SYLLABUS ECCC

Area: **Digital competences – DigComp 2.1**
Module: **DC 2.1 M4 Safety**
Level: **Advanced (C5)** - as well as guiding others.

Module DC 2.1 M4 Safety Level C5 includes proficiency Level 5 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 C5)

COURSE PURPOSES			LEARNING OUTCOMES	K	S	A
C5_CP1	(4.1) To acquire advanced skills of protecting devices.	DC2.1_1	Can apply different ways to protect devices and digital content.			
		DC2.1_2	Can differentiate a variety of risks and threats in digital environments.			
		DC2.1_3	Can apply safety and security measures.			
		DC2.1_4	Can employ different ways to have due regard to reliability and privacy.			
		C5_LO1	Knows the types of attacks targeting electronic devices and the known methods of ensuring their safety.	✓		
		C5_LO2	Knows what data encryption is.	✓		

COURSE PURPOSES			LEARNING OUTCOMES	K	S	A
		C5_LO3	Can monitor the connection status of a digital device with the network and react appropriately to the threat.		✓	
		C5_LO4	Can compress / encrypt data using complex passwords, including various data storage locations.		✓	
		C5_LO5	Is able to take steps to mitigate risk of fraud by using a password.		✓	
		DigComp 2.1 examples.	Protects the corporate account using different methods (e.g. a strong password, control the recent logins) and show to others how to do it.			✓
			Can detect risks like receiving tweets and messages from followers with false profiles or phishing attempts.		✓	
			Can apply measures to avoid risks (*e.g. control the privacy settings*).		✓	
			Can help others to detect risks and threats while using a corporate account, digital learning platform on their tablets (*e.g. controlling who can access the files*).			✓
			Can protect information, data and content on digital learning platform (*e.g. a strong password, control the recent logins*).			✓
			Can detect different risks and threats when accessing digital platform and apply measures to avoid them (*e.g. how to virus-check attachments before downloading*).		✓	
C5_CP2	(4.2) To develop knowledge about protecting personal data and privacy.	DC2.1_5	Can apply different ways to protect personal data and privacy in digital environments.			
		DC2.1_6	Can apply different specific ways to share own data while protecting self and others from dangers.			
		DC2.1_7	Can explain privacy policy statements of how personal data is used in digital services.			
		C5_LO6	Knows how to protect other people data that apply to his/her own context (*as a worker, a parent, a teacher, etc.)*	✓		
		C5_LO7	Knows that many interactive services use information about him or her to filter in commercial messages in more or less explicit manners.	✓		
		C5_LO8	Is able to act prudently regarding privacy issues.		✓	
		C5_LO9	Can delete or modify information about self or others she/he is responsible for.		✓	
		C5_LO10	Is able to monitor his/her digital identity and footprints.		✓	

COURSE PURPOSES		LEARNING OUTCOMES		K	S	A
C5_CP3	(4.3) To master knowledge of protecting health and well-being.	DC2.1_8	Can show different ways to avoid health -risks and threats to physical and psychological well-being while using digital technologies.			
		DC2.1_9	Can apply different ways to protect self and others from dangers in digital environments.			
		DC2.1_10	Can show different digital technologies for social well-being and social inclusion.			
		C5_LO11	Knows the effect of prolonged use of technologies.	✓		
		C5_LO12	Is able to manage the distracting aspects of working/living digitally		✓	
		C5_LO13	Is able to take preventive steps to protect his/her own health and the health of other she/he is responsible for.		✓	
		C5_LO14	Is aware of the health risks caused by addiction to digital technologies.			✓
C5_CP4	(4.4) To acquire advanced skills of protecting the environment.	DC2.1_11	Can show different ways to protect the environment from the impact of digital technologies and their use.			
		C5_LO15	Can determine if appropriate and safe digital means are available, that are efficient and cost-effective in comparison with other means.	✓		
		C5_LO16	Has a comprehensive mental map of how the online world works.	✓		
		C5_LO17	Is able to use digital services without being completely dependent on them (or: helpless without).		✓	

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).