# Annex: ADO IT-security Questionnaire

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Questions**  *(Reference to the IT-Principle the question may apply)* | **Your answers**  **"x"** | **Your Score**  *Report below the points corresponding to your answers* | |
| **I.** | **Organization User and IT-Staff** | | | |
| **1** | **What percentage of your organization's employees work remotely? (mobile or fixed outside of the main physical locations)** | | | |
| *ref. to: IT-Principles 1, 3, 4* | | | |
| <20% |  | 0 |  |
| 20% - 40% |  | 1 |
| 40% - 60% |  | 1 |
| 60% - 80% |  | 2 |
| >80% |  | 2 |
| **2** | **What percentage of your organization's employees have access to private or confidential data?** | | | |
| *ref. to principles 1, 4* | | | |
| <20% |  | n/a |  |
| 20% - 40% |  | n/a |
| 40% - 60% |  | n/a |
| 60% - 80% |  | n/a |
| >80% |  | n/a |
| **3** | **Do non-IT employees have a culture that places importance on awareness and proactivity toward security?** | | | |
| *ref. to principles 3* | | | |
| Not at all |  | 2 |  |
| Somewhat |  | 1 |
| Very Much |  | 0 |
| **4** | **Do you have staff dedicated to different IT-tasks?** | | | |
| *ref. to principle 2* | | | |
| o   None of the above |  | 2 |  |
| o   IT-tasks are outsourced |  | 1 |
| o   A dedicated person(s) for IT |  | 1 |
| o   A dedicated person(s) for Privacy |  | 1 |
| o   A dedicated person(s) for IT-security |  | 0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **II.** | **IT Requirements & Compliance** | | | |
| **5** | **Does your organization have legal regulatory compliance requirements related to confidentiality and privacy (i.e. HIPAA, GDPR, etc.)?** | | | |
| *ref. to principle 7* | | | |
| No |  | 2 |  |
| Minimal |  | 1 |
| Yes |  | 0 |
| **6** | **Does your organization adhere to an IT protocol or security framework?** | | | |
| *ref. to principle 7* | | | |
| o   No |  | 2 |  |
| o   Information Security Manual (ISM) |  | 1 |
| o   COBIT |  | 1 |
| o   ITIL |  | 1 |
| o   ISO/IEC 27000 |  | 0 |
| o   Other |  | 1 |
| **7** | **Select the processes and/or policies your organization has implemented to mitigate risks and respond to incidents:** | | | |
| *ref. to principle 7* | | | |
| o   None of the below |  | 2 |  |
| o   None of the below but plan on developing in next 12 months |  | 2 |
| o   Incident response plan |  | 1: if only this answer is selected  0: if two answers or more are selected |
| o   Information security policy or plan |  | 1: if only this answer is selected  0: if two answers or more are selected |
| o   Business continuity and disaster recovery plans |  | 1: if only this answer is selected  0: if two answers or more are selected |
| o   Information security strategy |  | 1: if only this answer is selected  0: if two answers or more are selected |
| o   Other governance documents |  | 1: if only this answer is selected  0: if two answers or more are selected |
| **8** | **How do you stay up to date on IT-security? (Several options possible)?** | | | |
| *ref. to principles 5, 7* | | | |
| o Ad-hoc |  | 2 |  |
| o In person training |  | 0 |
| o Rely on a service provider or consultant |  | 0 |
| o Internet sources |  | 1 |
| o Media |  | 1 |
| o Edx or similar online courses |  | 1 |
| o  Books |  | 1 |
| o  Other |  | 2 |
| **III.** | **Data** | | | |
| **9** | **How confident are you in your capacity to protect athlete information?** | | | |
|  | *ref. to principle 1* | | | |
|  | o 1 (no confidence) |  | 2 |  |
| o 2 (little confident) |  | 2 |
| o 3 (somewhat confident) |  | 1 |
| o 4 (confident) |  | 1 |
| o 5 (very confident) |  | 0 |
| **10** | **Do you inform in writing your providers/end-users (e.g. laboratories) with which of your staff they are authorized to share confidential and/or private information?** | | | |
| *ref. to principles 4, 5* | | | |
| Not at all |  | 2 |  |
| Somewhat |  | 1 |
| Very Much |  | 0 |
| **11** | **What percentage of your organization's data is considered to be confidential?** | | | |
| *ref. to principle 1* | | | |
| <20% |  | N/A |  |
| 20% – 40% |  | N/A |
| 40% - 60% |  | N/A |
| 60% - 80% |  | N/A |
| >80% |  | N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IV.** | **Complexity of Technology Environment** | | | |
| **12** | **Does your organization have two or more data centers?** | | | |
| *ref. to principles 2, 5, 6* | | | |
| No |  | N/A |  |
| Yes |  | N/A |
| **13** | **Do people use personal devices to access corporate systems and data?** | | | |
| *ref. to principles 3, 5, 6* | | | |
| No |  | N/A |  |
| Yes |  | N/A |
| **V.** | **Business Security Requirement** | | | |
| **14** | **How would you rate your level of documented IT-processes?** | | | |
| *ref. to principles 5, 6, 7* | | | |
| o Basic - Undocumented and dynamic change processes. |  | 2 |  |
| o Repeatable - Some processes are repeated. |  | 2 |
| o Fixed - A set of defined and documented standard processes. |  | 1 |
| o Managed - benchmarked processes, effective management controls and adaptation without losing quality. |  | 1 |
| o Optimized - focus is on continuous improvement and optimization. |  | 0 |
| **15** | **Do information security risks get marginalized or neglected in favor of end-user ease of use?** | | | |
| *ref. to principle 3* | | | |
| Not at all |  | 0 |  |
| Somewhat |  | 1 |
| Very Much |  | 2 |
| **16** | **What is your organization's information security risk tolerance level?** | | | |
| *ref. to principles 3, 5, 6* | | | |
| Low risk tolerance |  | 0 |  |
| Medium risk tolerance |  | 1 |
| High risk tolerance |  | 2 |
| **17** | **In the past 12 Months, has your organization suffered a security incident?** | | | |
| *ref. to principles 2, 5, 6* | | | |
| o   No incidents |  | N/A |  |
| o   Information not available |  | N/A |
| o   Compromise of an email or system account |  | N/A |
| o   Loss or unauthorized modification of data |  | N/A |
| o   Ransomware or other malware infection |  | N/A |
| o   Hacker attacks |  | N/A |
| o   Successful exploitation of a phishing email |  | N/A |
| o   Unauthorized system modification by a trusted user |  | N/A |
| o   Phishing or other attack via a compromised partner agency |  | N/A |
| o   Other |  | N/A |
| **18** | **Do you have an active Cyber Security plan/ program/ strategy?** | | | |
| *ref. to principles 3, 5, 6, 7* | | | |
| o   No |  | 2 |  |
| o   Partly/ in progress |  | 1 |
| o   Yes |  | 0 |
| **19** | **Is security and privacy discussed regularly at the Management/ Board Level?** | | | |
| *ref. to principle 3* | | | |
| o   No |  | 2 |  |
| o   Sometimes |  | 1 |
| o   Yes |  | 0 |
| **20** | **How often is information security and privacy reported to the Management and/or Board?** | | | |
| *ref. to principle 3* | | | |
| o Never |  | 2 |  |
| o Ad-hoc based on requests for information |  | 2 |
| o Annually |  | 1 |
| o Quarterly |  | 1 |
| o Monthly |  | 0 |
| o Weekly |  | 0 |
| **21** | **What would help you to improve the IT-security level of your organization?** | | | |
| *ref. to principle 7* | | | |
| o Board Awareness |  | N/A |  |
| o Increased funding or Government services |  | N/A |
| o Staff education programs |  | N/A |
| o Conferences on security and privacy |  | N/A |
| o Threat alerts |  | N/A |
| o Guidelines and advice |  | N/A |
| o  Other |  | N/A |

|  |  |
| --- | --- |
|  | |
| **Basic Level** | **Your score** |
| 21-30 |  |
| **Intermediate Level** |
| 11-20 |
| **Advanced Level** |
| 0-10 |