# Annex C: Surveillance Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Surveillance Plan ISO/IEC 27001:2013/27701:2019** | | | | | | |
| **1**: Initial Audit  **2:** Surveillance 1 Audit  **3**: Surveillance 2 Audit  **4**: Recertification Audit | | | **Plan** | | | |
| **1**  **(202X)** | **2**  **(202X)** | **3**  **(202X)** | **4**  **(202X)** |
| **ISO/IEC 27001:2013/27701:2019 Clauses** | | | | | | |
| **4/5.2 Context of the organization** | | | | | | |
| **4.1/5.2.1** | Understanding the organization and its context | |  |  |  |  |
| **4.2/5.2.2** | Understanding the needs and expectations of interested parties | |  |  |  |  |
| **4.3/5.2.3** | Determining the scope of the information security and privacy management system | |  |  |  |  |
| **4.4/5.2.4** | Information security and privacy management system | |  |  |  |  |
| **5/5.3 Leadership** | | | | | | |
| **5.1/5.3.1** | Leadership and commitment | |  |  |  |  |
| **5.2/5.3.2** | Policy | |  |  |  |  |
| **5.3/5.3.3** | Organizational roles, responsibilities and authorities | |  |  |  |  |
| **6/5.4 Planning** | | | | | | |
| **6.1/5.4.1** | Actions to address risks and opportunities | |  |  |  |  |
| **6.2/5.4.2** | Information security and privacy objectives and planning to achieve them | |  |  |  |  |
| **7/5.5 Support** | | | | | | |
| **7.1/5.5.1** | Resources | |  |  |  |  |
| **7.2/5.5.2** | Competence | |  |  |  |  |
| **7.3/5.5.3** | Awareness | |  |  |  |  |
| **7.4/5.5.4** | Communication | |  |  |  |  |
| **7.5/5.5.5** | Documented information | |  |  |  |  |
| **8/5.6 Operation** | | | | | | |
| **8.1/5.6.1** | Operational planning and control | |  |  |  |  |
| **8.2/5.6.2** | Information security and privacy risk assessment | |  |  |  |  |
| **8.3/5.6.3** | Information security and privacy risk treatment | |  |  |  |  |
| **9/5.7 Performance evaluation** | | | | | | |
| **9.1/5.7.1** | Monitoring, measurement, analysis and evaluation | |  |  |  |  |
| **9.2/5.7.2** | Internal audit | |  |  |  |  |
| **9.3/5.7.3** | Management review | |  |  |  |  |
| **10/5.8 Improvement** | | | | | | |
| **10.1/5.8.1** | Nonconformity and corrective action | |  |  |  |  |
| **10.2/5.8.2** | Continual improvement | |  |  |  |  |
| **Control objectives and controls ISMS/PIMS** | | | | | | |
| A.5/6.2 | Information security and privacy policies | |  |  |  |  |
| A.6/6.3 | Organization of information security and privacy | |  |  |  |  |
| A.7/6.4 | Human resource security | |  |  |  |  |
| A.8/6.5 | Asset management | |  |  |  |  |
| A.9/6.6 | Access control | |  |  |  |  |
| A.10/6.7 | Cryptography | |  |  |  |  |
| A.11/6.8 | Physical and environmental security | |  |  |  |  |
| A.12/6.9 | Operations security | |  |  |  |  |
| A.13/6.10 | Communications security | |  |  |  |  |
| A.14/6.11 | System acquisition, development and maintenance | |  |  |  |  |
| A.15/6.12 | Supplier relationships | |  |  |  |  |
| A.16/6.13 | Information security and privacy incident management | |  |  |  |  |
| A.17/6.14 | Information security aspects of business continuity management | |  |  |  |  |
| A.18/6.15 | Compliance | |  |  |  |  |
| Annex A – PIMS-specific reference control objectives and controls | | | | | | |
| A.7.2 | Conditions for collection and processing | |  |  |  |  |
| A.7.3 | Obligations to PII principals | |  |  |  |  |
| A.7.4 | Privacy by design and privacy by default | |  |  |  |  |
| A.7.5 | PII sharing, transfer and disclosure | |  |  |  |  |
| Annex B – PIMS-specific reference control objectives and controls | | | | | | |
| B.8.2 | Conditions for collection and processing | |  |  |  |  |
| B.8.3 | Obligations to PII principals | |  |  |  |  |
| B8.4 | Privacy by design and privacy by default | |  |  |  |  |
| B.8.5 | PII sharing, transfer and disclosure | |  |  |  |  |
| 11. Additional requirements | | | | | | |
|  | Use of Logo | |  |  |  |  |
|  | List of documents included in the audited MS | |  |  |  |  |
| **Notes and comments:** | |  | | | | |

*For completed visits, mark “X” in the box for each clause/process covered.*

*For planned visits, mark “O” in the box for each clause/process to be covered.*