SYLLABUS ECCC

Area: **Digital competences** – DigComp 2.1
Module: DC 2.1 M4 Safety
Level: **Advanced (C6)** - according to own needs and those of others, and in complex contexts.

Module DC 2.1 M4 Safety Level C6 includes proficiency Level 6 of the DigComp 2.1 framework in the Competence Area 4: Safety.

Competences are verified in the following competence titles:

1. Protecting devices.
   To protect devices and digital content, and to understand risks and threats in digital environments. To know about safety and security measures and to have a due regard to reliability and privacy.
2. Protecting personal data and privacy.
   To protect personal data and privacy in digital environments. To understand how to use and share personally identifiable information while being able to protect oneself and others from damages. To understand that digital services use a "Privacy policy" to inform how personal data is used.
3. Protecting health and well-being.
   To be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies. To be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying). To be aware of digital technologies for social well-being and social inclusion.
4. Protecting the environment.
   To be aware of the environmental impact of digital technologies and their use.

The competence verification is carried out in the following groups:
1. Knowledge (K).
2. Skills (S).
3.Abilities (A).

The scope verified by the ECCC exam of module DC 2.1 M4 (Level C6)

COURSE PURPOSES		LEARNING OUTCOMES		K	S	A
C6_CP1	(4.1) To acquire advanced skills of protecting devices.	DC2.1_1	Can choose the most appropriate protection for devices and digital content.			
		DC2.1_2	Can discriminate risks and threats in digital environments.			
		DC2.1_3	Can choose the most appropriate safety and security measures.			
		DC2.1_4	Can assess the most appropriate ways to have due regard to reliability and privacy.			
		C6_LO1	Knows the types of attacks targeting electronic devices and the known methods of ensuring their safety.	✓		

COURSE PURPOSES		LEARNING OUTCOMES		K	S	A
		C6_LO2	Knows what data encryption is.	✓		
		C6_LO3	Can monitor the connection status of a digital device with the network and react appropriately to the threat.		✓	
		C6_LO4	Can compress / encrypt data using complex passwords, including various data storage locations.		✓	
		C6_LO5	Is able to take steps to mitigate risk of fraud by using a password.			✓
C6_CP2	(4.2) To develop knowledge about protecting personal data and privacy.	DC2.1_5	Can choose the more appropriate ways to protect personal data and privacy in digital environments.			
		DC2.1_6	Can evaluate the most appropriate ways of using and sharing personally identifiable information while protecting self and others from damages.			
		DC2.1_7	Can evaluate the appropriateness of privacy policy statements on how personal data are used.			
		C6_LO6	Knows how to protect other people data that apply to his/her own context (*as a worker, a parent, a teacher, etc.)*	✓		
		C6_LO7	Knows that many interactive services use information about him or her to filter in commercial messages in more or less explicit manners.	✓		
		C6_LO8	Is able to act prudently regarding privacy issues.		✓	
		C6_LO9	Can delete or modify information about self or others she/he is responsible for.		✓	
		C6_LO10	Is able to monitor his/her digital identity and footprints.		✓	
		C6_LO11	Can exploit the benefits of having multiple identities to fit a number of purposes.			✓
		DigComp 2.1 examples.	Can select the most appropriate way to protect the personal data (*e.g. address, phone number*) when sharing digital content (*e.g. a picture*) on the corporate account.		✓	
			Can distinguish between appropriate and inappropriate digital content to share it on the corporate account, so that own privacy and that of others are not damaged.	✓		
			Can assess whether personal data are used on the corporate account appropriately according to the European Data Protection Law and Right to be Forgotten.	✓		
			Can deal with complex situations that can arise with personal data while on corporate account, such as removing pictures or names to protect personal information in accordance with the European Data Protection Law and Right to be Forgotten.		✓	

COURSE PURPOSES		LEARNING OUTCOMES		K	S	A
			Can select the most appropriate way to protect my personal data (e.g. address, phone number), before sharing it on the digital platform.		✓	
C6_CP3	(4.3) To master knowledge of protecting health and well-being.	DC2.1_8	Can discriminate the most appropriate ways to avoid health -risks and threats to physical and psychological well-being while using digital technologies.			
		DC2.1_9	Can adapt the most appropriate ways to protect self and others from dangers in digital environments.			
		DC2.1_10	Can vary the use of digital technologies for social well-being and social inclusion.			
		C6_LO12	Knows the effect of prolonged use of technologies.	✓		
		C6_LO13	Is able to manage the distracting aspects of working/living digitally		✓	
		C6_LO14	Is able to take preventive steps to protect own health and the health of other she/he is responsible for.		✓	
		C6_LO15	Is aware of the health risks caused by addiction to digital technologies.			✓
		C6_LO16	Is aware of the importance of digital technologies for social well-being and social inclusion.			✓
C6_CP4	(4.4) To acquire advanced skills of protecting the environment.	DC2.1_11	Can choose the most appropriate solutions to protect the environment from the impact of digital technologies and their use.			
		C6_LO17	Can determine if appropriate and safe digital means are available, that are efficient and cost-effective in comparison with other means.	✓		
		C6_LO18	Has a comprehensive mental map of how the online world works.	✓		
		C6_LO19	Is able to use digital services without being completely dependent on them (or: helpless without).		✓	
		C6_LO20	Understands the technologies s/he is using at a level that is sufficient to underpin good purchasing decisions, e.g., about devices or Internet service providers.			✓

Practical skills, verified by the ECCC DC2.1 M4 exam, concern:

1. A computer workstation as PC / laptop equipped with a WiFi network interface and with Internet access with a minimum bandwidth of 2 Mb/s.
2. Operating system: MS Windows 7 or newer or Linux (kernel 3.0 or newer) with an account with administrator rights available to the student.
3. Programs: Acrobat Reader, CCleaner, Eraser, Wireshark, Soft Perfect Network Scanner, GIMP, OpenVPN.
4. Microsoft Office 2007 or newer (Word, Excel, Power Point).
5. Anti-virus program working in "monitor" mode with the heuristic function.

6. Libre Office suite.
7. A web browser that allows to work in private mode and allows to install add-ons such as: WOT, Adblock, Ghostery and supports plugins: Flash, Java.
8. A firewall program (the default system is also acceptable).
9. A program that encrypts directories and files (e.g. based on the EncFS library).