Data Privacy and Protection Policy

Document No: ***IT-SEC-PG-030***

Revision No: 1.0

*Document Owner****: Information Technology***

*Document Classification****: Internal***

Released: 26th Apr 2016

DOCUMENT RELEASE NOTICE	
Document Title:	**Data Privacy and Protection Policy**
Document Code:	IT-SEC-PG-030
Version Draft:	1.0
Date of Release:	26th Apr 2016
Owner(s):	Information Technology
Author(s): Somak Shome	Date: 1st Apr 2016
Reviewer: Rajesh Jain	Date: 25th Apr 2016
Approved by: Sunder Raj Vijaynagar	Date: 26th Apr 2016

REVISION HISTORY				
Revision No.	**Release Date**	**Change Details (include Section No., if applicable)**	**Amended by**	**Approved by**
1.0	26th Apr 2016	First Release	-	Sunder Raj Vijaynagar

TABLE OF CONTENTS

1.0 Objective

The management of Srei (hereinafter referred to as "Srei") recognizes that privacy is of prime importance to employees, third party service providers and contractors, and therefore considers it with utmost sincerity while dealing with personal data.

The management also recognizes that exchange and use of substantial amount of client data is needed, both within and across borders, for client service and business purposes, and therefore considers it imperative to protect the confidentiality of clients' data.

This document outlines the policy which is adopted by Srei to manage its privacy and confidentiality needs and be compliant with data privacy and confidentiality legislations while conducting business with various countries globally.

Privacy

Srei recognizes and supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data; and Srei management shall ensure that all private information is used only as intended, and that precautions preventing misuse are both effective and appropriate.

Client Confidentiality

Srei recognizes and supports the right to confidentiality, including the rights of clients to control the dissemination and use of confidential information; and Srei management shall take reasonable efforts to ensure that all confidential client information maintained is accurate, timely, relevant, complete and is used only as intended, and that precautions preventing misuse are both effective and appropriate.

This document also outlines the data protection measures taken and incident management and escalation procedures in place in case of a privacy or confidentiality breach.

2.0 Scope

This policy applies to all employees, contractors, temporaries, consultants, and other workers working in Srei. All of these people are expected to be familiar with and fully in compliance with these policies.

3.0 Compliance with Local Laws and Regulations

Srei takes reasonable measures and precautions to maintain privacy and confidentiality of its internal firm data as well as confidential client data. It has put in place reasonable security practices and procedures in place to for protection of personal, sensitive and confidential data. The legal regime on IT Security and Data Protection in India has its roots to:

(a) Indian Contract Act, 1872 governing contractual obligations with respect to confidentiality and protection of data;

(b) The Information Technology Act, 2000, as amended from time to time, together with applicable rules;

(c) Indian Penal Code governing the consequences of the criminal breach of trust with respect to protection of data.

This policy provides a consistent standard for the protection of personal data and confidential client information. Srei takes responsibility for the development and enforcement of this policy, which is aimed at achieving compliance with the above laws, regulations and professional standards.

4.0 Srei Privacy Council

Head of Corporate Human Resources (HR), Chief Information Security Officer (CISO) and Heads of Internal Audit constitute the Srei Privacy Council. The Srei CISO is the custodian of privacy within Srei.

Srei Privacy Council reports to the Vice Chairman/CEO on matters related to privacy, and shall meet at least twice a year and review the following:

1. Level of policy enforcement
2. Various training and awareness programs

3. All non-compliance incidents and investigation reports
4. Customer requirements
5. New initiatives
6. Review of controls
7. Budgetary requirement; and
8. Current and emerging regulatory requirements.

5.0 Non Public Information (NPI)

Non Public Information (NPI) would encompass personal data, namely Personally Identifiable Information (PII), Personally Identifiable Financial Information (PIFI), and Personally Identifiable Health Information (PIHI) or Protected Health Information (PHI), and confidential client data as defined in this policy.

For Examples, refer to Annexure II

5.1 Personal Information

5.1.1 Definition

Personal information means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. Includes name, address, telephone number, address, Unique Identification Number, driver's license number, and personal business transaction details. The policy would also cover financial as well as statistical information of the clients of the network firms which are a part of the Srei.

5.1.2 Classification of Personal Information

Personally Identifiable Information (PII)

This refers to any information that identifies or can be used to identify, contact or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources or from which other personally identifiable information can be easily derived, including, but not limited to, name, address, phone number, fax number, e-mail address, financial profiles, Unique Identification Number, and credit card information. To the extent that unique information (which by itself is not Personally Identifiable Information) such as a personal profile, unique identifier, biometric information, and IP address is associated with Personally Identifiable Information, such unique information will also be considered Personally Identifiable Information. Personally Identifiable Information does not include information that is collected anonymously (i.e. without identification of the individual user) or demographic information not connected to an identified individual. In terms of P3P attributes, Personally Identifiable Information is: 1) physical contact or location information, 2) online contact or location information, 3) government-issued identifier, and 4) information about an individual's finances.

Personally Identifiable Financial Information (PIFI)

This refers to any information: (1) provided by a client to obtain credit, a loan or other financial product or service; (2) about a client resulting from a financial product or service transaction; or (3) obtained about a consumer in connection with providing a financial product or service. Examples of personally identifiable financial information include names, addresses, phone numbers, credit card account numbers, and Unique Identification Numbers, in both paper and electronic form.

Sensitive Personal Information (SPI)

"Sensitive personal information" means personal information that reveals race, ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, information that concerns health or sex life, or information relating to the commission of a criminal offense. As per the amended Information Technology Act, 2000, examples of sensitive personal information can be:

(i) password

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details

(iii) physical, physiological and mental health condition

(iv) sexual orientation

(v) medical records and history

(vi) biometric information

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Personally Identifiable Health Information (PIHI)

This refers to any oral or recorded information relating to the past/present/future physical/mental health of an individual, the provision of health care to an individual or the payment for health care. Protected Health Information is individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity. Individually identifiable information is a subset of health information that identifies or can be reasonably used to identify an individual. Elements that make information identifiable include, but are not limited to, name, address, phone number, date of birth, membership number and member ID.

5.2 Policy Guidelines

1. Srei supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences.
2. Srei supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.
3. Srei seeks consent from individuals for obtaining personal information and the individual agrees to share the same in writing.
4. Srei shall take reasonable efforts to ensure that all private information maintained is accurate, timely, relevant, and complete.
5. Srei shall make reasonable efforts to ensure that all private information is used only as intended, and that precautions preventing misuse are both effective and appropriate.
6. Management is responsible for establishing appropriate controls to ensure that private information is disclosed only to those who have a legitimate business need for such access.
7. Management must establish and maintain sufficient controls to ensure that information is free from a significant risk of undetected alteration.
8. Srei holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.
9. All the individuals granted access to the information shall sign a Non Disclosure agreement (NDA) with the company.
10. Private data shall not be kept in a form that permits identification of individuals / entities and for any longer than is necessary for the purposes for which the data was collected or for which it is further processed.
11. In case of changes to the Data Protection and Privacy Policy, an attempt to notify all individuals and entities involved must be promptly initiated. As a part of this notification, a summary shall be provided of the words that have changed and what these changes mean.
12. When building, testing, enhancing, and maintaining processing systems, developers must not use actual data. Instead, they must use fictional or sanitized data that preserves the essential characteristics of the data, but that does not relate to identifiable individuals / entities. In emergency situations where processing with actual data is required, use of such information shall be permitted under strict security procedures defined by Information Security.
13. Upon prior authorization by the sender of the data, and in accordance with the requirements of local laws and regulations, users will be provided with appropriate information on their personal data to confirm that it is accurate and up-to-date, as well as the right to request correction of their personal data.

14. All user access to processing systems and networks containing private data shall be logged so that every recent access to data can be traced to a specific user. Custodians of these systems and networks shall be responsible for the routine monitoring of such logs and the follow-up on potential security-relevant events.
15. When they are no longer needed, all copies of data, including those on backup tapes, must be irreversibly destroyed according to standards and procedures defined by the Information Security department. A document describing the data destroyed and the reasons for such destruction must be prepared for each destruction process, and promptly submitted to the relevant Owner. Permission to destroy data may be granted by only the Owner, and only if all legal retention requirements and related business purposes have been met.
16. Srei will take reasonable efforts to make its data protection and privacy policies and practices easily available to all concerned.

5.3 Employee Privacy Notice

"Srei, in its capacity as an employer, collects Employee Personal Information such as Date of Birth / Educational Details / Family Details / Address & Contact numbers / Past Work Experience etc and this personal data (also known as Non Public Information (NPI)) is stored and utilized for various internal purposes & for job-related purposes. By "job-related purposes" we mean legitimate purposes reasonably related to your employment with Srei, performance of your job responsibilities or Srei's ability to make services and benefits available to you as an employee (such as insurance coverage). This information is collected at the time of joining and further information is sought if the situation so demands. This information is gathered for the purpose of Human Resource, Compliance, Finance and Administration work and it is not further disseminated or used for any other purposes (e.g., Sales, Marketing). However, certain employee related information is furnished to regulatory authorities like Provident Fund Commissioner, Shops & Establishment Directorate etc for compliance purposes and may also be shared with legal authorities/police if needed.

Srei transfers your personal data internally for the purpose of payroll management, headcount, incentive, merit decisions, promotion and your participation in benefits programs such as Employee Health Insurance / Personal Accident Insurance / Statutory compliance related activities such as Provident Fund / Gratuity etc.

Employees who are eligible for healthcare, provident fund, social security benefits should be aware that for facilitating their participation in these programs, Srei shares a subset of the information with third parties that assist us in administering these programs. Those third parties receive the following information such as name, address, age, salary etc.

The information that we transfer includes your contact information such as Name, Address, Permanent Account Number (PAN), Existing Compensation and eligibility for participation in Srei benefits programs.

No sensitive Personnel information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs or trade union membership as defined in our Policy is sent outside Srei or cross-border.

You will be allowed to access your personal data and correct, amend or delete information where it is inaccurate. Company specific Human Resources (HR) personnel will assist you in accessing your personal data.

Our agreements with third parties require them to treat employee personal data in line with our Data Protection and Privacy Policy with regard to the protection and handling of their personnel information. In addition we use a variety of security mechanisms when communicating with them to protect your personnel information. However, if for any reason you are uncomfortable with the sharing of your personal data with these third-parties, you can prevent it by not enrolling or cancel the participation by contacting the Srei Privacy Council. However, no exception can be made for anyone with respect to sharing of information with regulatory authorities like Provident Fund Commissioner, Shops & Establishment Directorate etc for compliance purposes.

Employees who are eligible for healthcare, insurance, provident fund, social security benefits, should be aware that for facilitating their participation in these programs, Srei shares a subset of the information with third parties that assist us in administering these programs. Those third parties receive the following information such as name, address, age, base salary."

5.4 Employee Privacy Procedures

For New Hires (Entry Level and Lateral Hires)

1. Before or soon following the commencement of an employment relationship with Srei, employees and contractors will be presented with Srei Data Protection and Privacy Policy and the Employee Privacy Notice.
2. The HR Head will include copies of the Policy and Notice as part of their on-boarding process.

For Existing Employees

Employees will be provided with a copy of the Srei Data Protection and Privacy Policy and the Employee Privacy Notice when invited to participate in Srei affairs.

5.4.1 Employee Opt Out Process

Srei Privacy Council members and the Corporate HR Head in particular are the contacts for employees who wish to opt out of sharing of their personal information with third parties for direct marketing and non-essential services.

The Employee Opt Out Form will include the following categories:

a. Employee name
b. Employee ID number
c. Employee home address
d. Reporting Manager Name
e. Srei affiliate (third-party) company name
f. Description of the opt out request
g. Employee signature

1. Once an employee requests to opt out of the third party sharing before participation, the HR Head will send an email to the employee with an attachment of the Employee Opt out form. The form is to be completed in hardcopy and sent to the HR Head with all the requested information completed and the form signed.
2. The HR Head will verify the employee identity with the information provided in the Opt Out Form and will document the employee preference as described in the Employee Opt Out Log.
3. However, if an employee requests to opt out of the third party sharing after participation, the HR Head will contact the respective benefits administrators to inform the employee preference within five business days of receiving opt out request.
4. The benefits administrators will contact third-party and request them to remove the employee information from the data feeds.
5. The benefits administrators will provide the HR Head with an email message confirming the removal of the employee information from the communication to the third party.
6. HR Head will update the Employee Opt Out Log.

5.4.2 Employee Opt Out Log

The Employee Opt out Log will include the information obtained in the Opt out Form, and the confirmation dates from the benefit administrators.

5.4.3 Accessing and Updating Personal Data

Access Requests

1. Employees and Contractors are instructed to contact their HR Head with requests to access personal data beyond their default access that pertains to them.
2. When contacted by an employee with an access request, the HR Head will request the employee to submit their request in writing and specifically indicate the extent of the requested access (i.e., what is it that they want to review).
3. Upon receipt of a written access request, the HR Head will have to first determine whether one of the followings reasons but not limited to exist for denying or limiting the access request.

a. Interference with execution or enforcement of the law, including the prevention, investigation or detection of offenses or the right to a fair trial
b. Breaching a legal or other professional privilege or obligation
c. Prejudicing employee security investigations or grievance proceedings
d. Disclosure of personal information pertaining to other individual(s) where such references cannot be redacted
e. Prejudicing the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate re-organizations
f. Other circumstances in which the burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated.

4. If any of the exceptions may apply, the HR Head will consult with the Srei Privacy Council to determine the response to the access request.

Providing Access

5. If no reason exists for limiting the access of the employee to the record, the HR Head shall set an appointment with the employee and review the records with them in person. When holding the meeting, the HR Head will verify the employee's identity by requesting to see a photo ID. In cases where the HR Head cannot practically meet in person with the employee, the HR Head will make a copy of the records and arrange for the records to be sent to the employee's Manager. The Manager will meet with the employee and assist in the review of the records.
6. The HR Head will inform the Srei Privacy Council when providing employees with access to their records in response to an access request.

5.4.4 Employee Dispute Resolution Procedures

1. Employees, having a privacy concern or complaint, are to contact their Manager first and attempt to settle the issue at that level.
2. If the issue is not settled at the Manager level or if the Manager is one of the parties in dispute, it is to be raised to the HR Head.
3. When faced with a dispute that is raised by employees, the HR Head will:
    a. Respond directly within one business day, or
    b. Refer the employee to the Srei Privacy Council.
4. The Srei Privacy Council shall respond to the employee complaint within reasonable time of receiving.
5. If needed, the Srei Privacy Council shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances of provider of information expeditiously but within one month from the date of receipt of grievance.
6. The Srei Privacy Council shall be contacted to support the resolution of the complaint/concern if it involves the transfer of personal data to a different jurisdiction.
7. Principles of natural justice will be observed in dealing with grievances. All parties will have the opportunity to express their point of view, provide relevant information, and respond to the issues raised.
8. Clear and accurate written records must be kept of all interviews and the steps taken in the dispute resolution process, with a focus on factual information and objectiveness.

6.0 Confidential Client Data

6.1 Definition

"Confidential client information or data" refers to employees and Srei to professional secrecy, confidential and/or proprietary data relating specifically to a client's business, and other information identified as subject to professional secrecy, confidential and/or proprietary by a client. This information includes, but is not limited to, business procedures, marketing plans, merger and acquisition data, financial information, the names of the clients in certain cases, and descriptions of the work being performed. This information does not include publicly-available information or information in the public domain.

6.2 Policy Guidelines

1. Srei supports the right to confidentiality, including the rights of clients to control the dissemination and use of confidential information identified as subject to professional secrecy, confidential and/or proprietary by a client.
2. Srei supports domestic and international laws and regulations that seek to protect the confidentiality rights of such clients.
3. Srei shall take reasonable efforts to ensure that all confidential client information maintained is accurate, timely, relevant, and complete.
4. Srei shall make reasonable efforts to ensure that all confidential client information is used only as intended, and that precautions preventing misuse are both effective and appropriate.
5. Management is responsible for establishing appropriate controls to ensure that confidential client information is disclosed only to those who have a legitimate business need for such access.
6. Management must establish and maintain sufficient controls to ensure that information is free from a significant risk of undetected alteration.
7. All the individuals granted access to the information shall sign a Non-Disclosure agreement (NDA) with the company.
8. Confidential data shall not be kept in a form that permits identification of individuals / entities and for any longer than is necessary for the purposes for which the data was collected or for which it is further processed.
9. In case of changes to the Data Protection and Privacy Policy, an attempt to notify all individuals and entities involved must be promptly initiated. As a part of this notification; a summary shall be provided of the words that have changed and what these changes mean.
10. When building, testing, enhancing, and maintaining processing systems, developers must not use actual data. Instead, they must use fictional or sanitized data that preserves the essential characteristics of the data, but that does not relate to identifiable individuals / entities. In emergency situations where processing with actual data is required, use of such information shall be permitted under strict security procedures defined by Information Security.
11. Upon prior authorization by the sender of the data, and in accordance with the requirements of local laws and regulations, clients will be provided with appropriate information on their confidential data to confirm that it is accurate and up-to-date, as well as the right to request correction of their confidential data.
12. All user access to processing systems and networks containing confidential data shall be logged so that every recent access to data can be traced to a specific user. Custodians of these systems and networks shall be responsible for the routine monitoring of such logs and the follow-up on potential security-relevant events.
13. When they are no longer needed, all copies of data, including those on backup tapes, must be irreversibly destroyed according to standards and procedures defined by the Information Security department. A document describing the data destroyed and the reasons for such destruction must be prepared for each destruction process, and promptly submitted to the relevant Owner. Permission to destroy data may be granted by only the Owner, and only if all legal retention requirements and related business purposes have been met.

6.3 Privacy and Confidentiality Procedures

6.3.1 Monitoring of Internal Activities

1. In general terms, Srei does not engage in blanket monitoring of internal communications. It does, however, reserve the right at any time to monitor, access, retrieve, read, or disclose internal communications when a legitimate business need exists that cannot be satisfied by other means, the involved individual is unavailable and timing is critical to a business activity, there is reasonable cause to suspect criminal activity or policy violation, or monitoring is required by law, regulation, or third-party agreement.
2. At any time, Srei may log web sites visited, files downloaded, and related information exchanges over the Internet. It may record the numbers dialled for telephone calls placed through its telephone systems. Identified managers may receive reports detailing the usage of these and other internal information systems, and are responsible for determining that such usage is both reasonable and business-related.

3. At any time and without prior notice, Srei management reserves the right to examine archived electronic mail, personal computer file directories, hard disk drive files, and other information stored on the Srei information processing systems. This information may include personal data. Such examinations are typically performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the management of Srei information processing systems.

6.4 Data Protection

6.4.1 Data Integrity

1. Srei will take reasonable steps to ensure that the NPI processed is accurate, complete, reliable, and current by reviewing the information:
    a. When updating existing information (e.g., updating sales forecasts on a quarterly basis)
    b. When receiving new information (e.g., when receiving the proposed benefits and compensation for employees)
    c. When specific actions must be taken with the information, such as the creation of reports, reviews that are about to take place for specific decision making processes.
2. The data integrity steps to be taken in those circumstances include review for:
    d. Duplicate information.
    e. Missing data elements.
    f. Use of incorrect data elements.
    g. Including more identifiable information than necessary.
    h. Inaccurate use of identifiers (e.g., employee ID numbers).
    i. Inappropriate inclusion or exclusion of individuals for the intended process or purpose.

Distribution of NPI

1. Srei may be required to share NPI with governmental agencies or other companies assisting us in fraud prevention or investigation. Srei may do so when:
    a. Permitted or required by law; or,
    b. Trying to protect against or prevent actual or potential fraud or unauthorized transactions; or,
    c. Investigating fraud which has already taken place.
2. NPI will not be provided to these institutions for marketing purposes.
3. When transferring or receiving NPI across country borders, Srei shall comply with any relevant legal, professional or contractual requirements.

Onward Transfer Procedures

1. Srei will not provide a third party with the NPI without contractually committing that entity to appropriate protection of that information as described by these procedures.
2. All contracting with third parties that involves the processing of NPI on behalf of Srei will be reviewed by Srei Privacy Council to ensure appropriate level of compliance with the Policy and Jurisdiction specific Data Protection Law.
3. The Srei CISO will review the mechanism of transmission of NPI to a third party when first contracting with a new third party, and when changing the method of transmission with a third party.

Maintaining an Updated List of Third Parties

1. Srei Privacy Council will maintain a list of third parties with which contracts requiring compliance with Srei privacy requirements were implemented.
2. The list of Srei third parties will include the name of the company, the effective dates of the contracts, and the contract number.

Limiting the Information Shared with Third Parties

1. Srei will not provide a third party with more NPI than it deems as required to fulfil the task.

Inappropriate Disclosure

The notification procedure for inappropriate disclosure is defined under section Policy Violation of this document. If Srei gets notified or becomes aware of an inappropriate disclosure or protection of NPI or a practice of inappropriately disclosing NPI by a third party, the ISM will:

1. Stop the practice or disclosure
2. Document the event and the circumstances surrounding the event
3. Forward the report to Srei Privacy Council.
4. In consultation with Srei Privacy Council take steps to mitigate any negative impact that may result from the inappropriate disclosure, if practical.

6.4.2 General Security Procedures

Type of Data	Suggested Retention Period	Reason	Responsibility
Personnel files including records of application forms, interview notes disciplinary actions, Medical Leave	8 years	References and potential litigation	HR
Wages and salary records	8 years	Shops and establishment Act Regulations	HR
Income Tax Records	8 years		Finance
Confidential Client Information	As required		All business heads

1. All destruction/disposal of NPI would be done in accordance with applicable legislation, Applicable Data Protection Laws, Customer Master Service Agreement and pursuant to written retention policy/schedule. Records that have satisfied the period of retention would be destroyed or disposed off in an appropriate manner.
2. NPI (Soft & Hard copies) involved in any open investigation, audit or litigation shall not be destroyed or disposed off. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved
3. NPI (Soft & Hard copies) scheduled for destruction/disposal shall be secured against unauthorized or inappropriate access until the destruction/disposal of information is complete.
4. NPI (Soft & Hard copies) shall be destroyed or disposed of using a method that ensures information cannot be recovered or reconstructed. Appropriate methods for destroying/disposing of media are outlined in the Media Handling Procedure.
5. When NPI (Soft & Hard copies) is destroyed by an outside agency, that agency shall be contractually bound to observe the same security standards and considerations as those which apply to on-site disposal.

Web

1. Systems are designed in such a way that access and changes to NPI can be audited by date and user identification.
2. Access rights only provided to users who actually require access for stated purposes of collection or consistent purposes
3. Access control lists of systems containing personal information will be reviewed half-yearly by Srei CISO to identify and eliminate any outdated access privileges.
4. Audit trails are enabled for all system that contains NPI to reconstruct the following events:
    a. All individual user accesses to NPI.
    b. All actions taken by any individual with root or administrative privileges.
    c. Access to all audit trails.

d. Invalid logical access attempts.
e. Use of identification and authentication mechanisms.
f. Initialization of the audit logs.
g. Creation and deletion of system-level objects.

5. For each event we capture the following but not limited to
    a. User identification
    b. Type of event
    c. Date and time
    d. Success or failure indication
    e. Origination of event
    f. Identity or name of affected data, system component, or resource
6. We gather certain information automatically and store it in log files. This information includes Internet Protocol (IP) addresses, browser type, Internet Service Provider (ISP), referring/exit pages, operating system, date/time stamp, and click stream data.
7. Information is collected for analysis and statistical purposes. This information is not reported or used in any manner that would reveal NPI, and will not be released to any outside parties unless legally required to do so in connection with law enforcement investigations or other legal proceedings.

Remote Access

When required to remotely connect to a system that contains NPI we will:

2. Avoid directly accessing the NPI on the system if not required for performing the task at hand.
3. Avoid retaining any NPI from the system in any format (printing, electronic copies, image of the data, etc.) that is not necessary to fulfill a business need.

Enforcement Procedures

The Srei CISO either independently or along with Third-Party would conduct compliance reviews to ensure that the Data Protection and Privacy Policy and Procedures are effectively implemented.

Policy Violation

In the event of a violation of this policy, whether advertent or inadvertent, the following actions must be undertaken immediately:

1. Inform the Srei Privacy Council about the violation, giving all relevant details. Employees and Vendors may do so by contacting any member
2. The Privacy Council will arrange a confidential meeting with the employee(s) who are identified as allegedly failing to comply with the privacy requirements.
3. The Privacy Council will conduct a confidential investigation of the facts involved in the allegation.
4. A decision is taken by the Privacy Council, on which the CISS may escalate it to the relevant business head.

If confirmed of advertent violation by the employee:

1. The CISO will notify the HR Head and document the violation in the employee record as well as any other business unit specific operational reports.
2. In cooperation with the HR Head and business Head, the CISO will determine the sanction to impose on the employee.
3. Sanctions will be imposed as appropriate to the nature of the privacy violation. Imposed sanctions may range from a warning to termination of employment.

Queries and Complaints

For help with queries and complains about data privacy and protection, including compliance with local law, regulations and professional standards, reach out to the relevant contact, as given below:

Employees and Vendors

Employees and vendors should contact the Srei Privacy Council.

Clients and Prospective Clients

Clients and Prospective Clients should contact the business head, who in turn, will contact the Srei Privacy Council.

Annexure I - Identification of Team Members

Role	Member(s)
Srei Privacy Council	1. Chief Information Security Officer - Somak Shome 2. Head of Corporate HR – Rajesh Jain 3. Head of Internal Audit (SIFL) – Deepak Chatrath, and 4. Head of Internal Audit (SEFL) – Debshis Ghosh

Annexure II - Examples of Non Public Information

Examples of NPI:

Contact Information

1. Name
2. E-mail address
3. Mailing Address
4. Phone Number
5. Facsimile Number

Financial Information

1. Name of banking institution.
2. Card Holder Data like Primary Account Number (PAN), Cardholder Name, Service Code, and Expiration Date.
3. Sensitive Authentication Data like Full Magnetic Stripe, CVC2/CVV2/CID, PIN / PIN Block
4. Salary/Income
5. Bank Account Number
6. Tax Details
7. Credit History

Unique Identifiers

1. Unique Identification Number
2. Voter ID Card
3. Passport Number
4. Permanent Account Number
5. Date of Birth

Demographic Information

1. Age
2. Gender
3. Ethnicity
4. Marital Status

Medical Information

1. Medical History

2. Drug Screening
3. Health Insurance Provider

Employment Information

1. Employer Details
2. Business Contact Information
3. Background Check Results

Education Information

1. School(s) attended
2. Degrees/ Certifications conferred
3. Marks/Grade information

Legal Information

1. Criminal Record

Confidential Client Information

1. Business Plans and Procedures
2. Marketing Plans
3. Merger and Acquisition data
4. Financial Information
5. Names of the clients, in certain cases
6. Descriptions of work performed