

Email Id: ic@electronicpay.in

Committee Meeting: On a bi-annual basis or as and when required

Tenure of the Committee Members:

The Presiding officer or the Chairperson and the members of the Internal Committee shall hold office for such period not exceeding 3 years from the date of appointment as prescribed by the Employer.

Who cannot be a part of the Committee:

1. Anyone Convicted for an offence or enquiry under any law is for the time being pending against him/her.
2. Anyone who has been found guilty or disciplinary proceedings is pending against him/her.

3. He or She has abused his/her position so as to render their continuance in office prejudicial to the public interest.

As per EPS norms all the policies will be reviewed on a 2 yearly basis. If there is a change in the business environment, it will be reviewed as and when required.

VI. Grievance Policy

Purpose:

A platform where an aggrieved can express his or her dissatisfaction, or resentment, that will be taken due notice by the concerned authority and aggrieved may be entitled to seek relief through a particular series of steps.

This policy should be read in conjunction with other related policy documents such as the Code of Conduct, Prevention of Sexual Harassment Policy and any additional related policies passed by the organization will automatically become conjunct to this policy.

Scope:

- All employees on the rolls and off roll employees also
- General Public, Ex-Employees, Vendors and Clients

Objective

The respective teams would be responsible for providing solution to the grievances or complaints.

Aim:

• To identify the genuineness of the grievance

• The committees aim to resolve problems and grievances promptly
• Matter discussed will be kept confidential.

GRIEVANCE REDRESSAL MECHANISM:

I. Internal Grievance Committee: the grievance other than POSH can be filled with this committee.

II. Internal Committee: the POSH related grievance/complaint can be filled with this committee (refer POSH policy separately for the detailed procedure)

III. General Grievance Committee: the grievance related to external person (e.g. General public, Ex-Employee, Vendor, Customer or Client) can be filled with this committee.

PROCEDURE FOR GRIEVANCE REDRESSAL

1. The aggrieved person may make, in writing, a complaint to the dedicated email ID or his concern to the respective committees within a period of one month from the date of incident and in case of a series of incidents, within a period of one month from the date of the last incident.

2. A member of the respective committees would then hold an investigation and give a report to the concerned committee

3.If a member of the concerned committee is accused, then the member needs to step down during the investigation.

4. The Committee, before initiating the inquiry at the request of the aggrieved person, will take steps to settle the matter between him/her and the respondent through mutual settlement (conciliation) wherever such settlement has been arrived, the respective committee shall record it and send the same to the President HR to take action as per recommendation. Once such settlement has been

arrived at no further enquiry shall be conducted by the concerned committee. however, the aggrieved person can further refer the same to concerned committee for redressal if the terms of settlement have not been complied. The Committee, while investigating the complaint referred to it, will call upon the concerned parties separately, listen, look at proof (if any), verify documents produced by the parties, allow the parties to produce witnesses and to put forth their say. The parties during the course of enquiry are given an opportunity of being heard. At the end of the investigation, the senior member of the Committee shall prepare a report of findings on the complaint and submit it to the Chairperson. The findings of the report should be made available to the respondent and aggrieved person within 10 working days from the date of completion of enquiry. The Chairperson of the Committee shall ensure that the complaint is attended within 10 working days after receiving it and that the investigations are completed within 30 working days.

5. The Chairperson after studying the report and discussion with the Committee members shall submit his/her recommendation to the President -HR within 10 days.

6. The implementation of the recommendation of the concerned committee by President-HR should be done within 30 days of receipt of such recommendation.

7. The Committee may initiate any one or more of the following actions against the person is found guilty of having committed an offence according to complaints filed:

- Actions in accordance with misconduct mentioned in service rules or appointment letter
- Issue a verbal warning
- Issue a warning in writing
- Issue a suspension/termination
- Deprive of increment or promotion
- Order dismissal depending upon the severity and sensitivity of the incident
- Financial Penalty.

In case the concerned committee on conclusion of the enquiry finds that the allegation was malicious or has made the complaints knowing it to be false, or has produced any forged or misleading document, it will recommend action including termination to be taken by President –HR against the person who has made the complaint. In all such cases the malicious intent on the part of the that person must be established before any action is recommended.

8. The concerned committee will protect the identity of all individuals involved during the process, including the aggrieved person and respondent and contents of complaints and enquiry proceedings.

Guidelines for members of Grievance Redressal Mechanism:

• Believe in the reality of the complaint lodged.

• Handle complaints in a confidential manner and within 30 working days.

• Maintain all the data related to grievance in the company

• Provide safety for the complainant and his or her supporters, if such a need be felt and that the committee can recommend action against persons indulging in intimidation of the complainant or witness to a complaint.

• Make 'discreet' enquiries as to whether other employees have experienced similar problems.

• Document results of complaint/s or investigation. Not only the results, but also document any corrective action that the employee or senior /HOD was asked to take.

• Communication of policy and making it available on website for employees to refer.

• Display constitution of Internal Grievance Committee / Internal Committee/ General Grievance Committee.

• Making it a part of the Corporate Induction.

I. Internal Grievance Committee:

Objective:

Supports the right of every employee to lodge a grievance, if they believe a decision, behavior or action affecting their employment is unfair. An employee may raise a grievance about any performance improvement action taken against them.

Scope:

All the Employees on the rolls also entails off roll employees.

Procedure:

1. To start the grievance procedure, the aggrieved can either mark a mail, to **grievance@electronicpay.in** or personally meet the members of the grievance committee. The access to mails received on this Email Id would be strictly limited to the committee members.

2. The complainant must fully describe his or her grievance in writing, with details.

3. The person(s) against whom the grievance or complaint is made should be given the full details of the allegation(s) against them. They should have the opportunity and a reasonable time to respond before the process continues.

4. The grievance or complaint would be acknowledged within 3 days of receipt and the TAT for resolving of the complaint would be 30 days, in exceptional cases additional time can be extended depending upon the case for the further investigating the facts, but in any case, total time period (TAT)for resolving or closure of the complaint should not be more than 90 days from the receipt of complaint.

Internal Grievance Committee Members:

- VP – Governance and Risk Analytics (Chairperson)
- Senior Manager-HR
- VP – Digital & Corporate Communication

Reporting of any grievance by employees (except POSH related grievance) shall be addressed to below mentioned Chairperson of the Internal Grievance Committee through email or written communication on the below:

Mr. B. R. Nath
VP – Governance and Risk Analytics
Email Id: grievance@electronicpay.in

Committee Meeting: As and when required.

Tenure of the Committee Members:

The Chairperson and the members of the Internal Grievance Committee shall hold office for such period not exceeding 3 years from the date of appointment as prescribed by the Employer.

Who cannot be a part of the Committee:

1. Anyone Convicted for an offence or enquiry under any law is for the time being pending against him/her.
2. Anyone who has been found guilty or disciplinary proceedings is pending against him/her.
3. He or She has abused his/her position or generally perceived as bias either of parties

4. Immediate reporting authority or HOD of the person against whom the grievance is lodged.

II Internal Committee:

Refer POSH policy separately for the POSH related complaints.

III General Grievance Committee:

Objective:

Supports the right of every member of the General public to lodge a grievance, if they believe a decision, behavior or action affecting or has affected them is unfair.

Scope:

General public, Ex-Employee, Vendor, Customer or Client

Procedure

- To start the grievance procedure, the aggrieved can either mark a mail to **externalgrievance@electronicpay.in** or personally meet the members of the General Grievance committee. The access to mails received on this Email Id would be strictly limited to the committee members
- The complainant must fully describe his or her grievance in writing, with details.
- The person(s) against whom the grievance or complaint is made should be given the full details of the allegation(s) against them. They should have the opportunity and a reasonable time to respond before the process continues.
- The grievance or complaint would be acknowledged within 3 days of receipt and the TAT for resolving of the complaint would be 30 days. in exceptional cases additional time can be extended depending upon the case for the further investigating the facts, but in any case, total time period

(TAT) for resolving the complaint should not be more than 90 days from the receipt of complaint.

General Grievance Committee Members:

- President – HR (Chairperson)
- Vice President -Business Development
- COO

Reporting of any grievance by external person (General public, Ex-Employee, Vendor, Customer or Client) shall be addressed to below mentioned Chairperson of the General Grievance Committee through email or written communication on the below:

Mrs Vidya Mani Mamallan
President – HR
Email Id: externalgrievance@electronicpay.in

Committee Meeting: as and when required.

Tenure of the Committee Members:

The Chairperson and the members of the General Grievance Committee shall hold office for such period not exceeding 3 years from the date of appointment as prescribed by the Employer.

Who cannot be a part of the Committee:

1. Anyone Convicted for an offence or enquiry under any law is for the time being pending against him/her.
2. Anyone who has been found guilty or disciplinary proceedings is pending against him/her.
3. He or She has abused his/her position or generally perceived as biased to the either of parties.

4. Immediate reporting authority or HOD of the person against whom the grievance is lodged.

As per EPS norms all the policies will be reviewed on a 2 yearly basis. If there is a change in the business environment, it will be reviewed as and when required.

SECTION- 3

I. Risk Management Policy

4. Introduction:

This Policy is in compliance with SEBI (Listing Obligations and Disclosure Requirements), Regulations, 2015 and provisions of Companies Act, 2013 read with Rules made thereunder which requires the Company to lay down procedures about the risk assessment and risk minimization.

Electronic Payment and Services (P) Ltd (the "Company") recognizes that enterprise risk management is an integral part of good management practice. Risk management is an essential element in achieving business goals and deriving benefits from market opportunities.

5. Policy Overview:

The Company's risk management policy relates to identification, assessment, monitoring and mitigation of various risks to our business. The policy seeks to minimize adverse impact on our business objectives and enhance stakeholder value. Further, our risk management practices seek to sustain and enhance long–term competitive advantage of the Company.

6. Risk Management Framework:

3.1 Risk Management Structure:

The Audit Committee of Directors shall periodically review the risk management policy of the Company and evaluate the risk management systems so that management controls the risk through a properly defined network.

Head of Departments shall be responsible for implementation of the risk management system as may be applicable to their respective areas of functioning.

3.2 Risk Management Program:

The Company's risk management program comprises a series of processes, structures and guidelines which assist the Company to identify, assess, monitor and manage its business risk including any material changes to its risk profile.

To achieve this, the Company has clearly defined the responsibility and authority of its Board of Directors to oversee and manage the risk management program, while conferring responsibility and authority on the Company's senior management to develop and maintain the risk management program in the light of the day-to-day needs of the Company. Regular communication and review of the risk management practice provides the Company with important checks and balances to ensure the efficacy of its risk management program

3.3 Risk categories and Mitigation Measures:

The following broad categories of risks have been considered in the risk management framework:

Technology Risk: Unforeseen changes in regulations, standards and technology are the biggest risks, though by their very nature, such risks are difficult to quantify. Changes in the regulations pertaining to PKI and e-security may render some of the products irrelevant to the customer and can cause a dent in future revenue.

Mitigation: While compliance is a major selling point for our products, almost all of our products also address very important security needs for the customer. The management also plays an active role in monitoring e-security regulations and making appropriate changes to the product base to keep them relevant.

Major technological breakthroughs that render current cryptographic techniques for protecting information obsolete are another concern for

long-term business continuity. However, the senior management are constantly on guard for such indicators.

Cyber threats: As our products are used to protect transactions and sensitive customer data, the associated risks due to evolving cyber threats will always be a concern.

Mitigation: However, this risk is mitigated by constantly reengineering the products in response to such threats.

Company size and resource risk: Certain problems are faced by the Company in taking advantage of large opportunities due to Company size and resource limitations.

Mitigation: Such problems are addressed through active partnership with large vendors and system integrators. Leveraging such opportunities through our partners keeps us relevant in the market and provides brand visibility.

Receivables Risk: Since the Company is engaged in the business of providing technology and related services, risks associated with timely collection of payments from the customers will always be a concern. The Company enters into Service Agreement with its customers, where terms of payment and the payment process adopted by the customer is clearly defined. Any deviation from the terms of agreement or delay in receiving payments from customers owing to some delivery or product issues is a major risk.

Mitigation: The management takes stock of the receivables, exceeding beyond 90 days and takes necessary measures to recover payments from customers. Sending regular intimations to the customers for recovery of dues or discontinuing services are some measures adopted by the Company depending upon situation. An efficient receivables collection process has helped minimize this risk to a large extent.

Human Resource Risk: Employability risk, viz., attracting the right talent for the right role and attrition risk are two human resource risks faced by the Company. The attrition risk is not just restricted to losing talent (after providing them all the necessary training for the job) but additionally the Company has to absorb the attrition cost as well.

Mitigation: The staff compensation levels are almost on par with the best in the domestic industry. All efforts are made to ensure an innovative work environment to all our employees. The senior management strives to keep the attrition levels under reasonable control.

The Company has been continuously strengthening its internal HR processes to hold on to the critical employees and create a reserve of abundant talent.

4. Oversight and Key Risk Management Practices:

A. Board

The Board is responsible for framing, implementing and monitoring the risk management plan for the Company. The audit committee or management may also refer particular risk management issues to the Board for final consideration and direction.

B. Audit and Risk Committee

The audit committee is responsible for ensuring that the Company maintains effective risk management and internal control systems and processes, and provides regular reports to the Board on the effectiveness of the risk management program in identifying and addressing material business risks. To achieve this, the audit committee is responsible for:

- managing and monitoring the implementation of action plans developed to address material business risks within the Company and its business units, and regularly reviewing the progress of action plans;

- setting up internal processes and systems to control the implementation of action plans;
- regularly monitoring and evaluating the performance of management in managing risk;
- providing management and employees with the necessary tools and resources to identify and manage risks;
- regularly reviewing and updating the current list of material business risks;
- regularly reporting to the Board on the status of material business risks; and
- Ensuring compliance with regulatory requirements and best practices with respect to risk management.

C. Senior management

The Company's senior management is responsible for designing and implementing risk management and internal control systems which identify material risks for the Company and aim to provide the Company with warnings of risks before they escalate. Senior management must implement the action plans developed to address material business risks across the Company.

Senior management should regularly monitor and evaluate the effectiveness of the action plans and the performance of employees in implementing the action plans, as appropriate. In addition, senior management should promote and monitor the culture of risk management within the Company and compliance with the internal risk control systems and processes by employees. Senior management should report regularly to the Board regarding the status and effectiveness of the risk management

program.

D. Employees

All employees are responsible for implementing, managing and monitoring action plans with respect to material business risks, as appropriate.

5. Review of risk management program

The Company regularly evaluates the effectiveness of its risk management program to ensure that its internal control systems and processes are monitored and updated on an ongoing basis. The division of responsibility between the Board, audit committee and senior management aims to ensure that specific responsibilities for risk management are clearly communicated and understood. The reporting obligations of senior management and audit committee ensures that the Board is regularly informed of material risk management issues and actions. This is supplemented by the evaluation of the performance of the risk management program and audit committee, senior management and employees responsible for its implementation. The policy will be reviewed on a 2 yearly basis. If there is a change in the business environment, it will be reviewed as and when required.

II. Information Security Policy

1. Objective

The objective of the Information Security Policy is to ensure that internal data as well as any client information which includes data from the time it is received, stored, secured, disseminated, processed, backups created, and finally terminated. The policy addresses the Confidentiality, Integrity, Availability and Legality requirements of this data. This policy is defined at the enterprise level.

2. Scope and Applicability

The policy applies to Technology, Software Development and Infrastructure related operations at EPS and support functions comprising of, but not limited to HR, Admin, Finance and Marketing to provide secured and quality services. The policy would be inclusive, but not limited to following aspects:

- Information Classification
- Physical and Environmental Security
- End-User Security
- Acceptable use of Assets
- Data Privacy and Prevention of Leakage
- Use of Mobile Devices and Wireless Networks
- Teleworking and Remote Access
- Restrictions on Installation and Use of Software and Licenses
- Control of Malicious Programs
- Backup and Restoration
- Management of Technical Vulnerabilities
- Communications Security
- Use of Cryptographic Controls
- Privacy and Protection of Sensitive Data

- Management of Supplier Relationships

3. Policy

Information assets are critical to the success of our business. We shall therefore, ensure the confidentiality, integrity and availability of the information and information assets of our valued clients and our organization by deploying appropriate people, technology and processes.

- All employees of EPS and third party are responsible for compliance of Information Security in accordance with the documented policies and procedures.
- The Management is committed to satisfying applicable requirements relating to Information Security and continual improvement of the Information Security.
- The organization places great emphasis on the need for the strictest confidentiality in respect of client data. Access to client information is limited only to those individuals and partners who have a specific need to see or use that information.
- This Information Security policy shall be communicated to all employees through training
- It may be required to monitor, to duplicate, to record and to log all staff use of organization technology resources with or without notice. This includes but is not limited to e-mail, network and Internet access, key strokes, file access, login and authentication records, and changes to access or privilege levels within information systems.

Staff Responsibility and Accountability:

- Staff is accountable for their actions and therefore they own any events occurring under their user identification code(s).

- It is the staff's responsibility to abide by policies and procedures of all networks and systems with which they communicate, technically support and or utilize as an end-user.
- Staff responsibilities include but are not limited to:

1. Access and release only the data for which have authorized privileges and a need to know (including misdirected e-mail to only authorized and identifiable receipts).

2. Report information on security violations to the Information Security Officer or designee and cooperate fully with any organization-approved investigations regarding the abuse or misuse of organization-owned information technology resources.

3. Protect assigned user IDs, passwords, and other access keys from disclosure.

4. Secure and maintain confidential printed information, magnetic media or electronic storage mechanisms in approved storage containers when not in use and dispose of these items in accordance with the organization policy.

5. Log off from the system or initiate a password-protected screensaver before leaving a workstation unattended.

6. Use only organization acquired and licensed software.

7. Attend all assigned information security trainings provided by the organization's IT security team.

8. Follow all applicable procedures and policies.

4. Document Owner and Approval

The President-Technology is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review

requirements stated above. A current version of this document is available to all members of staff on the corporate intranet.

5. Policy Renewal

The policy will be reviewed on a 2 yearly basis. If there is a change in the business environment, it will be reviewed as and when required.

6. References

ISO or IEC 27001 standard.

SECTION- 4

I. Equal Opportunities Employer

1. **Objective:**

EPS recognizes that it is essential to provide equal opportunities to all persons without discrimination. This policy sets out the organization's position on equal opportunity in all aspects of employment, including recruitment and promotion, giving guidance and encouragement to employees at all levels to act fairly and prevent discrimination on the grounds of sex, race, marital status, part-time and fixed term contract status, age, sexual orientation or religion

2. **Statement:**

(a) It is the policy of EPS to ensure that no job applicant or employee receives less favorable treatment on the grounds of sex, race, marital status, disability, age, part-time or fixed term contract status, sexual orientation or religion, or is disadvantaged by conditions or requirements that cannot be shown to be justifiable. The organization is committed not only to its legal obligations but also to the positive promotion of equality of opportunity in all aspects of employment.

(b) The organization recognizes that adhering to the Equal Opportunities Policy, combined with relevant employment policies and practices, maximizes the effective use of individuals in both the organization's and employees´ best interests. EPS recognizes the great benefits in having a diverse workforce with different backgrounds, solely employed on ability.

(c) The application of recruitment, training, and promotion policies to all individuals will be on the basis of job requirements and the individual's ability and merits.

(d) All employees of the organization will be made aware of the provisions of this policy.

3**. Responsibility:**

EPS shall provide equal opportunities to all its employees and all qualified applicants for employment without regard to their race, caste, political opinion, religion, color, ancestry, marital status or civil partnership status, gender (including gender reassignment), sexual orientation, age, nationality, ethnic origin or disability.

Human Resource policies shall promote diversity and equality in the work place, as well as compliance with all the local labor laws, while encouraging the adoption of international best practices.

Employees of EPS shall be treated with dignity and in accordance with the EPS policy of maintaining a work environment free of all forms of harassment, whether physical, Verbal or Psychological.

Employee policies and practices shall be administered in manner consistent to the applicable laws and other provisions of this code. Respect to the right to privacy and the right to be heard and that in all matters an equal opportunity is provided to those eligible and decisions are based on merit.

II. Health and Safety Policy

Our Commitment

Towards this, the Company recognizes its responsibility to ensure safety and protection of health of its employees, during work and work related travel. This Policy document defines the vision, principles, aim, required actions and scope of the policy application as well as the responsibility for execution.

Our Vision

Our vision is to be an injury free organization. "Everyone Going Home Safe and Healthy Every Day".

Our Mission

We will bring safety on top of mind for all employees and will integrate it with all business processes. We will realize our Vision through an Integrated Safety Management approach, which focuses on People, Processes, Systems, Technology and Facilities, supported by demonstrated leadership and employee commitment at all levels as the prime drivers for ensuring a safe and healthy work environment.

Safety Principles

EPS's Occupational Safety and Health Policy is based on and supported by the following eight Principles.

These Principles have the same status as the Company's Code of Business Principles:

- All injuries and occupational illnesses are preventable
- All operational exposures can be safeguarded
- Safety evaluation of all business processes is vital
- Working safely is a condition of employment
- Training all employees to work safely is essential
- Management audits are a must
- Employee involvement is essential
- All deficiencies must be reported and corrected promptly

Electronic Payment and Services Private Limited (EPS) recognizes people as its most important asset and is committed to a safe and healthy work environment impacting those working for the organization. Management at all levels will be responsible and will be held accountable for the occupational safety and health performance of the Company. At the same time it is the duty of every employee to work in a safe manner so as not to endanger himself or herself or his or her colleagues at work and during travel. This is a condition of employment.

EPS aims to prevent occupational injuries and ill health through the following actions:

- Integrate safety into all business processes. Proactively evaluate risk of occupational injury or illness and implement actions to mitigate the risk.
- Design, adapt, operate and maintain technology other facilities within the designated safety criteria throughout their working life

Women employees are not allowed for late sitting beyond 7:00 pm and in case of doing so, it needs to be informed to the HR by the reporting supervisor (Pre-Facto or Same day) and a mail confirming the employee having reached home safely to follow the same day to HR Team and admin team. Transport reimbursement to be done and supervisor needs to ensure that late sitting is work related and covering work hours.

III. ESGI Policy

Objective:

This ESGI Action Plan ("Action Plan") outlines the actions in the areas of Economic, Social, Governance and Impact that are required for EPS and to encourage good ESGI practices within the Company in general.
To maintain robust ESGI principles, wherein there would be a significant developmental impact in the growth markets by improving the performance of companies and working conditions for workers and local communities, developing access to future capital, and also reducing investment risk. This includes high standards around financial inclusion, health and safety, environmental issues, social engagement, business integrity, corporate governance, as well as transparent accounting practices.

To ensure complete adherence of the above mentioned a committee has been designed. The details of the committee are as below mentioned:

ESGI committee:

- President HR and Administration- Overall ESGI responsibility
- GM – HR – Member
- Senior Manager-Corporate Affairs-Member
- GM – Administration – Member
- COO-Member
- AVP-HR-Member
- Vice-President-Analytics and Risk Governance-Member

Committee Meeting :

Second Friday of the month and or as and when required. (Quarterly basis)

Worker's Organizations:

Freedom of association ensures that workers and employers can associate to efficiently negotiate work relations. Combined with strong freedom of association, sound collective bargaining practices ensure that employers and workers have an equal voice in negotiations and that the outcome will be fair and equitable. ILO standards promote collective bargaining and help to ensure that good labor relations benefit everyone. EPS supports such ILO standards. Principles of collective bargaining can be read at:

http://www.ilo.org/global/standards/subjects-covered-by-international-labour-standards/collective-bargaining/lang--en/index.htm

Revise relevant company policies and governance documents to reflect an open attitude towards workers' organizations as per the ILO Freedom of Association and Protection of the Right to Organize Convention (No. 87) and the Right to Organize and Collective Bargaining Convention (No. 98)

IV. E-Waste Policy

Empanelment of dismantler or recycler

E-waste management is done by a dismantler or recycler or service provider or asset dealer or asset distributor or asset vendor.
Selection and empanelment is done as per the Procure to pay process.

Assembly, collection and disposal of E-waste

1. Details of the Electronic instruments that are set for disposal are recorded and documented. Form 2 and register is updated and maintained by Admin. IT assets that need to be disposed are reviewed and approved for disposal by the HOD – IT.

   Non-IT e-Waste (Refrigerator, Air conditioner, electrical fittings, wires etc.) are reviewed and approved for disposal by the HOD – Admin.

   Note: Once E-waste at ATM sites or Regional office is set for disposal, the disposal activity is managed by Admin and the local channel manager.

2. Once approval is taken, all E-waste is assembled in a safe place in the HO or ATM site or Regional office.

   E-waste is to be disposed of within 180 days of accumulation and updation on form2. The dismantler or recycler or service provider or asset dealer or asset distributor or asset vendor, is notified to collect the E-waste. Note: Care to be taken to ensure E-waste generated for electronic equipment mentioned in Schedule I, is not mixed with E-waste containing radioactive material under the provisions of the Atomic Energy Act, 1962.

3. The dismantler or recycler or service provider or asset dealer or asset distributor or asset vendor, collects the E-waste and proceeds with the E-waste disposal

Annual Return Filing

Annual return for the previous financial year is filed in Form-3, to the concerned State Pollution Control Board by 30th June every year.

Note: The authorities are state wise. Form to be submitted online wherever such a facility is available or to be sent by registered post.

SECTION- 5

I. Acceptable Usage Policy

1. Purpose

The purpose of this policy is to define acceptable usage of assets for users while accessing Organization computing resources. A clearly defined and enforced Acceptable Usage policy (AUP) is critical to maintain information security requirements. Internal practices that are inappropriate or insecure may compromise the overall information security posture.

2. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers, including all third parties having access to the organization information and systems, Internet access and electronic communication services. This policy applies to all organization Information Systems owned, leased or used by EPS as well as any non-Organization owned system device that connects to the organization resources

3. Responsibility

HR is responsible for user awareness training.

4. Acceptable Use

4.1 General Use and Ownership

4.1.1 Employees shall NEVER share their personal passwords to any organization's system, and employees shall not attempt to gain access to another employee's organization's systems and messages. The organization, however, reserves the right to access any organization system including but not limited to, email and voice mail messages at any time, without notice to the employee.

4.1.2 Users shall not seek to avoid and should uphold EPS' anti-malware policy and procedure, shall not intentionally interfere in the normal operation of the network or take any steps that substantially hinder others in their use of the network, and shall not examine, change or use another person's files or any other information asset for which they don't have the owner's explicit permission.

4.1.3 The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material, software or other material shall be expressly prohibited. While EPS' management desires to provide a reasonable level of privacy, users should be aware that the data they create on the organization's Systems remains the property of EPS. The organization reserves the right to access and disclose all Data that is sent, received or accessed by the organization's systems for any purpose. All such data, regardless of content or the intent of the sender, are a form of corporate correspondence, and are subject to the same internal and external regulation, security and scrutiny as any other corporate correspondence.

4.1.4 All communications including but not limited to text, images, photos, videos may be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. EPS may review communications and logs to maintain system-wide integrity and ensure that users are using the Systems in accordance with EPS policy.

4.1.5 While transmitting sensitive information, users shall notify the recipient or other designated person beforehand of incoming document(s) such that the receiving party should pick up the documents immediately following the transmission.

4.1.6 Users shall not carry out any other inappropriate activity as identified from time to time by EPS and shall not waste time or resources on

non-organization business. This includes downloading bandwidth intensive content such as streaming video and MP3 music files, sharing digital photographs, etc.

4.1.7 Employees are responsible for exercising good judgment in the personal use of organization systems. In the absence of specific policies regarding personal use of organization systems, employees should consult their supervisor or manager for guidance.

4.1.8 The distribution of any information through the Internet (including by e-mail, instant messaging systems and any other computer-based systems) may be scrutinized by EPS and also reserves the right to determine the suitability of the information.

4.1.9 Information processing facilities, assets including PCs, Laptops, iPad, tablets, mobile devices, work stations and network devices shall only be used by authorized personnel upon the approval of the respective owner.

4.1.10 Critical technologies usage:

- Explicit approval from authorized parties to use the technologies.
- All technology use shall be authenticated with user ID and password or other authentication item.
- A list of all devices and personnel authorized to use the devices.
- A method to accurately and readily determine owner, contact information, and purpose.
- Acceptable uses for the technology.
- Acceptable network locations for the technology.

4.1.11 EPS reserves the right to audit networks and organization systems on a quarterly basis to ensure compliance with this policy.

4.2 **Security and Proprietary Information**

4.2.1 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords shall be changed in accordance with EPS' Password Policy.

4.2.2 All PCs, laptops, iPads, tablets, mobile devices and workstations that access EPS' network or systems shall be secured with a password-protected screensaver with an automatic activation feature when the device will be unattended.

4.2.3 Because information contained on portable devices is especially vulnerable, special care should be exercised. Users shall protect portable devices in accordance with the EPS' Mobile Device Policy.

4.2.4 Postings by employees from EPS email addresses to newsgroups or social media networks such as Facebook and Twitter should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of EPS, unless posting is in the course of business duties in accordance with EPS' Social Media Policy.

4.2.5 Users shall use discretion when discussing Organization "Confidential" information. When possible, specific references to names and other identifiers should be excluded.

4.2.6 Employees shall not disclose Organization information over voice systems without identifying the caller. If the caller requests for "Confidential" information, users shall adhere to EPS`s Data Classification policy for dissemination.

4.2.7 Users shall use voice systems only for business usage.

4.2.8 All devices used by the employee that are connected to organization systems, whether owned by the employee or EPS shall comply with all EPS Policies.

4.2.9 Employees shall use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.2.10 While printing "Confidential" information; users shall be aware of the printer location and its vicinity and ensure that printed documents are retrieved immediately.

4.2.11 User shall use printer only for department usage.

4.3 **Unacceptable Use**

4.3.1 Under no circumstances is an employee of EPS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing organization systems. For guidance in such matters employees should consult their supervisor or manager.

4.3.2 The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities.

4.3.3 The list below is by no means exhaustive, but attempts to provide a framework for activities, which fall into the category of unacceptable use.

- Sending or posting discriminatory, harassing, or threatening messages or images

- Stealing, using, or disclosing someone else's code or password without authorization

- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
- Sending or posting messages or material that could damage the organization's image or reputation
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person
- Refusing to cooperate with a security investigation
- Jeopardizing the security of the EPS' Systems
- Sending or posting messages that disparage another organization's products or services
- Unauthorized use of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation or distribution of any copyrighted software for which EPS or the end user does not have an active license.

4.4 **System and Network Activities**

The following activities are strictly prohibited:

4.4.1 Exporting software, technical information, encryption software or technology, in violation of international or regional export control

laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.4.2 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.4.3 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.4.4 Using an EPS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

4.4.5 Making offers of products, items, services; or engaging in commercial activities originating from any EPS account unless it is part of normal job duties.

4.4.6 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.4.7 Any use for political purposes shall be prohibited, except to communicate with elected officials as part of normal job duties.

4.4.8 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.4.9 Port scanning or security scanning shall be expressly prohibited unless prior notification to EPS Management is made and approved.

4.4.10 Executing any form of network monitoring which shall intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job or duty.

4.4.11 Circumventing user authentication or security of any host, network or account.

4.4.12 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.4.13 Using any program or scrip tor command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Network.

4.4.14 Providing information about, or lists of, EPS employees to parties outside EPS.

4.4.15 Use of organization systems by anyone other than the authorized employee, unless required for performance of job, such as allowing access to a vendor or contractor if required. This restriction includes but is not limited to use by family members of organization systems.

4.5 **Email and Communications Activities**:

Email and communication activities are defined in EPS' Email Use Policy.

4.6 **Internet Use**

Internet usage policy is defined in EPS' Internet Use Policy

4.7 **Blogging**

Policy is documented in EPS' Social Media Policy.

5. **Violation of Policy**

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

6. **Enforcement**

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law.

7. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO

8. **References**

This procedure refers to the section 8.1.3 of the ISO or IEC 27001 standard and Section 43, 65, 66-E, 67, 67-A and 67-B of the IT Act 2008.

II. Clean Desk Policy

1. **Purpose**

The main purpose for a clean desk policy is to significantly reduce the threat of a security incident, as confidential information will be locked away when unattended.

2. **Scope**

All staff, employees and entities working on behalf of EPS are subject to this policy.

3. **Policy Statement**

3.1 At known extended periods away from your desk, for example a meeting or lunch break, all papers containing PI, confidential, restricted and customer related information shall be kept in locked drawers or offices.

3.2 At the end of the working day the employee is expected to clean their desk and lock up all papers containing PI, confidential, restricted and customer related information. EPS provides locking desks and filing cabinets for this purpose.

3.3 Computers and terminals should be left logged off or protected with a screensaver and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

3.4 Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) shall be prevented;

3.5 Media containing sensitive or classified information should be removed from printers immediately.

4. **Violation of Policy**

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

5. **Enforcement**

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law.

6. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

7. **References**

This procedure refers to the section 11.2.9 of the ISO or IEC 27001 standard.

SECTION- 6

I. Access Control Policy

1. Purpose

The purpose of this policy is to ensure that access to information systems are allocated based on business and security requirements. This policy identifies access controls necessary to protect information from unauthorized access, leakage and deletion.

2. Scope

This policy applies to all employees, contractors, consultants, all personnel (including system support staff with access to privileged administrative passwords) contractual third parties of the company with any form of access to EPS`s information and information systems.

3. Policy

3.1 Access to EPS's information processing facilities, application systems, databases, network, communication and operating systems shall be restricted on "Need to Know, Need to Do" basis to protect confidentiality, integrity and availability of its information.

3.2 EPS shall provide all employees and other users with the information they need in order to carry out their responsibilities in an effective and efficient manner as possible.

3.3 EPS shall assign all users a unique ID before allowing them to access system components or cardholder data.

3.4 The allocation and use of privileged access rights should be restricted and controlled.

3.5 Access control rules and rights to applications expressed in standard user profiles for each Users or group of users shall be clearly stated

along with the business requirements in Access Control Rules and Rights.

3.6 Access to the program source code shall be controlled and restricted.

3.7 Use of privileged utility programs shall be controlled and restricted.

3.8 All users should authenticate before accessing any system components using a password or token device or biometric.

3.9 Only database administrators should have the ability to directly access or query databases.

3.10 The security requirements of each business application shall be determined by a risk assessment that identifies all information related to the application and the risks to that information.

3.11 The access rights to each application takes into account:

3.11.1 The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and network(s).

3.11.2 Data protection (DPA 1988) and privacy and other contractual commitments regarding access to data or services.

3.11.3 The 'need to know' principle (i.e. access is granted at the minimum level necessary for the role) and

3.11.4 'Everything is generally forbidden unless expressly permitted'.

3.11.5 Rules that shall always be enforced and those that are only guidelines

3.11.6 Prohibit user initiated changes to information classification labels.

3.11.7 Prohibit user initiated changes to user permissions.

3.11.8 Enforcing rules that require specific permission before enactment.

3.11.9 Privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

3.12 All access control systems shall have a default "deny-all" setting.

3.13 EPS shall have standard user access profiles for common roles in EPS (Access Control Rules and Rights).

3.14 Management of access rights across the network(s) should be done by IT team and in line with User Access Management.

3.15 User access requests, authorization and administration shall be segregated as described in Access Control Rules and Rights.

3.16 User access requests are subject to formal authorization, to periodic review and to removal. 3.17 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).

4. Violation of Policy

All employees are obligated to report violations of this policy to ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

5. Enforcement

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law.

6. Document Owner and Approval

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

7. References

This procedure refers to the section 9.1.1, 9.4.4, 9.4.5 of the ISO or IEC 27001 standard and Section 29, 43, 43-A, 65, 66 and 70 of IT Act 2008.

II. Change Management Policy

1. Purpose

The purpose of this policy is to protect EPS' information assets, infrastructure and application environments by assuring that changes to any environment are made in a controlled manner, minimize risk, and limit unintended or adverse results.

2. Scope

This policy applies to all significant, non-routine changes to information assets, information processing facilities, infrastructure components and application environments.

3. Policy Statement

It is EPS' policy to assure that all significant, non-routine changes to information assets, information processing facilities, infrastructure components and application environments are documented, reviewed and approved by the Change Advisory Board (CAB) and designated approvers.

3.1 All change requests shall be submitted by the user and reviewed by the Change Manager to assure adherence to this policy.

3.2 All significant, non-routine changes shall follow the change management procedure.

3.3 All changes will go through a process where there is a segregation of duties between application development, promotion, and verification. There shall be named and identified resources for each application area.

3.4 Significant, non-routine changes to information or IT environments include but not limited to:

- Implementation of new resource or functionality;
- Modification to existing IT resource or functionality;
- Removal or disposal of existing IT resource or functionality.

- Interruption of service.

3.5 Change requests shall follow the process as outlined in Change Control Procedure which outlines the following:

- Type of change.
- Change authorization.
- Change monitoring
- Change deployment.
- Change review.

3.6 All changes shall be tested prior to deployment.

3.7 Assessment of the potential impacts, including information security impacts shall be conducted prior to deployment of any change.

3.8 Asset inventory shall be updated after every change.

3.9 Changes shall be communicated to relevant people with operational instructions as applicable.

3.10 A Change Log shall be maintained for all changes.

4. **Violation of Policy**

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

5. **Enforcement**

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law.

6. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

7. **References**

This procedure refers to the section 12.2.1, 12.1.4, 14.2.2 of the ISO or IEC 27001 standard and section 43 of IT Act 2008.

III. Data Classification Policy

1. **Purpose**

EPS creates, receives, stores, uses and transmits a wide range of confidential and internal information. The purpose of the Data Classification Policy is to define the types of information that EPS considers sensitive Scope.

2. **Scope**

This policy is applicable to all EPS employees and contractors as well as any vendors that create, receive, store, use, come in contact with or transmit EPS data. This policy covers information that is stored or shared via any means including electronic and paper information, and information shared orally or visually (such as telephone and video conferencing).

3. **Policy Statement**

3.1 All data shall be classified by the owner as per the criticality associated with the information. Once information is classified; all users shall adhere to the requirements for handling information based on the classification. Owners may choose to designate additional controls to further protect their information.

3.2 The guidelines below require employees to apply good business opinion with respect to treatment of EPS Information. When in doubt, contact your Manager, Information Security, or a member of the ISF for guidance.

3.3 EPS data shall not be disclosed by any means (for example, by paper, orally, or electronically) to third-parties such as contractors, vendors, competitors, and other non-EPS entities without express permission by authorized personnel. For example, business strategic plans shall not be disclosed to third-parties without ISF or Business Head or

ISMS head permission. Conversely, Company`s Human Resources may disclose confidential employee information to EPS's Background Verification Company since it is necessary to perform the HR job function.

3.4 Information received from third-parties under contractual arrangements including Non-Disclosure Agreements, Confidentiality Agreements, and general business contracts shall not be shared with any EPS`s employee or any other third-party unless that employee or other third-party is covered by the agreement or contract.

4. **Data Classification**

Classifications and associated protective controls for information takes into account business needs for sharing and restricting information and business impacts associated with such needs. The four classifications of data in EPS are as follows:

- Confidential
- Restricted or Privileged
- Internal
- Public

4.1 Classification of Information

4.1.1 Information will be classified in terms of its value, legal requirements, sensitivity and criticality to the organization. The asset owners will classify the assets as per appropriate security classification guidelines.

4.1.2 Security classification level of the asset will be identified based on the following factors:

- Impact on the business or process if the Confidentiality of the asset is breached.

- Impact on the business or process if the Integrity of the asset is compromised.

- Impact on the business or process if the Availability of the asset is not there.

4.1.3 Rules for Data Classification

- All information possessed by or used by a particular business unit within EPS shall have a designated information owner. The information owners shall be responsible for assigning or maintaining appropriate information classifications.

- Files or e-mails created by individuals shall be owned and classified by them.

- The Information classification process shall be completed for existing data and shall be undertaken for any new information whether it is in hard copy or soft copy.

- Information stored in several media formats (either hard copy or electronic) shall have the same level of classification.

4.1.4 Information Classification Matrix

Information owners of EPS will use the following matrix to classify information assets in a manner that balances the risk of compromise with the needs of normal business operations.

Classification Level	Definition	Examples
Confidential	Applies to sensitive business information, the unwanted disclosure of which can bring substantial financial damage, damage to company's reputation or lead to grave legal consequences. This also applies to information, which can be of value to competitors that can influence the success or the existence of the entire company or part of its business. Access to Confidential information is restricted only to few employees or associated entities. Confidential information or documents will not be available to all the people within EPS or outsiders.	• Company strategies; • Technology, or strategic planning; • Commercial and budget plans • Information about processes and innovations; • Information of equal confidentiality from business partners; • Information capable of influencing the information about crisis situations; • Business Agreements • Client Proposals and bids • Pricing details • Process Templates • Project documents or presentations • Approach Papers • Surveillance or Internal Audit Reports • Training course design and development material

Classification Level	Definition	Examples
		• Personnel data, e.g. remuneration, assessment documentation, • Client data and deliverables (Security assessments, VAPT reports and findings) • Confidential information about third parties (in particular within the context of secrecy agreements); • Information on security measures and serious deficiencies, information on internal network topology; • Copies, backups and archives of confidential information; • Standard deliverables, templates,
Restricted Or Privileged	This classification applies to sensitive or critical business information which is intended for use within EPS for a limited set of people (e.g. information for departmental or committee or subcommittee or functional unit).	• Project documents, • SOP's and • Operational reports of various departments and information systems therein.

Classification Level	Definition	Examples
	Its unauthorized disclosure could adversely impact EPS, its stakeholders, business partners, employees, and customers. Confidentiality, Integrity and Availability for this classification of information needs to be maintained at highest level.	
Internal	Applies to business information for which unwanted disclosure can have damaging consequences. This is generally information, which is accessible to a wide circle of employees but is not intended for outsiders.	• Internal communications, correspondance, Internal e-mails; • Internal guidelines, like circulars, instructions, organization plans; • Internal information like contracts, reports, plans;

1.1.1 **Classification or Treatment Guidelines**:

- Information shall be treated in accordance with its need for protection, irrespective of the media on which it is stored.
- The originator or issuer of information shall classify the information into one of the protection classes suiting its need for protection, then label it accordingly, and transmit the information together with its label.
- The recipient shall treat the information in accordance with the classification established by the originator or issuer.
- If it is found that information is classified too low, the classification shall be corrected and the originator or issuer shall be informed.
- In cases of doubt, information, which is not classified at all, shall be regarded as worthy of protection. As a minimum, this information shall be treated as if it were carrying the label "Internal".
- When classifying information as "Confidential" check whether the extra effort which such a decision entails can be justified by setting it against the possible disadvantages of not protecting the information in this way;
- Time limits can be set for the classification.
- When simultaneously distributing information, which is subject to different classifications, in a folder for example, the overall title page shall show the highest classification label.
- For public information, the date when the owner declared the information public, shall also be indicated. The ISO will have list of all Information classifications and Ownership.

- Documents may be preserved as below:

  a) Confidential or Controlled Copy: To be available in PDF format.

  b) Master Copy: The original copy to be available only with ISO (only in case of the ISMS)

  c) Internal: .doc or .xls format or any printed matter

1.1.2 Identification **or creation**

- The protection class shall be visible to the recipient right away.
- With written information, the label shall be in an area where it is readily visible and easy to read, for example:

  a) With paper documents, and their respective electronic versions, the label will be in the footer on each page of the document.

  b) Every transparency shall be labeled.

  c) Data media will be labeled on the envelope or on the labeling area.

  d) With electronic information this identification field is placed in the footer.

1.1.3 Minimum Baseline Security Control Matrix

- The requirements in the following table outline the minimum baseline security control (MBSC) mechanisms that shall be used for each information classification.

Security Objective	Public	Internal	Restricted Or Privileged	Confidential
Identification and Authentication	None	User-IDs and Passwords	User-IDs and Passwords, Strong Authentication	User-IDs and Passwords, Strong Authentication
Authorization and Access Control	Access Control for Modification	Authorization for granting access by business department head, access control as per functions, or directory level access control	Authorization for granting access by business department head, access control as per functions, or directory level access control	Fine-grained access control - by document and directories
Confidentiality	None	None	None	Encrypted communications (all), and encrypted files on storage media

1.1.1 Declassification or Downgrading of Information

- The designated information owner may, at any time, declassify or downgrade information. To achieve this, the owner shall change the classification label appearing on the original document and inform concerned HOD and all known recipients or users.
- If known, the date that confidential information will no longer be sensitive (declassified) shall be indicated on all sensitive information of EPS.
- The designated information owner may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at a certain classification level.
- To determine whether sensitive information may be declassified or downgraded, at least once a year, information owners shall review the sensitivity classifications assigned to information for which they are responsible.

2. Labeling of Information

2.1 Removable and storage media (CD-ROMs, USB sticks, tapes, etc.) shall be labeled to indicate classification levels.

2.2 Electronic documents and information assets shall be labeled by appropriate headers.

2.3 Information processing facilities shall be labeled as per sensitivity. For example: servers, desktops, laptops, networking equipment, server rooms, etc.

2.4 All e-mails have a standard disclaimer set out manually on the email to the effect that the views expressed in the e-mail are those of the sender alone and do not reflect the views of EPS.

- Copying
- Storage
- Transmission by post, fax, electronic mail
- Transmission by spoken word, mobile phone,
- Destruction

3. Handling of Assets

Information handling procedure for each type of assets, physical and electronic format, and each type of activity viz.

Label			
	Public	**Internal**	**Confidential**
1.Copying standards	No special permission required	No special permission required	Photocopying with approval from data owner. Photocopying minimized and when necessary only, to be personally supervised.
Storage standard			
a.Printed material	No special permission required	Reasonable precautions to prevent access by non-employees.	Storage in a secure manner, e.g. secure area, lockable enclosure
b.Electronic documents	Storage on all drives	Storage on all drives	Storage on secure drives. Storage on shared drives without password protection for reading is prohibited. Password protection of documents preferred.
c. E-mail	No special permission required	Reasonable precautions to prevent access by non-employees.	Storage in a secure manner, e.g. password access or reduce to written form, delete electronic form and store in accordance with storage of printed materials.
Transmission by Post, Fax, e-Mail			
a. Mail within organization (inter-office)	No special handling required	No special handling required	• Sealed envelope marked Confidential. Notify recipient in advance.

			• Personal delivery where possible,
b. Mail outside the organization	No special handling required	No special handling required	Registered mail, courier, traceable delivery preferred with return receipt mail. Personal delivery where possible,
c. E-mail within organization	No special handling required	No special handling required	Use of e-mail discouraged where practical unless digitally signed.
d. E-mail outside the organization	No special handling required	No special handling required	E-Mail will be encrypted. Broadcast to distribution lists prohibited.
Fax			
i. Location of fax machine	Located in area not accessible to general public	Located in area not accessible to general public	Located in area not accessible to general public and unauthorized persons
iii. Transmission safeguard	Reasonable care in dialing.	Reasonable care in dialing.	Procedure for telephone notification prior to transmission and subsequent telephone confirmation of receipt required.
4. Transmission by spoken word	No special permission required	Reason-able precautions to prevent inadvertent disclosure	Active measures to prevent unauthorized parties from overhearing information and close control to limit information to as few persons as possible

5. **Violation of Policy**

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

6. **Enforcement**

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law.

7. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

8. **References**

This procedure refers to the section 8.2 of the ISO or IEC 27001 standard and Section 43-A, 72, 72-A of the IT Act 2008.

IV. Data Protection and Privacy Policy

1. **Purpose**

Data protection and privacy policy of EPS deals with the process through which information concerning individuals including employees, third party users and client is obtained and disclosed. EPS respects the confidentiality of this information and strives to protect the privacy of individuals by regulating the collection, maintenance and disclosure of personal information.

1. Scope

All information concerning individuals including employees, third party users and clients are covered in the scope of this policy.

2. Policy Statement

EPS is committed to compliance with all relevant data protection policies. Personal data is classified as refer to classification levels in Data Classification Policy. The policy applies to all personal data held by the company, including on wireless notebook computers, personal digital assistants and mobile telephones.

All Employees or Staff will be provided training to ensure that they understand EPS's policies and procedures to implement them.

The disciplinary process will be invoked in circumstances where this policy may have been transgressed.

3. Violation of Policy

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

4. Enforcement

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law.

6. Document Owner and Approval

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

7. References

This procedure refers to the section 18.1.4 and 18.1.5 of the ISO or IEC 27001 standard and section 7, 14, 67-C of IT Act 2008.

V. Email Use Policy

1. **Purpose**

The purpose of EPS's Email Policy is to establish the rules for the use of EPS's email for the sending, receiving, or storing of electronic mail.

2. **Scope**

This policy covers appropriate use of any email sent from an EPS email address and applies to all employees, vendors, and agents operating on behalf of EPS.

3. **Responsibility**

3.1. Every employee, vendor, contractor or agent is responsible for not compromising EPS through the use of organizational e-mail facilities. 3.2. Information Security Officer is responsible for ensuring that all users of email are aware of acceptable use of email.

4. **Policy**

4.1 Prohibited Use: EPS email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, color, religion, sex, national origin, age, disability, genetic information, sexual orientation, military or veteran status, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any email with this content from any EPS employee should report the matter to their supervisor immediately.

4.1.1 The sending of unsolicited email messages, including the sending of "junk mail" or other advertising material to

individuals who did not specifically request such material (email spam).

4.1.2 Any form of harassment via email whether through language, frequency, or size of messages.

4.1.3 Unauthorized use, or forging, of email header information.

4.1.4 Sending email for the purpose of soliciting email addresses with the intent to harass or to collect replies.

4.1.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.1.6 Posting the same or similar non-business-related messages to Usenet newsgroups or public forums (newsgroup or public forums spam).

4.1.7 Modifying the header information or content of an email authored by someone else prior to forwarding or replying to it without clearly stating that the email has been modified and how it has been modified.

4.1.8 Users shall not transmit or disclose, via email or any other means, restricted or confidential information, as defined in EPS's Data Classification Policy, unless it is a necessary function of the user's duties, in which case such transmission shall be encrypted.

4.1.9 If a partner or client sends credentials (accounts and passwords) to EPS via email, EPS employees shall delete credential information before replying to the email. The credential information shall NOT be forwarded to other EPS employees.

4.1.10 Based on the content and the recipient of an email, such as confidential content emailed to external recipients, a standard legal disclaimer will be included in accordance with the Data Classification Policy.

4.1.11 Users shall not open incoming e-mail attachments that originate with unknown third parties or that, even if they appear to have been sent by a known party, were not expected.

4.2 Viruses and hoax virus messages: users are required to report any third party e-mail messages they receive about viruses to Information Security or Information Technology immediately, by telephone or in person, and on no account should it be forwarded, or copied on, to anyone, whether inside or outside the network.

4.3 Users are required to limit the use of group e-mail addresses, to limit copying to unnecessary recipients, to restrict use of the 'reply to all' function, and restrict the use of the blind copying feature as it will generate dozens of mail.

4.4 Users are required to delete non-essential e-mail messages as soon as possible and, on a regular basis, to clear e-mail boxes of correspondence that is no longer required. The archive facility should be used so that messages that need to be retained but which are no longer current can be removed from the inbox. These controls are necessary so as to avoid e-mail boxes becoming so full that more and more server space is required to support the system. The sent items box shall also be weeded on a regular basis.

4.5 Users are prohibited from setting up automatic forwarding of e-mails to addresses external to EPS or of copying e-mails to addresses outside EPS unless there is a legitimate business purpose for doing so.

4.6 Personal Use: Using a reasonable amount of EPS resources for personal emails is acceptable, but non-work related email shall be

saved in a separate folder from work related email. Sending or forwarding of chain letters or joke emails from EPS email account is prohibited. The use of EPS email to solicit EPS employees is prohibited.

4.7 Monitoring: EPS employees shall have no expectation of privacy in anything they store, send or receive using EPS's email system. EPS may monitor and read messages without prior notice stored within or passing through its mail system even if deleted or marked personal or confidential. EPS is not obliged to monitor email messages. EPS may also share any messages with outside parties such as attorneys and law enforcement agents without prior notice.

4.8 Email Disclaimers: All EPS employees shall use the Email Signature template located in which includes an official Confidentiality Notice. EPS will notify employees when the template is updated and employees shall update their email signature within one week of receiving this notice.

5. Violation of Policy

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

6. Enforcement

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law.

7. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

8. **References**

This procedure refers to the section 8.1.3 of the ISO or IEC 27001 standard and Section 43, 65, 66-A, 66-E, 66-F, 67, 67-A and B, 72, 72-A and 84-C of the IT Act 2008.

VI. Password Policy

1. **Purpose**

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. **Scope**

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at EPS facility, has access to EPS's network, or stores any non-public EPS information.

3. **Policy Statement**

3.1. **General**

3.1.1 All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) shall be stored in an encrypted repository and must be changed at least on

a quarterly basis. Any password change frequency greater than this must be approved by the ISMS Head.

3.1.2 All passwords used to access partner and client systems must be stored in EPS's secure location, EPS employees, contractors, and vendors should never store partner or client credentials in clear text or in any other repository other than the one said above.

3.1.3 All user-level passwords or passphrases (e.g., Windows, email, web, desktop computer, etc.) shall be changed every 90 days.

3.1.4 Use of group and shared IDs and passwords or other authentication methods are explicitly prohibited.

3.1.5 User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

3.1.6 All temporary passwords shall be changed at first log-on.

3.1.7 Any user requesting a change in password should be duly verified.

3.1.8 Passwords shall not be manually inserted into email messages or other forms of unencrypted electronic communication.

3.1.9 Password or passphrases history shall be maintained for 5 past used passwords or pass phrases.

3.1.10 Do not use vendor-supplied defaults for system passwords.

3.1.11 All user-level and system-level passwords must conform to the guidelines described below.

3.2 **General Password Construction Guidelines**:

3.2.1 Everyone should be aware of how to select strong passwords.

3.2.2 Passwords shall have the following characteristics: Where a system does not allow one or more of these characteristics all other characteristics that are supported by the system must be incorporated.

- Passwords or passphrases must contain a minimum of 8 characters.
- Passwords or pass phrases must contain both upper case and lower case letters as well as at least one digit and punctuation character, e.g., 0-9, !@#$%^and*()_+|~-=\`{}[]:";'<>?,.or).
- Password Complexity should be enabled.
- Reversible encryption should be enabled.

3.3 Password Protection Standards:

3.3.1 Do not use the same password for EPS accounts as for any non-EPS account.

3.3.2 Do not share EPS passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential EPS information.

- Passwords should never be written down or stored on-line.
- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to any colleague, supervisor or manager unless specifically required to resolve a technical

problem in which case the password must be immediately changed once the problem is resolved

- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.

3.3.3 All users shall be trained to keep passwords confidential and not share it with anyone.

3.3.4 If someone demands a password, have them contact Information Technology.

3.3.5 Do not use the "Remember Password" feature of applications for any applications that contain Sensitive Information.

3.3.6 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including mobile devices such as BlackBerry, iPhone, iPads, etc.) without encryption.

3.3.7 If an account or password is suspected to have been compromised, report the incident to Information Technology team to have all passwords changed.

3.3.8 Password cracking or guessing may be performed on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

4. **Violation of Policy**

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

5. **Enforcement**

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.

b. Disciplinary action, up to and including termination.

c. Civil or criminal penalties as provided by law

6. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

7. **References**

This procedure refers to the section 9.2.4, 9.3.1, 9.4.3 of the ISO or IEC 27001 standard and Section 66-C of the IT Act 2008.

VII. Social Media Policy

1. **Purpose**

1.1 The purpose of this policy is to establish practical, reasonable and enforceable guidelines by which employees can conduct responsible, constructive social media engagement in both official and unofficial capacities.

1.2 Prepare EPS employees to utilize social media channels to help each other and the communities it serves.

1.3 Protect EPS employees from violating Municipal, State or Federal rules, regulations or laws through social media channels.

1.4 This policy supplements Acceptable Usage Policy.

2. **Scope**

EPS recognizes that emerging online collaboration platforms are fundamentally changing the way individuals and organizations communicate, and this policy is designed to offer practical guidance for responsible, constructive communications via social media channels for employees, when representing EPS.

3. **Responsibility**

All employees of EPS and third party users shall be responsible for adhering to and remain in compliance with the Information Security Management System (ISMS) in accordance with the policies and procedures.

4. **Policy Statement**

4.1 **Content Publishing and Confidentiality**

The following guidelines outline acceptable use for publishing content in social media. These guidelines apply to all social media communications, whether personal or company-sponsored. Effectively managing and protecting EPS's confidential information is a critical responsibility for all employees. Confidential information is an asset, whether we work in the field or the office. Failure to manage and protect confidential information correctly may result in legal or regulatory fines, damages to EPS's reputation and lost productivity. These guidelines are not inclusive of all possible content publishing scenarios and are not a substitute for good judgment.

4.1.1 Be aware of and follow all privacy and confidentiality guidelines in the EPS's Training.

4.1.2 DO NOT give away or use EPS confidential or proprietary information or that of any other person or company. For example, personnel information, upcoming (but unannounced) events, hiring or terminations, business plans, client information, etc.

4.1.3 DOES NOT comment on EPS confidential financial information such as future business operation or business plans.

4.1.4 DO NOT cite or reference clients, partners or suppliers without their written approval.

4.1.5 Identify yourself. Some individuals work anonymously, using pseudonyms or false screen names. EPS discourages that practice.

4.1.6 Be professional. If you have identified yourself as an EPS employee within a social website.

4.1.7 You are connected to your colleagues, managers and even EPS' client. You should ensure that content associated with you is consistent with your work at EPS.

4.1.8 Ask permission – to publish or report on conversations that are meant to be private or internal to EPS and when in doubt, always ask permission from the EPS legal department.

4.1.9 Speak in the first person when engaging in personal social media communications. Make it clear that you are speaking for yourself and not on behalf of EPS.

4.1.10 Use a disclaimer – If you publish personal social media communications EPS and it has something to do with the work you do or subjects associated with EPS, use a disclaimer such as this: "The postings on this site are my own and don't necessarily represent those of EPS."

4.1.11 Link back to the source – When you do make a reference to a customer, partner or supplier, where possible link back to the source.

4.1.12 Be aware of your association with EPS social media – If you identify yourself as an EPS employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and clients.

4.1.13 Use your best judgment – Remember that there are always consequences to what you publish. If you're about to publish something that makes you even the slightest bit uncomfortable, review the suggestions above and think about why that is. If you're still unsure, and it is related to EPS business, discuss it with your manager or simply do not publish it. You have sole responsibility for what you post to your blog or publish in any form of social media.

4.1.14 DO NOT use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the EPS workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory.

4.1.15 DO NOT conduct confidential business with a customer or partner business through your personal or other social media.

4.1.16 DO NOT register accounts using the EPS brand name or any other unregistered or registered trademarks.

5. **Violation of Policy**

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

5. Enforcement

Failure to comply with these policies may result in:

a. Withdrawal, without notice, of access to information and information resources.
b. Disciplinary action, up to and including termination.
c. Civil or criminal penalties as provided by law.

7. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

8. **References**

This procedure refers to the section 8.1.3 of the ISO or IEC 27001 standard and Section 43, 65, 66-A, 66-E, 66-F, 67, 67-A and B, 72, 72-A and 84-C of the IT Act 2008.

SECTION- 7

I. Physical Security Policy

1. Purpose

Controlling physical access to EPS's Information Resources is an important function of EPS's security program. This policy sets forth rules for establishing, controlling, and monitoring physical access to Information Resources.

2. Scope

All individuals within EPS responsible for Information Resources are within the scope of this policy.

3. Policy Statement

EPS' Information Resources must be physically protected in proportion to the criticality, sensitivity, or business importance of their function(s).

3.1 General

3.1.1 Physical security systems used to protect Information Resources must comply with all applicable regulations, including, but not limited to, building codes and fire prevention codes.

3.1.2 Each EPS employee with ongoing physical access to Information Resources must receive training on emergency procedures for the facility.

3.2 **Physical access management**

3.2.1 Appropriate facility entry controls shall be used to limit and monitor physical access to systems in the cardholder data environment.

3.2.2 Personnel, including full and part-time staff, contractors, vendors and service staff, should be granted access only to facilities and systems that are necessary for the fulfillment of their job responsibilities.

3.2.3 Requests for access to restricted facilities or restricted areas within a facility such as a data center, must be approved by the most senior onsite member of the IT or Information Security department.

3.2.4 Physical access to wireless access points, gateways, handheld devices, networking or communications hardware, and telecommunication lines shall be restricted.

3.3 **Protection of physical access cards and keys**

3.3.1 Personnel must not share or transfer access cards and to other individuals within or external to EPS.

3.3.2 Access cards and keys that are no longer needed must be returned to IT. Individuals that leave or change roles within EPS shall have all access rights revoked. Cards must not be transferred or reallocated to another individual, bypassing the return process.

3.3.3 Lost or stolen access cards and keys must be reported to Information Security within an hour of becoming aware of the loss.

3.4 **Monitoring and documentation for co-located data centers**

3.4.1 Physical access to all card holder data environment and other sensitive areas must be documented and monitored through CCTV cameras by appropriately trained personnel.

3.4.2 All co-located data centers that allow visitors must track visitor access with a sign in or sign out log.

3.4.3 Card access records and visitor logs for co-located data centers must be kept for no less than 90 days for routine review based upon the criticality of the Information Resources being protected.

4. **Violation of Policy**

All employees are obligated to report violations of this policy to the ISMS Head or Information Security officer (ISO) immediately. The ISMS Head must approve any exceptions to this policy in advance.

5. **Enforcement**

Failure to comply with this policy may result in:

a. Withdrawal, without notice, of access to information and information resources.
b. Disciplinary action, up to and including termination.
c. Civil or criminal penalties as provided by law.

6. **Document Owner and Approval**

The ISMS Head is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above. A current version of this document is available to all members of staff on the corporate intranet and is available with the ISO.

7. **References**

This procedure refers to the section 11 of the ISO or IEC 27001 standard and section 29, 43, 65, 66A, 66B, 66D, 67A, 66B, 66F, 70, 76, 87 of IT Act 2008.

Policies and Procedures Owner & Reviewer

Content	Policy Owner	Custodian	Reviewer
1. Corporate Affairs Policies	Sr. Manager – Corporate Affairs	Vice President – Analytics & Risk Governance	AVP – Corporate Affairs
2. Human Resource Policies	AVP – Human Resources	Vice President – Analytics & Risk Governance	Vice President – Human Resources
3. Information Technology Policies	General Manager – Information Technology	Vice President – Analytics & Risk Governance	Chief Operating Officer
Note: Policies related to the board are also reviewed by the Managing Director			

Policies and Procedures Sign-offs

Version	Description	Reviewed & Approved by	Date
V1.00	New Document	Mr. Narendra Deshmukh & Mr. Mani Mamallan	25-09-2017
V1.01	Revision: 1. Following policies requiring board approval have been reviewed and approved by the board. 1)AML 2)COC 3)Grievance 4)InfoSec 5)Risk mgmt. 6)POSH 7)Whistle-blower	Board	10-05-2018

	8)Anti-bribery – change in acceptance of gift by employees. 2. Annexure of high risk countries is replaced with the FATF		
V1.02	Revision: 1. Following policies requiring board approval have been reviewed and approved by the board. 1)COC 2)InfoSec 3)POSH	Board	02.11.2020
V3.1	Revision: 1. Following policies requiring board approval have been reviewed and approved by the board. 1)AML 2)COC 3)Grievance 4)InfoSec 5)Risk mgmt. 6)POSH 7)Whistle-blower 8)Anti-bribery – change in acceptance of gift by employees. 9) Version no. changed to 3.1 from 1.02 to be in line with all other EPS policies	Board	27.12.2022