Assignment 3. Security plan

A Security Plan is an obligation for organizations due to the EU cyber defence policy, especially after the publication of NIS2. In this assignment, each group must define and propose a security plan that fulfils this policy.

The number of components that should be covered in the proposed security plan varies depending on the members of the group.

As a basis, a General Security Policy is mandatory (however, shown at the table below). Additionally, the group must create:

Number of group members	General Security Policy	Assets inventory	Risk management	Incident management	Technical and physical (if applicable) controls
1	X	X	X[1]		
2	X	X	X[1]	X[2]	
3	X	X	X[1]	X[2]	X[3]

[1] At least two risks
[2] At least two incidents
[3] At least two controls

This is a group work, not a singular activity! As so, consistency between the parts must be observed. As an example, if risk management encompasses earthquakes, that should be addressed both in incident management and in technical and physical controls.

The scenario to be employed is as follows:

A single student from each group must upload the report in PDF format to Moodle by the date specified therein. The name of the report must comply with the format

<teacher_acronym>_<student_1_number>[_<student_2_number>[_<student_3_number>]].pdf

The group should indicate in the document each student's contribution to each part of the security plan.

Suggested but not compulsory templates can be downloaded from Moodle.

Evaluation criteria:

Report: 70%
Individual questions for each group member: 30%
A classification will only be launched if both parts of the evaluation are satisfied