

Module D4 – Local Session 3 (Cybersecurity II)

Instructions for students

Task 1 – Create a Security Policy

- ➔ Individual work
- ➔ Time allocated: around 80 min
- ➔ Setting: At the beginning, please decide for which company situation (e.g., industry, environment such as laboratory, location such as field work,...) you want to create the information security policy. Choosing the same company and setting the tasks in the previous local session is suggested.

Objectives and Conversion:

1. Become aware of information security and how to protect (in general) different levels of data in your organization
2. You will be able to assess and classify data based on a (pre-defined) template – **the Harvard information security policy** – check to moodle for the word document.

Relevant sources: see provided presentation in lecture 3 -- Coaching Session III.pptx
or below the excerpt of the slide deck with the selected cases.

Excerpt presentation:

Coaching

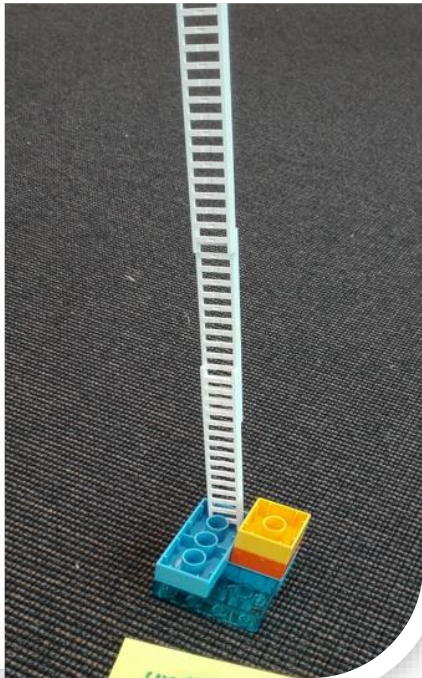
The theme is "be protected"

You have one individual task described in the following, which you should work during your coaching session.

The aim is that you

- a) **"be protected"** in terms of developing a tailored control – an Information Security Policy
- b) get an experience of how to create such a policy based on the NIST "Information Security Handbook" and the selected example from Harvard University.

Note: There will be a FAQ, if any, from after the coaching sessions – on Moodle



Task 2 – Create the Handbook Entry (graded!)

- ➔ Individual work
- ➔ Time estimated: around 150 min
- ➔ Setting: At the beginning, please consult your recently created information security policy.

Objectives and Conversion:

1. Describe an organizational scenario (a company) from an information security perspective
2. Outline and conduct a process to classify data-level entries for the identified corporate scenario
3. Describe: Select in your handbook section 2) "Information Security Policy" and write about
 - a.) the organizational scenario and identified relevant aspects for an information security policy
 - b.) what are the drivers for your classification in your information security policy?
 - c.) what are effective measures to successfully implement an information security policy in your organization?

Relevant sources: see provided presentation in lecture 3 -- Coaching Session III.pptx or below the excerpt of the slide deck with the selected cases.

Excerpt documents:



Handbook Guidance

The content should describe (see template for the handbook on Moodle) how an "information security policy" could be set up / defined for "your" company.

The basis for this "information security policy" is the system of Harvard University, which has been uploaded as a template on Moodle. Data from individual activities of "your" (actual) company should be entered into these five categories. This table then serves as a basis for decision-making to be able to classify entire processes based on how worthy of protection the data they contain is.

A possible approach would be: First, define "basic terms" regarding information security policy in written form, then put yourself in the position of your (former) employer and imagine all possible processes in this company. These processes provide the basis for data that can be entered into the Harvard University matrix (the information security policy template). This is followed by an explanation of the circumstances that led you to classify this data into the respective "level". Chapter 2 of the handbook contains written explanations/justifications, while the completed matrix should be filed in the appendix.

Your chapter 2 in the handbook could therefore look like this:

2.1 Definition of information security/terms

2.2 Own perspective

- *What is data worth protecting (generally in the private/professional environment)?*

2.3 Organizational perspective

- *How are data worthy of protection classified (possibly (government) requirements)?*
- *Effective implementation of protection measures for such data in the company?*
- *Your chosen company scenario/description?*

Link to information security policy in appendix

2.4 Additional thoughts

- *Possibly address difficulties in protecting data in the context of "home office"?*