**Suggested minimum steps to be taken towards POPI Act compliance**

**After completing your risk assessments**

**Action Plan as at (date)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **What** | **Who** | **When** |
| 1 | Complete appointment letter for your Information Officer / Deputy Information Officer |  |  |
| 2 | Confirm which POPI Act compliance framework you are going to use and deploy the framework as per POPI Regulations |  |  |
| 3 | Develop or update your POPIA compliance policy |  |  |
| 4 | Develop or update any subsidiary policies referred to in the main POPIA policy; deploy the policies including required training   * CCTV Policy * Clean desk policy * Information Security including staff acceptable use and all aspects of IT management concerning personal information * Marketing including Social Media * Personal Information Quality * Physical Security * Records Management including retention periods * Staff compliance commitment * Other policies as required by your unique needs |  |  |
| 5 | Create or update POPIA-compliant privacy notices as required for different stakeholder groups   * Staff * Customers * Suppliers * Operators * Other third parties |  |  |
| 6 | Update all of your contracts referring to an appropriate privacy notice   * Business partners * Customers * Operators * Staff * Suppliers * When sharing PI |  |  |
| 7 | Deliver POPIA awareness training to your stakeholders (potentially multiple groups with different needs) on a periodic basis   * On induction of new staff * Periodically to all staff |  |  |
| 8 | Create or update your PAIA manual; include PAIA request handling process |  |  |
| 9 | Develop and implement your plan to work with the Information Regulator South Africa (IRSA)   * Monitor developments * Meet registration requirements * Meet reporting requirements * Deal with IRSA requests and instructions |  |  |
| 10 | Implement identified technical measures for improved personal information loss prevention, such as but not limited to   * Anti-Malware * Improved access control * Encryption * Asset protection measures (theft reduction) |  |  |
| 11 | Develop and implement your security compromise / incident response plan and test the plan regularly |  |  |
| 12 | Implement any other remedial actions to an acceptable level as identified in your POPIA compliance assessments |  |  |
| 13 | Build and maintain a log / record set of all your compliance activities |  |  |
| 14 | Develop and deploy an ongoing compliance plan |  |  |