University of Applied Sciences Northwestern Switzerland
School of Business

D4 Data and Ethics

Autumn 2022 | Lecture 3 – Coaching

Focus: Information security & cybersecurity | Author: Prof. Dr. Petra Maria Asprion | FHNW

© Picture Raphael Stöckli, MT cover 2018

Agenda

Part I -- Repetition L1 → SD1

Part II -- Organization Layer: Relevant References → SD2

Part III -- Organization Layer: First control - IS Policy → SD3

Part IV -- Organization Layer: Selective control - GEIGER → SD4

Coaching Session #3 → SD5

→ SD = Slide Deck

The theme is "be protected"

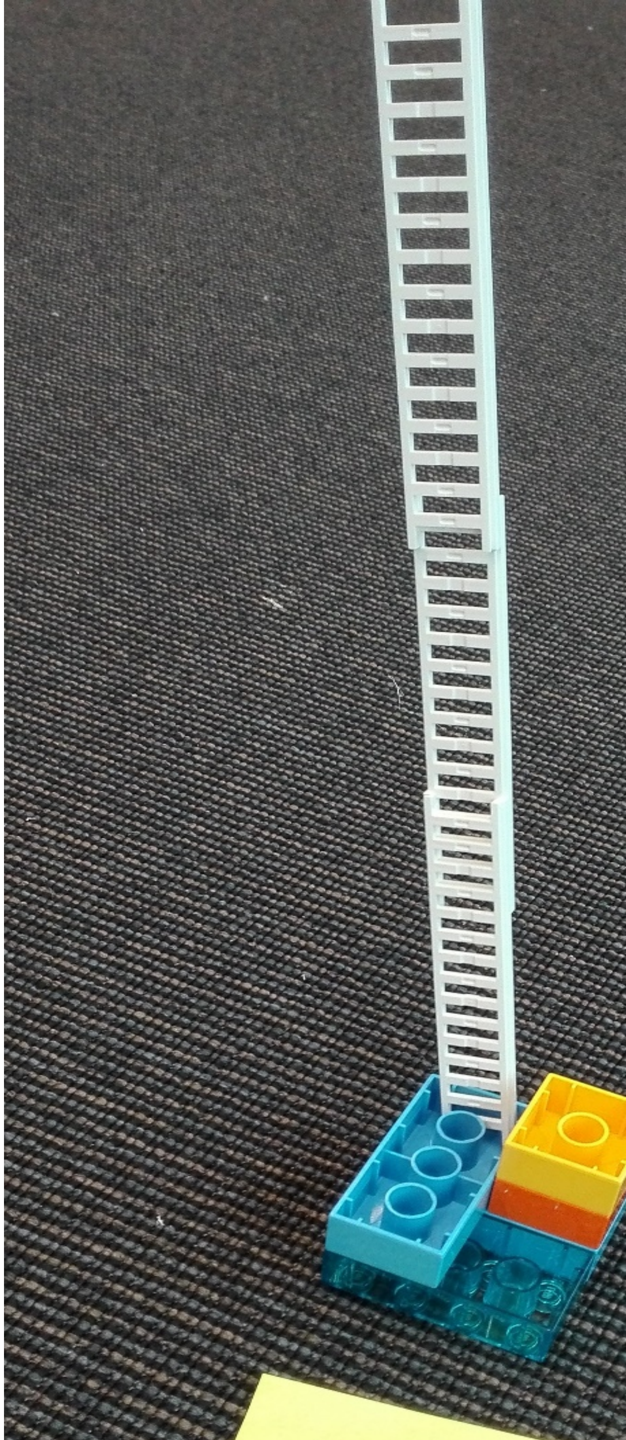
You have one individual task described in the following, which you should work during your coaching session.

The aim is that you

a) “**be protected**” in terms of developing a tailored control – an **Information Security Policy**

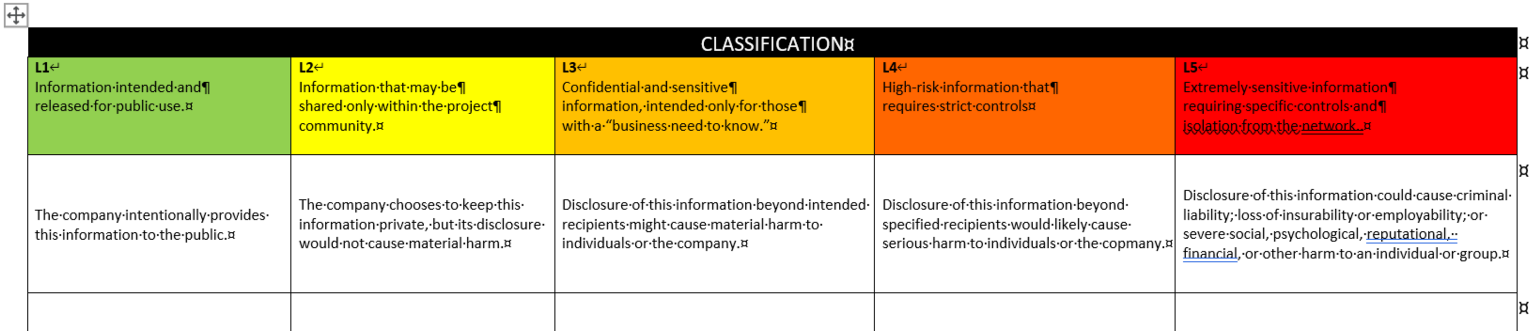
b) get an experience of how to create such a policy based on the NIST “Information Security Handbook” and the selected example from Harvard University.

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

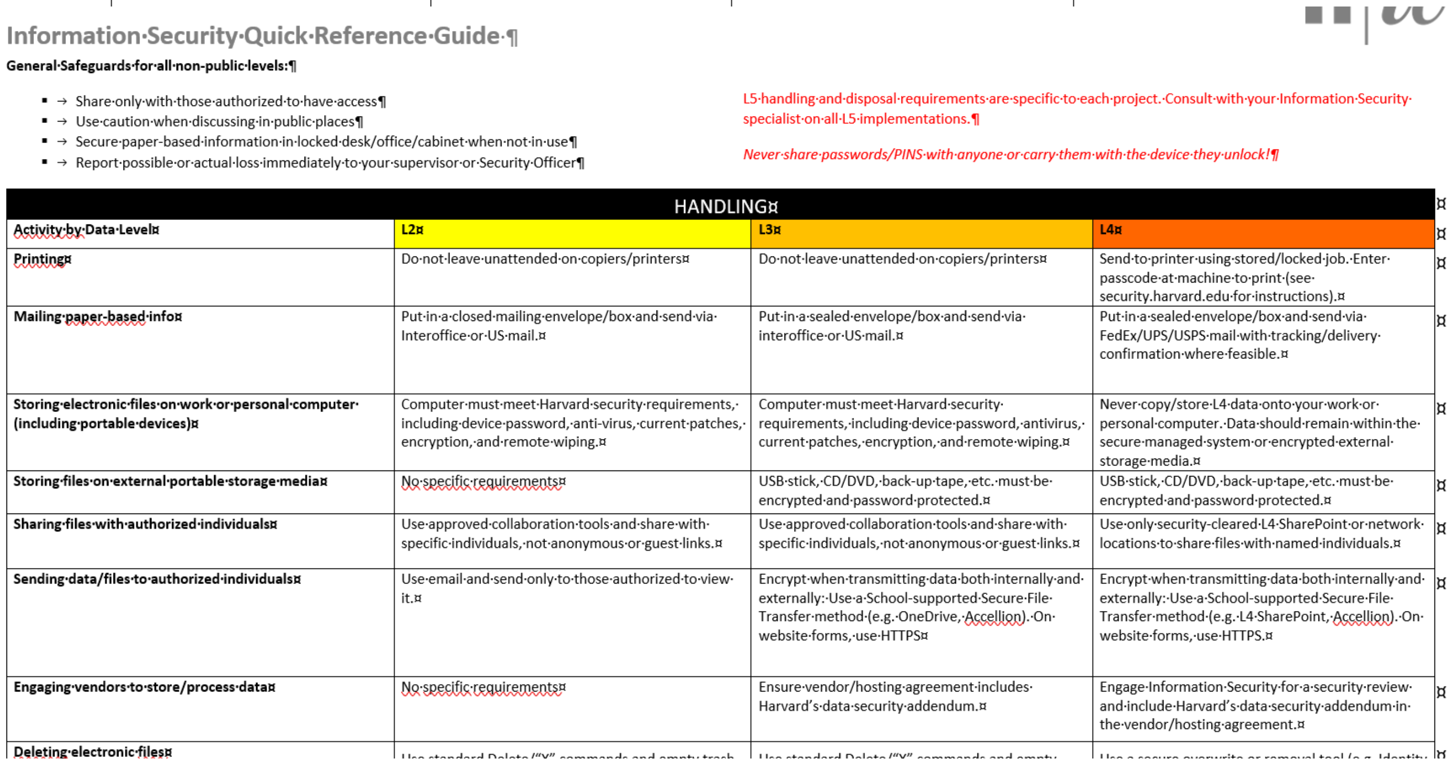


Develop an Information Security Policy

Use the outlines from slide deck III about an “Information Security Policy” as control as well as the provided template.



CLASSIFICATION				
L1 Information intended and released for public use.	L2 Information that may be shared only within the project community.	L3 Confidential and sensitive information, intended only for those with a “business need to know.”	L4 High-risk information that requires strict controls	L5 Extremely sensitive information requiring specific controls and isolation from the network.
The company intentionally provides this information to the public.	The company chooses to keep this information private, but its disclosure would not cause material harm.	Disclosure of this information beyond intended recipients might cause material harm to individuals or the company.	Disclosure of this information beyond specified recipients would likely cause serious harm to individuals or the copmany.	Disclosure of this information could cause criminal liability; loss of insurability or employability; or severe social, psychological, reputational, financial, or other harm to an individual or group.



Information Security Quick Reference Guide

General Safeguards for all non-public levels:

- Share only with those authorized to have access
- Use caution when discussing in public places
- Secure paper-based information in locked desk/office/cabinet when not in use
- Report possible or actual loss immediately to your supervisor or Security Officer

L5 handling and disposal requirements are specific to each project. Consult with your Information Security specialist on all L5 implementations.

Never share passwords/PINS with anyone or carry them with the device they unlock!

HANDLING			
Activity by Data Level	L2	L3	L4
Printing	Do not leave unattended on copiers/printers	Do not leave unattended on copiers/printers	Send to printer using stored/locked job. Enter passcode at machine to print (see security.harvard.edu for instructions).
Mailing paper-based info	Put in a closed mailing envelope/box and send via Interoffice or US mail.	Put in a sealed envelope/box and send via interoffice or US mail.	Put in a sealed envelope/box and send via FedEx/UPS/USPS mail with tracking/delivery confirmation where feasible.
Storing electronic files on work or personal computer (including portable devices)	Computer must meet Harvard security requirements, including device password, anti-virus, current patches, encryption, and remote wiping.	Computer must meet Harvard security requirements, including device password, antivirus, current patches, encryption, and remote wiping.	Never copy/store L4 data onto your work or personal computer. Data should remain within the secure managed system or encrypted external storage media.
Storing files on external portable storage media	No specific requirements	USB stick, CD/DVD, back-up tape, etc. must be encrypted and password protected.	USB stick, CD/DVD, back-up tape, etc. must be encrypted and password protected.
Sharing files with authorized individuals	Use approved collaboration tools and share with specific individuals, not anonymous or guest links.	Use approved collaboration tools and share with specific individuals, not anonymous or guest links.	Use only security-cleared L4 SharePoint or network locations to share files with named individuals.
Sending data/files to authorized individuals	Use email and send only to those authorized to view it.	Encrypt when transmitting data both internally and externally: Use a School-supported Secure File Transfer method (e.g. OneDrive, Accellion). On website forms, use HTTPS	Encrypt when transmitting data both internally and externally: Use a School-supported Secure File Transfer method (e.g. L4 SharePoint, Accellion). On website forms, use HTTPS.
Engaging vendors to store/process data	No specific requirements	Ensure vendor/hosting agreement includes Harvard’s data security addendum.	Engage Information Security for a security review and include Harvard’s data security addendum in the vendor/hosting agreement.
Deleting electronic files	Use standard Delete (“X” commands and empty trash	Use standard Delete (“X” commands and empty	Use a secure overwrite or removal tool (e.g. Identity

Recommended Literature

NIST SP 800-53, Revision 1, ‘Recommended Security Controls for Federal Information Systems,’ 2006

Information Security Handbook – A Guide for Managers - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf.
And see also: https://csrc.nist.gov/publications/detail/sp/800-100/final

Example: Harvard University -- https://policy.security.harvard.edu/policies

This is your self learning area: it is recommended that you walk through the recommended and provided publications to achieve an understanding about a.) reference models (as the information security handbook from NIST) or b.) how it is transferred into practice - an example like the one from Harvard University.