# Documents Mapping of ISO 27001, ISO 27017 and ISO 27018

| | | Mandatory Documents | | |
|---|---|---|---|---|
| **Document Name** | **Relevant clauses in the Standard** | **ISO 27001** | **ISO 27017** | **ISO 27018** |
| Information Security Policy | ISO/IEC 27001 5.2 and 5.3<br>ISO/IEC 27017 5.1.1<br>ISO/IEC 27018 5.1.1 and A.9.2 | x | x | x |
| Cloud Security Policy | ISO/IEC 27001 standard, clauses A.12.1.1, A.12.1.3, A.12.4.1, A.12.4.3, A.12.4.4, A.13.1.3, A.14.2.4<br>ISO/IEC 27017 6.1.1, 9.4.4, 12.1.3, 12.4.1, 12.4.4, 13.1.3, 18.1.2, CLD.6.3.1, CLD.9.5.1, CLD.9.5.2, CLD.12.1.5, CLD.12.4.5 and CLD.13.1.4<br>ISO/IEC 27018 12.4.1 and A.9.2 | | x | x |
| Policy for Data Privacy in the Cloud | ISO/IEC 27001 A.5.1.1, A.7.1.2, A.12.4.1, A.12.4.2, A.14.3.1, A.16.1.2 and A.18.1.4<br>ISO/IEC 27017 5.1.1, 12.4.1, 16.1.2<br>ISO/IEC 27018 5.1.1, 11.2.7, 12.4.1, 12.4.2, 12.4.3, 16.1.2, A.1.1, A.2.1, A.2.2, A.5.1, A.5.2, A.7.1, A.9.1, A.9.2, A.10.1 and A.10.2 | | x | x |
| Risk Assessment and Risk Treatment Methodology | ISO/IEC 27001 6.1.2, 6.1.3, 8.2, and 8.3 | x | | |
| Appendix 1 – Risk Assessment | ISO/IEC 27001 6.1.2 and 8.2 | x | | |
| Appendix 2 – Risk Treatment Table | ISO/IEC 27001 6.1.3 and 8.3 | x | | |
| Appendix 3 – Risk Assessment and Treatment Report | ISO/IEC 27001 8.2 and 8.3 | x | | |
| Statement of Applicability | ISO/IEC 27001 6.1.3 d)<br>ISO 27017, all clauses from sections 5 to 18 and Annex A<br>ISO 27018, all clauses from sections 5 to 18 and Annex A | x | x | x |
| Risk Treatment Plan | ISO/IEC 27001 6.1.3, 6.2 and 8.3 | x | | |
| (Annex A – controls) | | | | |

| | | | | |
|---|---|---|---|---|
| Bring Your Own Device (BYOD) Policy | ISO/IEC 27001 A.6.2.1, A.6.2.2 and A.13.2.1<br>ISO/IEC 27018 13.2.1 and A.9.2 | | | x |
| Mobile Device and Teleworking Policy | ISO/IEC 27001 A.6.2 and A.11.2.6<br>ISO/IEC 27017 11.2.6<br>ISO/IEC 27018 11.2.6 | | x | x |
| Confidentiality Statement | ISO/IEC 27001 A.7.1.2, A.13.2.4 and A.15.1.2<br>ISO/IEC 27017 7.1.2, 13.2.4 and 15.1.2<br>ISO/IEC 27018 7.1, 13.2.4, 15 and A.10.1 | x | x | x |
| Statement of Acceptance of ISMS Documents | ISO/IEC 27001 A.7.1.2<br>ISO/IEC 27017 7.1.2<br>ISO/IEC 27018 7.1 | x | x | x |
| Inventory of Assets | ISO/IEC 27001 A.8.1.1 and A.8.1.2<br>ISO/IEC 27017 8.1.1 and 8.1.2 | | x | x |
| Acceptable Use Policy | ISO/IEC 27001 A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3 and A.18.1.2 | x | | |
| Information Classification Policy | ISO/IEC 27001 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1 and A.13.2.3<br>ISO/IEC 27017 15.1.2 | | x | |
| Access Control Policy | ISO/IEC 27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1 and A.9.4.3<br>ISO/IEC 27017 6.1.1, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.1, 9.4.2 and 9.4.3<br>ISO/IEC 27018 6.1.1, 9.1, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.2, A.9.2, A.10.8, A.10.9 and A.10.10 | x | x | x |
| Password Policy (Note: it may be implemented as part of Access Control Policy) | ISO/IEC 27001 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 and A.9.4.3<br>ISO/IEC 27017 9.2.4<br>ISO/IEC 27018 9.2.1 and A.9.2 | | x | x |
| Policy on the Use of Cryptographic Controls | ISO/IEC 27001 A.10.1.1, A.10.1.2 and A.18.1.5<br>ISO/IEC 27017 10.1.1 and 18.1.5<br>ISO/IEC 27018 A.9.2 and A.11.1 | | x | x |

|  |  |  |  |  |
|---|---|---|---|---|
| Clear Desk and Clear Screen Policy (Note: it may be implemented as part of Acceptable Use Policy) | ISO/IEC 27001 A.11.2.8 and A.11.2.9 |  |  |  |
| Disposal and Destruction Policy (Note: it may be implemented as part of Operating Procedures for | ISO/IEC 27001 A.8.3.2 and A.11.2.7<br>ISO/IEC 27017 11.2.7<br>ISO/IEC 2701811.2.7, A.9.2, A.10.7 and A.10.13 |  | x | x |
| Procedures for Working in Secure | ISO/IEC 27001 A.11.1.5 |  |  |  |
| Operating Procedures for Information and Communication Technology | ISO/IEC 27001 A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2 and A.14.2.4<br>ISO/IEC 27017 11.2.7, 12.1.2, 12.1.3, 12.3.1, 12.4.1 and 12.4.3<br>ISO/IEC 27018 11.2.7, 12.1.4, 12.3.1, 12.4.1, 13.2.1, A.9.2, A.10.4, A.10.5, A.10.6 and A.11.2 | x | x | x |
| Change Management Policy (Note: it may be implemented as part of Operating Procedures for ICT) | ISO/IEC 27001 A.12.1.2 and A.14.2.4<br>ISO/IEC 27017 12.1.2<br>ISO/IEC 27018 A.9.2 |  | x | x |
| Backup Policy (Note: it may be implemented as part of Operating Procedures for ICT) | ISO/IEC 27001 A.12.3.1<br>ISO/IEC 27017 12.3.1<br>ISO/IEC 27018 A.12.3.1 and A.9.2 |  | x | x |
| Information Transfer Policy (Note: it may be implemented as part of Operating Procedures for ICT) | ISO/IEC 27001 A.13.2.1, A.13.2.2<br>ISO/IEC 27018 A.9.2, A.9.3, A.10.4 and A.10.5 |  |  | x |
| Secure Development Policy | ISO/IEC 27001 A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9 and A.14.3.1<br>ISO/IEC 27017 14.2.1 and 14.2.9<br>ISO/IEC 27018 A.9.2 | x | x | x |
| Appendix – Security Requirements Specification | ISO/IEC 27001 A.14.1.1<br>ISO/IEC 27017 14.1.1<br>ISO/IEC 27018 A.4.1 | x | x | x |

| | | | | |
|---|---|---|---|---|
| Supplier Security Policy | ISO/IEC 27001 A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1 and A.15.2.2<br>ISO/IEC 27017 7.2.2, 15.1.2, 15.1.3 and CLD.8.1.5<br>ISO/IEC 27018 7.2.2 and A.9.2 | | **x** | **x** |
| Appendix – Security Clauses for Clients, Suppliers and Partners | ISO/IEC 27001 A.7.1.2, A.14.2.7, A.15.1.2 and A.15.1.3,<br>ISO/IEC 27017 6.1.1, 6.1.3, 8.2.2, 9.2.1, 9.2.2, 9.2.4, 9.4.1, 9.4.4, 10.1.1, 11.2.7, 12.1.2, 12.1.3, 12.3.1, 12.4.1, 12.4.4, 12.6.1, 14.1.1, 14.2.1, 15.1.2, 15.1.3, 16.1.1, 16.1.2, 16.1.7, 18.1.1, 18.1.3, 18.1.5, 18.2.1, CLD.6.3.1 and CLD.8.1.5<br>ISO/IEC 27018 5.1.1, 6.1.1, 6.1.3, 9.2, 9.4.1, 10.1.1, 12.1.4, 12.3.1, 12.4.1, 16.1, 18.2.1, A.1.1, A.5.1, A.9.1, A.10.1, A.10.3, A.10.4, A.10.5, A.10.6, A.10.11, A.10.12 and A.11.1 | **x** | **x** | **x** |
| Incident Management Procedure | ISO/IEC 27001 A.7.2.3, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6 and A.16.1.7<br>ISO/IEC 27017 16.1.1, 16.1.2,16.1.7 and 18.1.2<br>ISO/IEC 27018 16.1.1 and A.9.2 | **x** | **x** | **x** |
| Appendix – Incident Log | ISO/IEC 27001 A.16.1.6 | | | |
| Disaster Recovery Plan | ISO/IEC 27001 A.17.1.2 | **x** | | |
| Training and Awareness Plan | ISO/IEC 27001 7.2 and 7.3 | | | |
| Internal Audit Procedure | ISO/IEC 27001 9.2 | | | |
| Appendix 1 – Annual Internal Audit | ISO/IEC 27001 9.2 | | | |
| Appendix 2 – Internal Audit Report | ISO/IEC 27001 9.2 | **x** | | |
| Appendix 3 – Internal Audit Checklist | ISO/IEC 27001 9.2<br>ISO/IEC 27017, all clauses from sections 5 to 18 and Annex A<br>ISO/IEC 27018, all clauses from sections 5 to 18 and Annex A | | **x** | **x** |
| Management Review Minutes | ISO/IEC 27001 9.3 | **x** | | |
| Procedure for Corrective Action | ISO/IEC 27001 10.1 | | | |
| Appendix – Corrective Action Form | ISO/IEC 27001 10.1 | **x** | | |