# Guidance for reporting Research Question, PICO elements, Search string, Inclusion and Exclusion criteria

This Document has two tables (shown with an example) to be included in your Interim report and Final report (updated Final Report version based on feedback received on Interim report). Populate both tables with content relevant to your group work and provide a number and caption for each table. For your final report, add the table information in the List of Tables along with a List of Figures and Table of Contents at the beginning of the report after Title page.

**Note:**

* Replace the Text in Blue colour with content relevant to your project.
* Delete Red text before adding these tables to the report.

|  |  |
| --- | --- |
| Table 1: PROTOCOL Part 1: RESEARCH QUESTION with PICO ELEMENTS | |
| Elements | Example content |
| Topic:  Write your general topic. | Comparison of signature-based detection method and anomaly-based detection method in intrusion detection systems (IDS) |
| Research Question:  Write down your research question. | How does the signature-based detection method compare to the anomaly-based detection method in detecting attacks to an intrusion detection system? |
| Context:  State the context for your research question. | Cybersecurity and intrusion detection systems (IDS). |
| Population:  State the population to which the intervention of your research question is applied (who or what might change based on the intervention?). | Intrusion detection systems |
| Intervention:  State the intervention (treatment) to which the intervention of your research question is applied. | Intrusion detection methods |
| Comparison:  State the comparison between subsets of the population that receive different treatments. | Signature-based detection method vs Anomaly-based detection method |
| Outcome:  State the outcome that the comparison between subsets of the population that receive different treatments will consider. | A list of similarities and differences in how the signature-based detection method compares to the anomaly-based detection method in detecting attacks to an intrusion detection system. |

|  |  |
| --- | --- |
| TABLE 2: PROTOCOL Part 2 – SEARCH STRINGS and INCLUSION/EXCLUSION CRITERIA | |
| Elements | Example Content |
| Search string:  Write your search string, on one line, after testing it using the IEEEXplore command search window. | ("signature-based" AND "anomaly-based" AND "intrusion detection system") |
| No. of papers:  Write the number of papers identified by your search string when you test it using the IEEEXplore command search window. | 85 |
| Inclusion Criteria:  Write up to five inclusion criteria. | 1. Studies that compare the accuracy of the signature-based detection method and the anomaly-based detection method. 2. Studies that are published in peer-reviewed journals or conference proceedings. 3. Studies that are written in English. |
| Exclusion Criteria:  Write up to five exclusion criteria. | 1. Studies that focus on detection methods not listed in the RQ. 2. Duplicated papers (where the same authors write a conference and journal paper, just choose most comprehensive). 3. Book chapters and PowerPoint slides, incomplete papers are excluded. |