These security requirements are extracted from the previous course solutions. Do they correspond to the “criteria of good requirements”? If not, please refine them so that they would correspond to the “criteria of good requirements”.

Do not write like this

• Ambiguity – or
  – The ERIS system shall also be able to generate visible or audible caution or warning signal for the attention of security or business analyst

• Multiple requirements – and, or, with, also
  – The warning indicator shall light up when an ERIS intrusion is detected and the current Football Federation Employees workspace or Game report data shall be saved

[Alexander and Stevens, 2002]
Do not write like this

• Let-out clauses
  *if, when, except, unless, although, always*
  - The fire alarm shall always be sounded *when* the smoke in Football Federation building is detected, *unless* the alarm is being tested *when* the antivirus is deployed

• Long rumpling sentences
  - Provided that the designated Game report input signals from the specified mobile devices are received in the correct order by the way which the ERIS is able to differentiate the designators, the security solution should comply with the required framework to indicate the desired security states

[Alexander and Stevens, 2002]
Do not write like this

• Speculation
  *usually, generally, often normally, typically*
  – *Umpires and Team Representatives normally require early indication of intrusion into ERIS*

• Vague, undefinable terms
  *user-friendly, versatile, approximately, as possible, efficient, improved, high-performance, modern*
  – *Security-related messages should be versatile and user-friendly*
  – *The OK status indicator shall be illuminated as soon as possible after ERIS security self-check is completed*

[Alexander and Stevens, 2002]
Do not write like this

• Wishful thinking

100% reliable/ safe/ secure. Handle all unexpected failures. Please all users. Run on all platforms. Never fail. Upgrade to all future situations.

– The gearbox shall be 100% secure in normal operation
– The network shall handle all unexpected errors without crashing

[Alexander and Stevens, 2002]
Do not write like this

• System design:
  no *names of components, materials, software objects/procedures, database fields*
    – The antenna shall be capable of receiving FM signals, *using a copper core with nylon armoring and a waterproof hardened rubber shield*

• Mix of requirements and design:
  no references to *system, design, testing, or installation*
    – The user shall be able to view the current selected channel number which shall be displayed in 14pt Swiss type on an LCD panel tested to standard 657-89 and mounted with shockproof rubber washers

[Alexander and Stevens, 2002]
Good requirements

• Use simple direct sentences
  – Security analyst should be able to view ERIS status.

• Use a limited vocabulary
  – Security analyst should be able to change the infected ERIS component in less than 12 h; or
  – Security analyst should be able to reconfigure the infected ERIS component in less than 12 h

[Alexander and Stevens, 2002]
Good requirements

• Identify the type of user who wants each requirements
  – The Football Federation Employee shall be able to …

• Focus on stating result
  – … view game reports …

• Define verifiable criteria
  – … after 2 h after the game.

[Alexander and Stevens, 2002]
Criteria for writing good requirements

- **What**, not how (external observability)
  - Avoid premature design or implementation decisions
- **Understandability, clarity** (not ambiguous)
- **Cohesiveness** (one thing per requirement)
- **Testability**
  - Somehow possible to test or validate whether the requirement has been met, clear *acceptance criteria*
  - Often requires quantification, this is more difficult for security than e.g. for performance
    - *The response time of button press should be max 2 s.*
    - *The security of function F should be at least 99.9%*
Refine them so that they would correspond to the “criteria of good requirements”.

SecReq.1: Automation of the receipt generation or checking fuel capacity and sold amount of fuel as often as possible.

SecReq.2: Cash registers must compare data about company car / employee ID to ERP and give warning if there is a mismatch.

SecReq.3: IT department must follow security advisories and patch vulnerable systems, given that solutions are available.

SecReq.4: Implement at least two workplaces for serving customers in filling station.

SecReq.5: Appropriate trainings shall be provided to all employees of PowerAB with regards to information security awareness.

SecReq.6: Database backup server accounts should be sufficiently protected against unauthorized access.

SecReq.7: IT managers should plan the placement of card readers near 24/7 cameras, which are monitored from a security officer.

SecReq.8: Have a backup server for redundancy and push uptime to near 100%.

SecReq.9: Using better security applications.

SecReq.10: The firewall should continuously monitor the communication channel and block suspicious software while transmitting message from account department to personnel department.

• Use **simple direct sentences**
• Use a **limited vocabulary**
• Identify the **type of user who wants requirements**
  – Focus on stating **result**
  – Define **verifiable criteria**
Refine them so that they would correspond to the “criteria of good requirements”.

**SecReq.1**: Automation of the receipt generation or checking fuel capacity and sold amount of fuel as often as possible.

**SecReq.1.1**: Fuel system should check fuel capacity

**SecReq.1.2**: Receipt system should generate receipts

**SecReq.2**: Cash register computer must compare data about company car / employee ID to ERP and give warning if there is a mismatch.

**SecReq.2**: Cash register computer should notify attendant about mismatch between car number and employee ID

**SecReq.3**: IT department must follow security advisories and patch the vulnerable systems, given that solutions are available.

**SecReq.3**: IT department should patch PowerAB software systems
Refine them so that they would correspond to the “criteria of good requirements”.

**SecReq.4**: Implementing at least two workplaces for serving customers in filling station.

**SecReq.5**: Appropriate trainings shall be provided to all employees of PowerAB with regards to information security awareness.

**SecReq.6**: Database backup server accounts should be sufficiently protected against unauthorized access.

**SecReq.4**: Management should create two workplaces for serving customers.

**SecReq.5**: Management should provide security awareness training for the PowerAB employees.

**SecReq.6**: Database backup server accounts should be protected against unauthorized access.
Refine them so that they would correspond to the “criteria of good requirements”.

SecReq.7: IT managers should plan the placement of card readers near 24/7 cameras, which are monitored from a security officer.

SecReq.7: Security officer should monitor the card readers.

SecReq.8: Have a backup server for redundancy and push uptime to near 100%.

SecReq.8: The backup server should ensure the uptime of 99.1%.
Refine them so that they would correspond to the “criteria of good requirements”.

**SecReq.9**: Using better security applications.

**SecReq.9**: “I do not know how to fix it”

**SecReq.10**: The firewall should continuously monitor the communication channel and block suspicious software while transmitting message from account department to personnel department.

**SecReq.10.1**: The firewall should monitor the communication channel.

**SecReq.10.2**: The firewall should block the untrusted software.

*Explain “untrusted”!*