# Annex C: Surveillance Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Surveillance Plan ISO/IEC 27001:2022, ISO/IEC 27701:2019 and ISO/IEC 27017:2015** | | | | | | |
| **1**: Initial Audit  **2:** Surveillance 1 Audit  **3**: Surveillance 2 Audit  **4**: Recertification Audit | | | **Plan** | | | |
| **1**  **(202X)** | **2**  **(202X)** | **3**  **(202X)** | **4**  **(202X)** |
| **Clauses and Controls** | | | | | | |
| **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 management system | |  |  |  |  |
| **4.4/5.2.4** | Information security management system | |  |  |  |  |
| **5/5.3Leadership** | | | | | | |
| **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 | |  |  |  |  |
| **6.1.1/5.4.1.1** | General | |  |  |  |  |
| **6.1.2/5.4.1.2** | Information security risk assessment\*\* | |  |  |  |  |
| **6.1.3/5.4.1.3** | Information security risk treatment\*\* | |  |  |  |  |
| **6.2/5.4.2** | Information security objectives and planning to achieve them | |  |  |  |  |
| **6.3** | Planning of changes | |  |  |  |  |
| **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 | |  |  |  |  |
| **7.5.1/5.5.5.1** | General | |  |  |  |  |
| **7.5.2/5.5.5.2** | Creating and updating | |  |  |  |  |
| **7.5.3/5.5.5.3** | Control of documented information | |  |  |  |  |
| **8/5.6 Operation** | | | | | | |
| **8.1/5.6.1** | Operational planning and control | |  |  |  |  |
| **8.2/5.6.2** | Information security risk assessment | |  |  |  |  |
| **8.3/5.6.3** | Information security risk treatment | |  |  |  |  |
| **9/5.7 Performance Evaluation** | | | | | | |
| **9.1/5.7.1** | Monitoring, measurement, analysis and evaluation | |  |  |  |  |
| **9.2/5.7.2** | Internal audit | |  |  |  |  |
| **9.2.1** | General | |  |  |  |  |
| **9.2.2** | Internal audit program | |  |  |  |  |
| **9.3/5.7.3** | Management review | |  |  |  |  |
| **9.3.1** | General | |  |  |  |  |
| **9.3.2** | Management review inputs | |  |  |  |  |
| **9.3.3** | Management review results | |  |  |  |  |
| **10/5.8 Improvement** | | | | | | |
| **10.1/5.8.2** | Continual improvement | |  |  |  |  |
| **10.2/5.8.1** | Nonconformity and corrective action | |  |  |  |  |
| **Control objectives and controls** | | | | | | |
| **A.5** | Organizational controls | |  |  |  |  |
| **A 5.1/6 2.1.1/6.3.2.1** | Policies for information security | |  |  |  |  |
| **A 5.2/6.3.1.1** | Information security roles and responsibilities | |  |  |  |  |
| **A 5.3/6.3.1.2** | Segregation of duties | |  |  |  |  |
| **A 5.4/6.3.2.1** | Management responsibilities | |  |  |  |  |
| **A 5.5 /6.3.1.3** | Contact with authorities | |  |  |  |  |
| **A 5.6/6.3.1.4** | Contact with special interest groups | |  |  |  |  |
| **A 5.7** | Threat intelligence | |  |  |  |  |
| **A 5.8/6.3.1.5** | Information security in project management | |  |  |  |  |
| **A 5.9** | Inventory of information and other associated assets | |  |  |  |  |
| **A 5.10** | Acceptable use of information and other associated assets | |  |  |  |  |
| **A 5.11** | Return of assets | |  |  |  |  |
| **A 5.12/6.5.2.1** | Classification of information | |  |  |  |  |
| **A 5.13/6.5.2.2** | Labelling of information | |  |  |  |  |
| **A 5.14/6.5.3.3/ 6.10.2.1** | Information transfer | |  |  |  |  |
| **A 5.15** | Access control | |  |  |  |  |
| **A 5.16** | Identity management | |  |  |  |  |
| **A 5.17** | Authentication information | |  |  |  |  |
| **A 5.18** | Access rights | |  |  |  |  |
| **A 5.19** | Information security in supplier relationships | |  |  |  |  |
| **A 5.20/6.12.1.2** | Addressing information security within supplier agreements | |  |  |  |  |
| **A 5.21** | Managing information security in the information and communication technology (ICT) supply chain | |  |  |  |  |
| **A 5.22** | Monitoring, review and change management of supplier services. | |  |  |  |  |
| **A 5.23** | Information security for use of cloud services | |  |  |  |  |
| **A 5.24/6.13.1.1** | Information security incident management planning and preparation | |  |  |  |  |
| **A 5.25** | Assessment and decision on information security events | |  |  |  |  |
| **A 5.26/6.13.1.5** | Response to information security incidents | |  |  |  |  |
| **A 5.27** | Learning from information security incidents | |  |  |  |  |
| **A 5.28** | Collection of evidence | |  |  |  |  |
| **A 5.29** | Information security during disruption | |  |  |  |  |
| **A 5.30** | ICT refines for business continuity. | |  |  |  |  |
| **A 5.31/6.15.1.1** | Legal, statutory, regulatory and contractual requirements | |  |  |  |  |
| **A 5.32** | Intellectual property rights | |  |  |  |  |
| **A 5.33/6.15.1.3** | Protection of records | |  |  |  |  |
| **A 5.34** | Privacy protection of personal identifiable information (PII) | |  |  |  |  |
| **A 5.35/6.15.2.1** | Independent review of information security | |  |  |  |  |
| **A 5.36/6.15.2.3** | Compliance with policies, rules and standards for information security | |  |  |  |  |
| **A 5.37** | Documented operating procedures | |  |  |  |  |
| **CLD 8.1.5** | Removal of cloud service customer assets | |  |  |  |  |
| **A.6** | People controls | |  |  |  |  |
| **A 6.1** | Screening | |  |  |  |  |
| **A 6.2** | Terms and conditions of employment | |  |  |  |  |
| **A 6.3/6.4.2.2** | Information security awareness education and training | |  |  |  |  |
| **A 6.4** | Disciplinary process | |  |  |  |  |
| **A 6.5** | Responsibilities after termination or change of employment. | |  |  |  |  |
| **A 6.6/6.10.2.4** | Confidentiality or non-disclosure agreements | |  |  |  |  |
| **A 6.7** | Remote working | |  |  |  |  |
| **A 6.8** | Information security event reporting | |  |  |  |  |
| **CLD 6.3.1** | Cloud service customer | |  |  |  |  |
| **A.7** | Physical Controls | |  |  |  |  |
| **A 7.1** | Physical security perimeters | |  |  |  |  |
| **A 7.2** | Physical entry | |  |  |  |  |
| **A 7.3** | Securing offices, rooms and facilities | |  |  |  |  |
| **A 7.4** | Physical security monitoring | |  |  |  |  |
| **A 7.5** | Protecting against physical and environmental threats | |  |  |  |  |
| **A 7.6** | Working in secure areas | |  |  |  |  |
| **A 7.7/6.5.3.1/ 6.8.2.9** | Clear desk and clear screen | |  |  |  |  |
| **A 7.8** | Equipment siting and protection | |  |  |  |  |
| **A 7.9** | Security of assets off-premises | |  |  |  |  |
| **A 7.10/6.5.3.2** | Storage media | |  |  |  |  |
| **A 7.11** | Supporting utilities | |  |  |  |  |
| **A 7.12** | Cabling security | |  |  |  |  |
| **A 7.13** | Equipment maintenance | |  |  |  |  |
| **A 7.14** | Secure disposal or re-use of equipment | |  |  |  |  |
| **A.8** | Technological controls | |  |  |  |  |
| **A 8.1** | User end point devices | |  |  |  |  |
| **A 8.2** | Privileged access rights | |  |  |  |  |
| **A 8.3** | Information access restriction | |  |  |  |  |
| **A 8.4** | Access to source code | |  |  |  |  |
| **A 8.5** | Secure authentication | |  |  |  |  |
| **A 8.6** | Capacity management | |  |  |  |  |
| **A 8.7** | Protection against malware | |  |  |  |  |
| **A 8.8** | Management of technical vulnerabilities | |  |  |  |  |
| **A 8.9** | Configuration management | |  |  |  |  |
| **A 8.10** | Information deletion | |  |  |  |  |
| **A 8.11** | Data masking | |  |  |  |  |
| **A 8.12** | Data leakage prevention | |  |  |  |  |
| **A 8.13** | Information backup | |  |  |  |  |
| **A 8.14** | Redundancy of information processing facilities | |  |  |  |  |
| **A 8.15** | Logging | |  |  |  |  |
| **A 8.16** | Monitoring activities | |  |  |  |  |
| **A 8.17** | Clock synchronization | |  |  |  |  |
| **A 8.18** | Use of privileged utility programs | |  |  |  |  |
| **A 8.19** | Installation of software on operational systems | |  |  |  |  |
| **A 8.20** | Networks security | |  |  |  |  |
| **A 8.21** | Security of network services | |  |  |  |  |
| **A 8.22** | Segregation of networks | |  |  |  |  |
| **A 8.23** | Web filtering | |  |  |  |  |
| **A 8.24** | Use of cryptography | |  |  |  |  |
| **A 8.25** | Web filtering | |  |  |  |  |
| **A 8.26** | Use of cryptography | |  |  |  |  |
| **A 8.27** | Secure development life cycle | |  |  |  |  |
| **A 8.28** | Application security requirements | |  |  |  |  |
| **A 8.29** | Security testing in development and acceptance | |  |  |  |  |
| **A 8.30** | Outsourced development | |  |  |  |  |
| **A 8.31** | Separation of development, test and production environments | |  |  |  |  |
| **A 8.32** | Change management | |  |  |  |  |
| **A 8.33** | Test information | |  |  |  |  |
| **A 8.34** | Protection of information systems during audit testing | |  |  |  |  |
| **CLD 9.5.2** | Virtual machine hardening | |  |  |  |  |
| **CLD 12.1.5** | Administrator’s operation security | |  |  |  |  |
| **A.7.2** | Conditions for collection and processing | |  |  |  |  |
| **A 7.2.1** | Identify and document purpose | |  |  |  |  |
| **A 7.2.2** | Identify lawful basis | |  |  |  |  |
| **A 7.2.3** | Determine when and how consent is to be obtained | |  |  |  |  |
| **A 7.2.4** | Obtain and record consent | |  |  |  |  |
| **A 7.2.5** | Privacy impact assessment | |  |  |  |  |
| **A 7.2.6** | Contract with PII processors | |  |  |  |  |
| **A 7.2.7** | Joint PII controller | |  |  |  |  |
| **A 7.2.87** | Records related to processing PII | |  |  |  |  |
| **A.7.3** | Obligations to PII principals | |  |  |  |  |
| **A 7.3.1** | Determining and fulfilling obligations to PII principals | |  |  |  |  |
| **A 7.3.2** | Determining information for PII principals | |  |  |  |  |
| **A 7.3.3** | Providing information to PII principals | |  |  |  |  |
| **A 7.3.4** | Providing mechanism to modify or withdraw consent | |  |  |  |  |
| **A 7.3.5** | Providing mechanism to object to PII processing | |  |  |  |  |
| **A 7.3.6** | Access, correction and/or erasure | |  |  |  |  |
| **A 7.3.7** | PII controllers’ obligations to inform third parties | |  |  |  |  |
| **A 7.3.8** | Providing copy of PII processed | |  |  |  |  |
| **A 7.3.9** | Handling requests | |  |  |  |  |
| **A 7.3.10** | Automated decision making | |  |  |  |  |
| **A.7.4** | Privacy by Design and privacy by default | |  |  |  |  |
| **A 7.4.1** | Limit collection | |  |  |  |  |
| **A 7.4.2** | Limit processing | |  |  |  |  |
| **A 7.4.3** | Accuracy and quality | |  |  |  |  |
| **A 7.4.4** | PII minimization objectives | |  |  |  |  |
| **A 7.4.5** | PII de-identification and deletion at the end of processing | |  |  |  |  |
| **A 7.4.6** | Temporary files | |  |  |  |  |
| **A 7.4.7** | Retention | |  |  |  |  |
| **A 7.4.8** | Disposal | |  |  |  |  |
| **A 7.4.9** | PII transmission controls | |  |  |  |  |
| **A.7.5** | PII sharing, transfer and disclosure | |  |  |  |  |
| **A 7.5.1** | Identify basis for PII transfer between jurisdictions | |  |  |  |  |
| **A 7.5.2** | Countries and international organizations to which PII can be transferred | |  |  |  |  |
| **A 7.5.3** | Records of transfer of PII | |  |  |  |  |
| **A 7.5.4** | Records of PII disclosure to third parties | |  |  |  |  |
| **B.8.2** | Conditions for collection and processing | |  |  |  |  |
| **B 8.2.1** | Customer agreement | |  |  |  |  |
| **B 8.2.2** | Organization’s purposes | |  |  |  |  |
| **B 8.2.3** | Marketing and advertising use | |  |  |  |  |
| **B 8.2.4** | Infringing instruction | |  |  |  |  |
| **B 8.2.5** | Customer obligations | |  |  |  |  |
| **B 8.2.6** | Records related to processing PII | |  |  |  |  |
| **B.8.3** | Obligations to PII principals | |  |  |  |  |
| **B 8.3.1** | Obligations to PII principals | |  |  |  |  |
| **B.8.4** | Privacy by Design and privacy by default | |  |  |  |  |
| **B 8.4.1** | Temporary files | |  |  |  |  |
| **B 8.4.2** | Return, transfer or disposal of PII | |  |  |  |  |
| **B 8.4.3** | PII transmission controls | |  |  |  |  |
| **B.8.5** | PII sharing, transfer and disclosure | |  |  |  |  |
| **B 8.5.1** | Basis for PII transfer between jurisdictions | |  |  |  |  |
| **B 8.5.2** | Countries and international organizations to which PII can be transferred | |  |  |  |  |
| **B 8.5.3** | Records of PII disclosure to third parties | |  |  |  |  |
| **B 8.5.4** | Notification of PII disclosure requests | |  |  |  |  |
| **B 8.5.5** | Legally binding PII disclosures | |  |  |  |  |
| **B 8.5.6** | Disclosure of subcontractors used to process PII | |  |  |  |  |
| **B 8.5.7** | Engagement of a subcontractor to process PII | |  |  |  |  |
| **B 8.5.8** | Change of subcontractor to process PII | |  |  |  |  |
| **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.*