**Safeguard Scooby-Snack**

Instructions:

Fill in the cell with the corresponding answer, be specific. Use this worksheet with your staff, like your Finance and Sales teams, to brainstorm what PPI (Private Personal Information) is collected in conjunction with your ITPP (Identity Theft Prevention Program). Remember, employees at many levels of your organization (not just you!) play a key role in identity theft deterrence and detection.

1. **Who** has access to PPI? (Name the persons taking, storing, holding, transferring PPI, and include third party contractors.)
2. **What** PPI is being collected? (Name the documents that are being collected.)
3. **Where** is the information being stored? (Name the physical devices that hold PII, emails, online locations, file cabinets, etc.)
4. **Why** is that PII collected? (To verify identity, establish credit, proof of income, proof of address, etc.)
5. **How** long are you storing this information? (How often is old PII sitting there before properly disposed of or stored?)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **What are you doing with PPI after you have collected it as part of your ITPP?** | | | | |
| **ITPP (Red Flags)** | **Current Practice** | **Protecting PPI** | **Safeguards Best Practice** | **Any Changes?** |
| 1. **Who** |  | **Take Stock** | Inventory computers, emails, mobile devices, flash drives, copiers, home computers, file cabinets, info that flows from websites and contractors for PII. |  |
| 2. **What** |  | **Scale Down** | Don’t collect it if you don’t need it and dispose of it once the business need is over. Limit employee access who don’t need to access PII. |  |
| 3. **Where** |  | **Lock It** | The PII must have physical security and/or electronic security, employee training and/or security by contractors from collection (start) to disposal (finish). |  |
| 4. **Why** |  | **Pitch It** | Burn, shred, or pulverize physical documents. Delete, erase, and wipe, digital storage when finished. |  |
| 5. **How** |  | **Plan Ahead** | Designate responsibility, disconnect from risky networks, and investigate vulnerabilities, notify someone to make changes |  |

Definitions:

* Take stock
  + Know what personal information you have in your files and on your computers
* Scale down
  + Keep only what you need for your business
* Lock it
  + Protect the information that you keep
* Pitch it
  + Properly dispose of what you no longer need
* Plan ahead
  + Reevaluate your plan and respond to security incidents
* Identity Theft Prevention Program
  + Written day-to-day operations that the business does to detect red flags. The plan should take steps to prevent identity theft and mitigate damage in the case of identity theft. Four elements of an ITPP: (1) identify red flags, (2) detect the red flags identified, (3) appropriate response plan, (4) update the plan to reflect new threats.
* Red Flag
  + Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft.
* Private Personal Information
  + PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to an individual. Some PII is not sensitive, such as that found on a business card. Other PII is Sensitive PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines.
    - Examples of Sensitive PII include: Social Security number (SSN), alien registration number (A-Number), or biometric identifier (e.g., fingerprint, iris scan). Other data elements such as a driver's license number, financial information, citizenship or immigration status, or medical information, in conjunction with the identity of an individual, are also considered Sensitive PII.