VIRAJ	VIRAJ PROFILES LTD	Doc No. VPL:P:003:15
	PERSONALLY IDENTIFIABLE INFORMATION (PII) POLICY	Date : 22.07.2015

Page No : 01	1 of 2	Issue No :	01	Rev. No :	00

Scope : Employees of all Divisions in Group.

Purpose:

To safeguard the Personally Identifiable Information (PII) in concern of "Stake Holders" and to represent the Organization as Professional, growing Business Entity and to promote the professional culture in the Organization.

PERSONALLY IDENTIFIABLE INFORMATION (PII) POLICY

BEST PRACTICES

1. The Personally Identifiable Information (PII) Policy is created in response to concerns about collection, use, and accuracy of sensitive/personal data pertaining to individuals, such as PII. PII is data that can be used to distinguish or trace a person's identity, or any other personal information that can be linked to a specific individual. Examples of PII include: name, home mailing address, telephone number, social security number, home e-mail address, biometric identifiers (e.g., fingerprints), any unique identifying number or characteristic, and other information where it is reasonably foreseeable that the information will be linked with other personal identifiers of the individual.
2. In accordance with the VPL's PII Policy, improper treatment and handling of VPL correspondence and PII include but are not limited to posting of incorrect addresses, use of incorrect mailing labels, forwarding such to individuals who do not have a need to know the information, and inappropriately posting such to the internet.
3. Some PII is not "sensitive", such as the PII on a business card. Other PII is Sensitive Personally Identifiable Information (Sensitive PII), such as a Social Security number or alien number, and requires stricter handling guidelines because of the increased risk to an individual if compromised.
4. VPL defines "Sensitive" PII as personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
5. In every case, all members must ensure all personal information is not shared with anyone unless absolutely necessary in the performance of your duties. Do not discuss another individual's PII unless they have a need to know.
6. As Personally Identifiable Information (PII) will be maintained in Server/System. Authorized person from concerned Departments should not recreate/Modify/ change/delete/share the PII without the written consent of Department Head.

Prepared by:	Checked by: Deepak Bhave	Approved by: Neeraj Kochhar
HR Team	President - HR	Chairman & Managing Director

7. Do not create unnecessary or duplicate Sensitive PII. If you need to create duplicate copies of Sensitive PII to perform a particular task or project, delete or destroy it when no longer needed. Return incomplete forms containing PII to the individual for their retention or disposal at their discretion. There are only a few occasions when files must be kept. When this is the case, store it in a locked drawer, cabinet, cupboard, safe, or other secure container when you are not using it. Never leave Sensitive PII unattended and unsecured.
8. The Information and Life Cycle Management provides policies and procedures for administering VPL records, forms, and reports program as they relate to the life cycle management of both paper and electronic documents/data.
9. Do not dispose of PII in recycling bins or regular trash unless it has first been shredded.
10. When PII information must be mailed, ensure information is properly packaged and sent in accordance with the Mail Sensitive PII materials using an accountable commercial delivery service (e.g., DHL etc.). If any unit desires additional protection and accountability that may be afforded by using other than the Postal Service (e.g., commercial express carriers like FedEx, UPS etc., registered/certified mail), then the time and cost associated with the use of those systems shall be the responsibility of the VPL or the unit.
11. Do not email PII unless absolutely necessary. When you are emailing Sensitive PII, encrypt the e-mail using "message options" in outlook, or use an encrypted attachment with the password provided separately (e.g., by phone or in person). As a last resort, the password can be sent in a separate email, but never in the same email containing the attachment.
12. Contact Staff prior to faxing PII information to ensure someone is there and ready to receive it.
13. Loss of control, breach, compromise, unauthorized disclosure/ acquisition/access is considered a Privacy Incident where unauthorized users have access or potential access to PII. Report any unauthorized disclosures of personal information to your leadership immediately who should then contact VPL.

Note: This Policy comes w.e.f 01 April 2015 and may be changed / Modified/ updated on discretion of Management as per law of land.

Prepared by:	Checked by: Deepak Bhave	Approved by: Neeraj Kochhar
HR Team	President - HR	Chairman & Managing Director