

# Statement of Applicability

Version 3.7  
Date feb 2022  
Classification: Public

## Reasons to include

| Section     | Information security control                           | Applicable | Implemented | Risk Analysis | Legal requirement |
|-------------|--|------------|-------------|---------------|-------------------|
| <b>A5</b>   | <b>Information security policies</b>                   |            |             |               |                   |
| <b>A5.1</b> | <b>Management direction for information security</b>   |            |             |               |                   |
| A5.1.1      | Policies for information security                      | Yes        | Yes         | X             |                   |
| A5.1.2      | Review of the policies for information security        | Yes        | Yes         | X             |                   |
| <b>A6</b>   | <b>Organization of information security</b>            |            |             |               |                   |
| <b>A6.1</b> | <b>Internal organization</b>                           |            |             |               |                   |
| A6.1.1      | Information security roles and responsibilities        | Yes        | Yes         | X             |                   |
| A6.1.2      | Segregation of duties                                  | Yes        | Yes         | X             |                   |
| A6.1.3      | Contact with authorities                               | Yes        | Yes         | X             |                   |
| A6.1.4      | Contact with special interest groups                   | Yes        | Yes         | X             |                   |
| A6.1.5      | Information security in project management             | Yes        | Yes         | X             |                   |
| <b>A6.2</b> | <b>Mobile devices and teleworking</b>                  |            |             |               |                   |
| A6.2.1      | Mobile device policy                                   | Yes        | Yes         | X             |                   |
| A6.2.2      | Teleworking  | Yes        | Yes         | X             |                   |
| <b>A7</b>   | <b>Human resource security</b>                         |            |             |               |                   |
| <b>A7.1</b> | <b>Prior to employment</b>                             |            |             |               |                   |
| A7.1.1      | Screening  | Yes        | Yes         | X             |                   |
| A7.1.2      | Terms and conditions of employment                     | Yes        | Yes         | X             |                   |
| <b>A7.2</b> | <b>During employment</b>                               |            |             |               |                   |
| A7.2.1      | Management responsibilities                            | Yes        | Yes         | X             |                   |
| A7.2.2      | Information security awareness, education and training | Yes        | Yes         | X             |                   |
| A7.2.3      | Disciplinary process                                   | Yes        | Yes         | X             |                   |
| <b>A7.3</b> | <b>Termination and change of employment</b>            |            |             |               |                   |
| A7.3.1      | Termination or change of employment responsibilities   | Yes        | Yes         | X             |                   |
| <b>A8</b>   | <b>Asset management</b>                                |            |             |               |                   |
| <b>A8.1</b> | <b>Responsibility for assets</b>                       |            |             |               |                   |
| A8.1.1      | Inventory of assets                                    | Yes        | Yes         | X             |                   |
| A8.1.2      | Ownership of assets                                    | Yes        | Yes         | X             |                   |
| A8.1.3      | Acceptable use of assets                               | Yes        | Yes         | X             |                   |
| A8.1.4      | Return of assets                                       | Yes        | Yes         | X             |                   |
| <b>A8.2</b> | <b>Information classification</b>                      |            |             |               |                   |
| A8.2.1      | Classification of information                          | Yes        | Yes         | X             |                   |
| A8.2.2      | Labelling of information                               | Yes        | Yes         | X             |                   |
| A8.2.3      | Handling of assets                                     | Yes        | Yes         | X             |                   |

|              |  |     |     |   |  |
|--------------|--|-----|-----|---|--|
| <b>A8.3</b>  | <b>Media handling</b>                                    |     |     |   |  |
| A8.3.1       | Management of removable media                            | Yes | Yes | X |  |
| A8.3.2       | Disposal of media  | Yes | Yes | X |  |
| A8.3.3       | Physical media transfer                                  | Yes | Yes | X |  |
| <b>A9</b>    | <b>Access control</b>                                    |     |     |   |  |
| <b>A9.1</b>  | <b>Business requirements of access control</b>           |     |     |   |  |
| A9.1.1       | Access control policy                                    | Yes | Yes | X |  |
| A9.1.2       | Access to networks and network services                  | Yes | Yes | X |  |
| <b>A9.2</b>  | <b>User access management</b>                            |     |     |   |  |
| A9.2.1       | User registration and de-registration                    | Yes | Yes | X |  |
| A9.2.2       | User access provisioning                                 | Yes | Yes | X |  |
| A9.2.3       | Management of privileged access rights                   | Yes | Yes | X |  |
| A9.2.4       | Management of secret authentication information of users | Yes | Yes | X |  |
| A9.2.5       | Review of user access rights                             | Yes | Yes | X |  |
| A9.2.6       | Removal or adjustment of access rights                   | Yes | Yes | X |  |
| <b>A9.3</b>  | <b>User responsibilities</b>                             |     |     |   |  |
| A9.3.1       | Use of secret authentication information                 | Yes | Yes | X |  |
| <b>A9.4</b>  | <b>System and application access control</b>             |     |     |   |  |
| A9.4.1       | Information access restriction                           | Yes | Yes | X |  |
| A9.4.2       | Secure log-on procedures                                 | Yes | Yes | X |  |
| A9.4.3       | Password management system                               | Yes | Yes | X |  |
| A9.4.4       | Use of privileged utility programs                       | Yes | Yes | X |  |
| A9.4.5       | Access control to program source code                    | Yes | Yes | X |  |
| <b>A10</b>   | <b>Cryptography</b>                                      |     |     |   |  |
| <b>A10.1</b> | <b>Cryptographic controls</b>                            |     |     |   |  |
| A10.1.1      | Policy on the use of cryptographic controls              | Yes | Yes | X |  |
| A10.1.2      | Key management   | Yes | Yes | X |  |
| <b>A11</b>   | <b>Physical and environmental security</b>               |     |     |   |  |
| <b>A11.1</b> | <b>Secure areas</b>                                      |     |     |   |  |
| A11.1.1      | Physical security perimeter                              | Yes | Yes | X |  |
| A11.1.2      | Physical entry controls                                  | Yes | Yes | X |  |
| A11.1.3      | Securing offices, rooms and facilities                   | Yes | Yes | X |  |
| A11.1.4      | Protecting against external and environmental threats    | Yes | Yes | X |  |
| A11.1.5      | Working in secure areas                                  | Yes | Yes | X |  |
| A11.1.6      | Delivery and loading areas                               | Yes | Yes | X |  |
| <b>A11.2</b> | <b>Equipment</b>   |     |     |   |  |
| A11.2.1      | Equipment siting and protection                          | Yes | Yes | X |  |
| A11.2.2      | Supporting utilities                                     | Yes | Yes | X |  |
| A11.2.3      | Cabling security   | Yes | Yes | X |  |
| A11.2.4      | Equipment maintenance                                    | Yes | Yes | X |  |
| A11.2.5      | Removal of assets  | Yes | Yes | X |  |

|              |   |     |     |   |  |
|--------------|---|-----|-----|---|--|
| A11.2.6      | Security of equipment and assets off-premises                   | Yes | Yes | X |  |
| A11.2.7      | Secure disposal or reuse of equipment                           | Yes | Yes | X |  |
| A11.2.8      | Unattended user equipment                                       | Yes | Yes | X |  |
| A11.2.9      | Clear desk and clear screen policy                              | Yes | Yes | X |  |
| <b>A12</b>   | <b>Operations security</b>                                      |     |     |   |  |
| <b>A12.1</b> | <b>Operational procedures and responsibilities</b>              |     |     |   |  |
| A12.1.1      | Documented operating procedures                                 | Yes | Yes | X |  |
| A12.1.2      | Change management   | Yes | Yes | X |  |
| A12.1.3      | Capacity management   | Yes | Yes | X |  |
| A12.1.4      | Separation of development, testing and operational environments | Yes | Yes | X |  |
| <b>A12.2</b> | <b>Protection from malware</b>                                  |     |     |   |  |
| A12.2.1      | Controls against malware  | Yes | Yes | X |  |
| <b>A12.3</b> | <b>Backup</b>   |     |     |   |  |
| A12.3.1      | Information backup  | Yes | Yes | X |  |
| <b>A12.3</b> | <b>Logging and monitoring</b>                                   |     |     |   |  |
| A12.4.1      | Event logging   | Yes | Yes | X |  |
| A12.4.2      | Protection of log information                                   | Yes | Yes | X |  |
| A12.4.3      | Administrator and operator logs                                 | Yes | Yes | X |  |
| A12.4.4      | Clock synchronisation   | Yes | Yes | X |  |
| <b>A12.5</b> | <b>Control of operational software</b>                          |     |     |   |  |
| A12.5.1      | Installation of software on operational systems                 | Yes | Yes | X |  |
| <b>A12.6</b> | <b>Technical vulnerability management</b>                       |     |     |   |  |
| A12.6.1      | Management of technical vulnerabilities                         | Yes | Yes | X |  |
| A12.6.2      | Restrictions on software installation                           | Yes | Yes | X |  |
| <b>A12.7</b> | <b>Information systems audit considerations</b>                 |     |     |   |  |
| A12.7.1      | Information systems audit controls                              | Yes | Yes | X |  |
| <b>A13</b>   | <b>Communications security</b>                                  |     |     |   |  |
| <b>A13.1</b> | <b>Network security management</b>                              |     |     |   |  |
| A13.1.1      | Network controls  | Yes | Yes | X |  |
| A13.1.2      | Security of network services                                    | Yes | Yes | X |  |
| A13.1.3      | Segregation in networks   | Yes | Yes | X |  |
| <b>A13.2</b> | <b>Information transfer</b>                                     |     |     |   |  |
| A13.2.1      | Information transfer policies and procedures                    | Yes | Yes | X |  |
| A13.2.2      | Agreements on information transfer                              | Yes | Yes | X |  |
| A13.2.3      | Electronic messaging  | Yes | Yes | X |  |
| A13.2.4      | Confidentiality or nondisclosure agreements                     | Yes | Yes | X |  |
| <b>A14</b>   | <b>System acquisition, development &amp; maintenance</b>        |     |     |   |  |
| <b>A14.1</b> | <b>Security requirements of information systems</b>             |     |     |   |  |

|              |  |     |     |   |  |
|--------------|--|-----|-----|---|--|
| A14.1.1      | Information security requirements analysis and specification           | Yes | Yes | X |  |
| A14.1.2      | Securing application services on public networks                       | Yes | Yes | X |  |
| A14.1.3      | Protecting application services transactions                           | Yes | Yes | X |  |
| <b>A14.2</b> | <b>Security in development and support processes</b>                   |     |     |   |  |
| A14.2.1      | Secure development policy  | Yes | Yes | X |  |
| A14.2.2      | System change control procedures                                       | Yes | Yes | X |  |
| A14.2.3      | Technical review of applications after operating platform changes      | Yes | Yes | X |  |
| A14.2.4      | Restrictions on changes to software packages                           | Yes | Yes | X |  |
| A14.2.5      | Secure system engineering principles                                   | Yes | Yes | X |  |
| A14.2.6      | Secure Development Environment   | Yes | Yes | X |  |
| A14.2.7      | Outsourced development   | Yes | Yes | X |  |
| A14.2.8      | System security testing  | Yes | Yes | X |  |
| A14.2.9      | System acceptance testing  | Yes | Yes | X |  |
| <b>A14.3</b> | <b>Test data</b>   |     |     |   |  |
| A14.3.1      | Protection of test data  | Yes | Yes | X |  |
| <b>A15</b>   | <b>Supplier relationships</b>  |     |     |   |  |
| <b>A15.1</b> | <b>Information security in supplier relationships</b>                  |     |     |   |  |
| A15.1.1      | Information security policy for supplier relationships                 | Yes | Yes | X |  |
| A15.1.2      | Addressing security within supplier agreements                         | Yes | Yes | X |  |
| A15.1.3      | ICT supply chain   | Yes | Yes | X |  |
| <b>A15.2</b> | <b>Supplier service delivery management</b>                            |     |     |   |  |
| A15.2.1      | Monitoring and review of supplier services                             | Yes | Yes | X |  |
| A15.2.2      | Managing changes to supplier services                                  | Yes | Yes | X |  |
| <b>A16</b>   | <b>Information security incident management</b>                        |     |     |   |  |
| <b>A16.1</b> | <b>Management of information security incidents &amp; improvements</b> |     |     |   |  |
| A16.1.1      | Responsibilities and procedures  | Yes | Yes | X |  |
| A16.1.2      | Reporting information security events                                  | Yes | Yes | X |  |
| A16.1.3      | Reporting information security weaknesses                              | Yes | Yes | X |  |
| A16.1.4      | Assessment of and decision on information security events              | Yes | Yes | X |  |
| A16.1.5      | Response to information security incidents                             | Yes | Yes | X |  |
| A16.1.6      | Learning from information security incidents                           | Yes | Yes | X |  |
| A16.1.7      | Collection of evidence   | Yes | Yes | X |  |
| <b>A17</b>   | <b>Information security aspects of BCM</b>                             |     |     |   |  |
| <b>A17.1</b> | <b>Information security continuity</b>                                 |     |     |   |  |
| A17.1.1      | Planning information security continuity                               | Yes | Yes | X |  |
| A17.1.2      | Implementing information security continuity                           | Yes | Yes | X |  |
| A17.1.3      | Verify, review and evaluate information security continuity            | Yes | Yes | X |  |
| <b>A17.2</b> | <b>Redundancies</b>  |     |     |   |  |

|              |   |     |     |   |   |
|--------------|---|-----|-----|---|---|
| A17.2.1      | Availability of information processing facilities                     | Yes | Yes | X |   |
| <b>A18</b>   | <b>Compliance</b>   |     |     |   |   |
| <b>A18.1</b> | <b>Compliance with legal and contractual requirements</b>             |     |     |   |   |
| A18.1.1      | Identification of applicable legislation and contractual requirements | Yes | Yes | X |   |
| A18.1.2      | Intellectual property rights  | Yes | Yes | X |   |
| A18.1.3      | Protection of records   | Yes | Yes | X | X |
| A18.1.4      | Privacy and protection of personally identifiable information         | Yes | Yes | X | X |
| A18.1.5      | Regulation of cryptographic controls                                  | Yes | Yes | X |   |
| <b>A18.2</b> | <b>Information security reviews</b>                                   |     |     |   |   |
| A18.2.1      | Independent review of information security                            | Yes | Yes | X |   |
| A18.2.2      | Compliance with security policies and standards                       | Yes | Yes | X |   |
| A18.2.3      | Technical compliance review   | Yes | Yes | X |   |