ISTC МНТЦ

INSTITUTE FOR SECURITY AND SAFETY

TRAINING SESSION AGENDA

Research Vetting, Knowledge Security, Responsible Science, and Individual Cybersecurity Training for Ukrainian Researchers.

June 13-15, 2023

Day 1: Knowledge Security		
9:00-09:45	Welcome, general introduction round, agenda of the seminar, expectation for the seminar, rules of seminar	
9:45-10:30	Understanding Knowledge Security and its relevance for scientists	Inject: Presentation of case studies of knowledge theft/misuse
		Group Work: what could happen? Presentation of 1 Scenario per group (e.g., nuclear, chemistry, biology, cyber); Participants are asked to develop worst case scenarios
		Presentation of the group work's results & discussion
10:30-11:00	Break	
11:00-12:00	Compliance & National/International Best Practices	Presentation: National and international instruments for stronger knowledge security
		Question-led discussion: former experiences with compliance and Nation state's actions. Problems/Solutions/addressing this in research projects & proposals
12:00-13:30	Lunch Break	
13:30-15:00	Understanding the Life Cycle of Knowledge/ Information	Presentation: Information and knowledge relations & the information/data life cycle
		Group work: 3 Case Studies & according to tasks/question-led exercise: participants reflect on what kind of form of knowledge is mostly used, which one is most unprotectable, which one is mostly interesting for seekers
		Presentation of the group work's results & discussion
15:00-15:15	Break	
15:15-16:00	Intellectual Property Infringement & Open Science	Presentation: Case studies on intellectual property infringement
		Question-led discussion: Open Science and Knowledge sharing issues
16:00-16:20	Reflection of own Research	Individual Exercise: Reflections in how far own research would be interesting to others (Knowledge Security), strategies in place to protect that knowledge, where is my knowledge in the information/data life cycle? Which regulation/compliance is relevant for my research?
16:20-17:00	Closing session	Key take aways of the reflection exercise and the day's presentations/Tasks

		Feedback on Content & Moderation through online anonymous polling
Day 2: Cyber Security		
9:00-9:15	Welcome & Agenda for the day	
9:15-10:30	Introduction to Cybersecurity	Experience Exchange: who has experienced a cyber attack as a victim or target (private or workspace)?
		Interactive Presentation: What is Cyber Security? Threat landscape, relevant attacker types, relevant means of attack (botnets, malware, worms, trojans, rubber ducks, social engineering etc.), relevant means of defense (technological & human)
10:30-11:00	Break	
11:00-12:30	Cybersecurity Culture in an Organization	Presentation: Organizational Culture & Security Culture Theory
		Interactive: how do I assess the cybersecurity culture of my organization?
		Group work: how can different roles support a cybersecurity culture?
		Presentation of the group work's results & discussion
		Discussion: Role of People, Processes and Technologies in Cybersecurity
12:30-13:30	Lunch Break	
13:30-15:00	Individual cybersecurity hygiene	Presentation: Case studies on cybersecurity incident and leaks
		Individual Task: Find out everything about other participant in the room
		Presentation of tasks findings
		Interactive discussion: Individual hygiene best practices
15:00-15:15	Break	
15:15-16:00	Spear Phishing	Practice: Detecting spear phishing
		Question-led discussion: who do I trust?
16:00-16:40	Demo hacking session	How everyday things can be dangerous?
16:40-17:00	Closing session	Open Q&A
		Key Take aways of the day
		Feedback on Content & Moderation

Day 3: Research Vetting and Risk Management		
9:00-09:15	Welcome & Agenda for the day	
9:15-10:00	Introduction to Risk Assessment in Research	Presentation: Risk management for IP frameworks and strategies
		Group Work: Identifying and assessing risks associated with dual-use technologies
10:00-10:30	Break	
10:30-12:00	Risk Management and Mitigation Best Practices	Question-led discussion: Risk mitigation strategies and best practices
		Presentation: Cybersecurity risk management for dual-use technologies
		Group work: Scenarios provided with Questions on how to assess and mitigate risks on potential dual use Research
		Presentation of Group work
12:00-13:30	Lunch Break	
13:30-15:15	Partner Vetting	Question-led discussion: Assessing future Research Partners
		Interactive Presentation: Understanding Trust in Relationships
		Group work: Partner-Vetting, what would you do?
		Presentation of Group work
15:15-15:30	Break	
15:30-16:30	Convergence of all Seminar Topics	Draw a Picture of the relationship between the Course's Contents: Knowledge security, Cyber security, Research vetting & trust.
		Individual: write down 5 key Take-aways for secure behaviour in the future
		Comparison of Take-aways, clustering & Voting
16:30-17:00	Closing session	Open Q&A
		Feedback on Content & Moderation
		Review and Evaluation of the Training Course
		Closing remarks