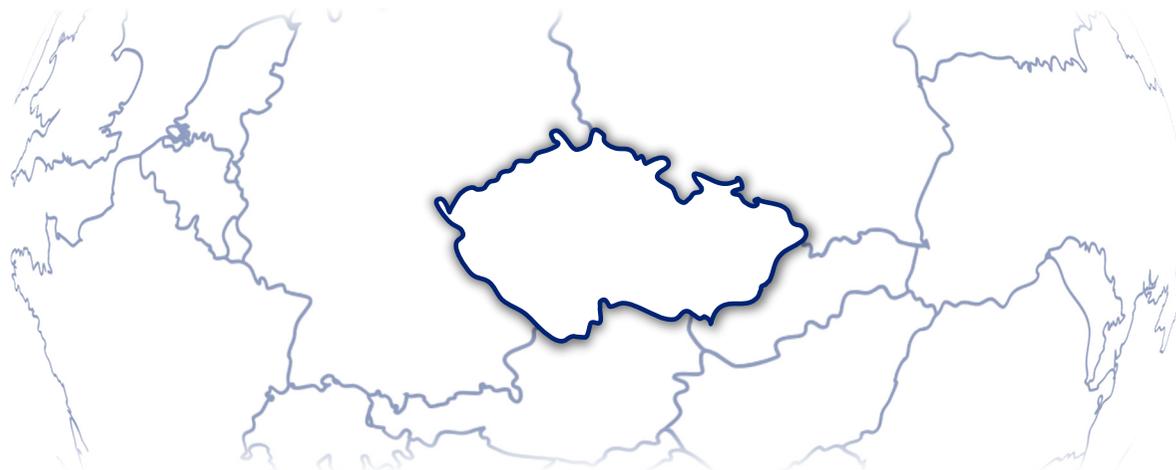
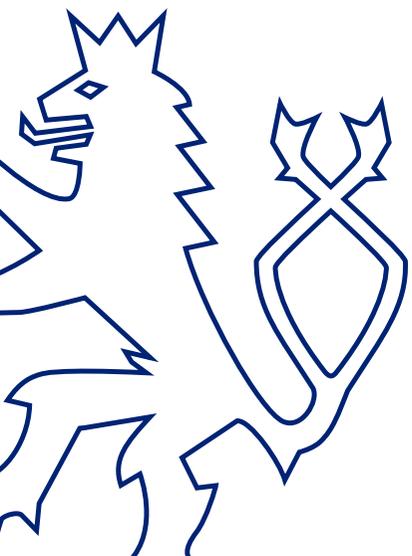


**ACTION PLAN FOR THE NATIONAL
CYBERSECURITY STRATEGY
OF THE CZECH REPUBLIC FROM 2021 TO 2025**





FOREWORD

Achievement of the main goals of the *National Cybersecurity Strategy of the Czech Republic* is subject to the successful implementation and timely fulfilment of the tasks defined in this *Action Plan for the National Cybersecurity Strategy for the years 2021 to 2025*.

Certain tasks defined by the Action Plan require a close cooperation between the public authorities and other entities subject to Act No. 181/2014 Coll. (Act on Cyber Security), as amended, and other public administration institutions. Each such task is to be coordinated by a designated body, which may require the cooperation of other entities.

The designated bodies are responsible for fulfilling the tasks with the legal authority given and within their legally-defined range of competence. By the same measure, the roles and competence of individual institutions are not affected by this Action Plan.

The abbreviations used herein are explained at the end of this document in the section *List of Abbreviations*.





TABLE OF CONTENTS

A. IN CYBERSPACE WITH CONFIDENCE	3
A COMMON APPROACH TO CYBERSECURITY	3
STRATEGIC COMMUNICATION	4
SECURE INFRASTRUCTURE	5
DEVELOPMENT OF CAPABILITIES	5
RESPONDING CONFIDENTLY	7
PREVENTING AND COMBATTING CRIME	7
NATIONAL LEGISLATION	8
AMENDMENTS AND UPDATES TO THE REGULATORY FRAMEWORK	9
RESEARCH AND DEVELOPMENT	9
B. STRONG AND RELIABLE ALLIANCES.....	11
EFFECTIVE INTERNATIONAL COOPERATION.....	11
BUILDING AND STRENGTHENING ACTIVE ALLIANCES	12
INTERNATIONAL LAW, INTERNET GOVERNANCE, AND HUMAN RIGHTS ONLINE	13
SHARING CAPABILITIES AND EXPERTISE	14
C. RESILIENT SOCIETY 4.0	15
SECURING DIGITAL PUBLIC ADMINISTRATION	15
QUALITY EDUCATION SYSTEM.....	16
AWARENESS-ENHANCING AND TRAINING ACTIVITIES.....	17
VOCATIONAL TRAINING AND STRENGTHENING EXPERTISE LEVELS	18
LIST OF ABBREVIATIONS.....	19



A. IN CYBERSPACE WITH CONFIDENCE

	Code	Task	Responsible body	Timeframe
A COMMON APPROACH TO CYBERSECURITY	1.	At the national level, create and operate a secure platform for communication and the sharing of information about cyber threats and vulnerabilities, in particular as regards addressing more extensive national and international cybersecurity incidents.	NÚKIB	From Q2 2021, continuously
	2.	Develop effective and coordinated cooperation between the NÚKIB, the Czech Republic police force, and the intelligence services in the field of cybersecurity, including cooperation with the public authorities and persons subject to ACS in dealing with cybersecurity incidents; set clear processes for the cooperation.	Intelligence services NÚKIB PCR	Continuously
	3.	Design a unified procedure for notifications of cybersecurity incidents to the relevant public administration bodies which require such notifications.	NÚKIB in cooperation with relevant parties	Q4 2022
	4.	Converge an approach to cybersecurity and protection of classified information in information and communication systems in compliance with the <i>“Development Concept of the National Cyber and Information Security Agency”</i> . Propose potential alterations to the approach based on the analysis of the current state and needs.	NÚKIB in cooperation with: Intelligence services MD MFA MoI NSA OG CR	From Q1 2024, continuously
	5.	Deepen cooperation based on the memoranda concluded with state inspection and regulatory bodies, making the control and regulatory activities of the bodies in question more effective.	CAA CDPA CNB CTU NÚKIB SONS	Continuously
	6.	Design an assessment of supplier risk profile and application of restrictions to high-risk suppliers at the national level for secure introduction and implementation of next-generation telecommunication networks.	NÚKIB in cooperation with: CTU Intelligence services MFA MTI	Q2 2022

	7.	Design an assessment of supplier risk profile at the national level and applications of restrictions to high-risk suppliers to systems under the scope of ACS.	NÚKIB in cooperation with: Intelligence services MFA MoI MTI	Q1 2024
	8.	Establish and deepen cooperation with umbrella organisations from individual OES sectors (unions or other platforms) and collaborate with them on developing cybersecurity.	NÚKIB	Continuously
	9.	Appropriately connect activities leading to increased cybersecurity with activities increasing the Czech Republic's resiliency against hybrid threats.	ACR Intelligence services MD MFA MoI NÚKIB	Continuously
	10.	Draft a national policy proposal for the coordinated disclosure of vulnerabilities.	NÚKIB	Q4 2021
	11.	Expand and step up cooperation with the private sector; improve awareness of the activities of the NÚKIB and possibilities of mutual cooperation.	NÚKIB	Continuously
STRATEGIC COMMUNICATION	12.	Carry out communication campaigns to support national cybersecurity objectives.	NÚKIB in cooperation with the relevant actors depending on the issue being addressed	Continuously
	13.	Create a methodology for strategic communication between relevant bodies at the national level to be used in the case of cyber incidents, attacks and other threats.	NÚKIB in cooperation with: HPPO Intelligence services MD MFA MoI PCR PGO	Q2 2022

SECURE INFRASTRUCTURE	14.	Assist and provide national administration methodological support in the application of detection systems for network traffic monitoring and cybersecurity incidents within public administration.	NÚKIB	Continuously
	15.	Search for vulnerabilities among public authorities and persons subject to ACS, as well as entities outside the scope of the ACS.	NÚKIB	Continuously
	16.	Continue with the implementation of penetration testing under the previously agreed conditions to detect faults and vulnerabilities in the information systems and networks of public authorities and persons subject to ACS.	NÚKIB	Continuously
	17.	Prepare a guidance document for contractor security management and distribute it to public authorities and persons subject to ACS.	NÚKIB in cooperation with: MF MoI MTI	Q4 2022
	18.	Prepare a draft update of encryption standards for public authorities and persons subject to ACS that reflects the arrival of quantum computers and the associated threat of cracking current encryption methods.	NÚKIB	Q1 2024
	19.	Improve the cybersecurity of the healthcare sector by creating methodological guidelines, carrying out training, providing e-learning courses, and other relevant methods.	NÚKIB in cooperation with: MH	Continuously
	20.	Design, organise and implement technical, non-technical and combined cybersecurity exercises for public authorities and persons subject to ACS and other relevant partners, and organize extensive sectoral training with tailor-made scenarios.	NÚKIB	Continuously
	21.	Propose a design for a unified public administration network and relevant associated follow-up projects that use a standardized set of security norms to improve the cybersecurity of state institutions.	MF MI MoI NÚKIB in cooperation with: BIS	Q2 2022
DEVELOPMENT OF CAPABILITIES	22.	Implement the “ <i>Development Concept of the National Cyber and Information Security Agency</i> ” to further develop the skills and competencies of the NÚKIB, e.g. in the fields of supervision, new technologies, and sectoral specialisations.	NÚKIB	Continuously in compliance with the approved document

23.	Continue to strengthen the cybersecurity system by developing NCOC competencies as a part of the MI, focusing on logistical, personnel, and financial security, as well as other aspects vital to its effective operations.	MI	Continuously
24.	Update the national system of cyberattack detection to employ all available national resources.	Intelligence services MoI NÚKIB	Q4 2022
25.	Strengthen personnel and other capacities required to create, prepare, and organise technical, non-technical and other relevant cybersecurity exercises in order to ensure the defence of the Czech Republic.	ACR MD MI	Continuously
26.	In cooperation with the organisers, incorporate cybersecurity elements into relevant existing national or sectoral training.	NÚKIB	Continuously
27.	Create and actively participate in communication and procedural training exercises focused on the efficiency of cooperation between parties and quick information exchange in the areas of cybersecurity, cybercrime and defence.	NÚKIB in cooperation with: ACR Intelligence services MD MFA PCR	Continuously
28.	Involve national partners in the preparation of scenarios for international cybersecurity training sessions and thereby contribute to the strengthening of cooperation, as well as the setting and coordination of procedures used to address actual cyber threats.	ACR MD NÚKIB	Continuously
29.	Create a platform involving volunteer cybersecurity experts and institutionalise their involvement in ensuring cybersecurity.	NÚKIB	Q3 2023
30.	Involve the private sector in cyber defence and cooperate actively with it.	MI in cooperation with: BIS MD NÚKIB OFRI	From Q1 2022, continuously

RESPONDING CONFIDENTLY	31.	Create, implement, and, as needed, mobilise an effective national framework for the attribution of serious cyberattacks.	Intelligence services MFA NÚKIB OG CR PCR	From 2021, continuously
	32.	Consolidate the framework for potential responses to cyberattacks and immediate threats, and establish a system for its coordinated use.	ACR Intelligence services MD MFA NÚKIB PCR in cooperation with: MoI	Q4 2022
	33.	Consolidate approaches to deter cyberattacks with a view to subsequent coordinated use of all available capabilities for the most effective deterrence of the perpetrators.	MD MFA MI NÚKIB in cooperation with: BIS OFRI	Q4 2023
	34.	Prepare a concept of development of fast response capability to address extensive security incidents.	Intelligence services NÚKIB PCR	Q4 2024
PREVENTING AND COMBATTING CRIME	35.	Develop and strengthen the cybercrime capabilities of the Czech Republic police force in compliance with the <i>“Development Concept of the Police of the Czech Republic until 2027”</i> and <i>“Strategy to Combat Cybercrime”</i> .	PCR	Continuously based on the approved concept notes
	36.	Coordinate the activities of the NÚKUB and the Czech Republic police force with the most synergy possible in the area of preventive programmes, especially by means of information exchange.	MoI NÚKIB PCR	Continuously

	37.	Carry out analyses of international legal obligations in the area of cybercrime and cybersecurity, take those obligations into account in cooperation between the actors in cybersecurity and cybercrime, and implement them into relevant methodologies.	NÚKIB in cooperation with: Intelligence services MFA MJ MoI PCR PGO	Q2 2022
NATIONAL LEGISLATION	38.	Based on analyses and taking technological and social developments into consideration, update and create clear, effective, and proportional legislative and regulatory acts on cybersecurity, especially in terms of setting the security levels prescribed by the public authorities and persons subject to ACS.	NÚKIB	Continuously
	39.	Based on continuously performed analyses of the impacts of regulation in compliance with the ACS, define systems of importance to the state's operations and security that are not yet governed by law thus far. If such systems already exist, draft relevant legislative amendments.	NÚKIB	From Q4 2024
	40.	Carry out a legal review of the state of cybercrime threats in the context of other crisis situations, and draft potential legislative changes.	NÚKIB in cooperation with: Intelligence services MD MFA MoI OG CR	Q2 2023
	41.	Analyse the legal options for the immediate operational purchase of technical and programme means necessary to take countermeasures in crisis situations and the measures under Section 11 of the ACS or in a state of cyber danger and propose a legislative change if necessary.	MoI NÚKIB in cooperation with: MRD	Q4 2021
	42.	Analyse and draft legislation as needed on competence requirements for persons performing any of the roles designated by the DCS.	NÚKIB	Q4 2025

	43.	Analyse the current state of competencies and cooperation in order to propose amendments to the respective legal norms so that they are in line with best practices in the area of cybercrime, cybersecurity, and cyber protection.	MI NÚKIB PCR in cooperation with: BIS MJ MoI OFRI PGO	Q1 2023
AMENDMENTS AND UPDATES TO THE REGULATORY FRAMEWORK	44.	Compare the selected currently used methods of risk analysis to check whether they comply with the requirements of the DCS and, at the same time, are effectively applicable to various organisations. In general, the output of this project will be offered to public authorities and persons subject to ACS and to the general public.	NÚKIB in cooperation with: MoI	Q2 2022
	45.	Update and create a set of recommended standards and good practices which would also be helpful in addressing cybersecurity risks for entities outside the regulatory scope of the ACS.	NÚKIB	Continuously
	46.	Fulfil the tasks stipulated in the “Act on Cyber Security” in EU cybersecurity certification of information and communication technologies.	NÚKIB in cooperation with: CAI	Continuously
	47.	Establish a regulatory framework for Cloud computing security.	NÚKIB	Q3 2022
RESEARCH AND DEVELOPMENT	48.	Regularly update the “National Research and Development Plan for Cybersecurity and Information Security”, including priority research topics and specific measures to meet the objectives of the National Plan, and in particular, identify the priority research topics that are vital to secure Czech cyberspace. Set further objectives to include specific tools that will contribute to developing the research and innovation environment in the Czech Republic, and deepen the cooperation between public, private, and academic sectors.	NÚKIB in cooperation with: Intelligence services MD MEYS MFA MoI MRD MTI PCR	Continuously every two years

49.	Take into account the priority research topics stipulated in the “ <i>National Research and Development Plan for Cybersecurity and Information Security</i> ” in calls for public procurements and both national and international research, development, and innovation support programmes.	MD MEYS MFA MoI MRD MTI OG CR TA CR	Continuously
50.	Initiate and participate in research projects with partners from public, private and academic areas at the national, European, and global levels.	NÚKIB in cooperation with: Intelligence services MD MFA MoI PCR TA CR TC CAS	Continuously
51.	Support the creation and operations of a European centre of excellence in AI in the Czech Republic, focusing on cybersecurity as one of its priority areas.	OG CR in cooperation with: MEYS MFA MT MTI NÚKIB	Continuously

B. STRONG AND RELIABLE ALLIANCES

	Code	Task	Responsible body	Timeframe
EFFECTIVE INTERNATIONAL COOPERATION	52.	Create and regularly congregate international platforms for the coordination of activities of state administration central bodies in cyberspace that affect international relationships, including activities of the Czech Republic in international organisations and integration groupings.	MFA in cooperation with: CTU MD MJ MoI MTI NÚKIB OG CR	From Q3 2021, continuously
	53.	Cooperate with other sectors in cross-border activities relating to cybersecurity and cyber protection.	CTU MD MFA MJ MoI MTI NÚKIB OG CR	Continuously
	54.	Within the EU, actively cooperate with the European Commission and other EU institutions and agencies to ensure improved cohesion in cyber issues.	MFA NÚKIB in cooperation with: MD MoI MTI	Continuously
	55.	Strengthen the active role and promote the interests of the Czech Republic in the area of cybersecurity within the EU and cooperate with foreign partners, the other Member States and European authorities to that end. Create functional and purposeful European regulations and design and implement both legislative and non-legislative EU documents.	MFA NÚKIB in cooperation with: CTU MoI MTI	Continuously
	56.	Cooperate with NATO and allies to implement the NATO cyber protection and security strategy and to react to current challenges. Deepen cooperation, namely with respect to responding to cybersecurity incidents and the exchange of both technical and non-technical information about threats and vulnerabilities.	MFA MI NÚKIB in cooperation with: ACR MD PCR	Continuously

	57.	Actively participate in sharing information about cybersecurity incidents; exchange information about malicious codes between countries at the appropriate international level of organisations of which the Czech Republic is a member; the ENISA, and other TF-CSIRT or FIRST-type platforms.	NÚKIB	Continuously
	58.	Support the creation and consolidation of international communication and information channels between CERT/CSIRT workplaces, international organisations, and academic centres.	NÚKIB	Continuously
	59.	Promote the interests of the Czech Republic in cyber issues within the OSCE and strengthen its active role, especially by cooperating in the creation and the subsequent implementation of measures to increase trust between states in cyberspace.	MFA NÚKIB	Continuously
	60.	Strengthen the active role of the Czech Republic within the OECD in the area of cyber and digital security; and in particular, participate in the preparation of strategic documents and recommendations.	MFA MTI NÚKIB OG CR	Continuously
	61.	Actively cooperate with national cybersecurity organisations in the Central European region (incl. using the existing CECSP), Eastern European region, and the area of western Balkan countries.	NÚKIB	Continuously
	62.	Update and adjust international cooperation procedures that determine OES/CII, with particular focus upon the determination of cross-border dependencies, in compliance with the forthcoming amendment to the NIS Directive.	NÚKIB	From Q3 2023, based on adoption of the NIS directive revision
BUILDING AND STRENGTHENING ACTIVE ALLIANCES	63.	Establish and deepen bilateral cooperation with partner institutions of select countries in the area of cybersecurity and protection, especially with the Czech Republic's key partners in the area, such as the EU member states, the USA, Israel, South Korea, and Australia, among others.	MFA NÚKIB in cooperation with: ACR Intelligence services MD	Continuously
	64.	In justified cases, send cyber attachés and national experts abroad to deepen strategically important cooperation with crucial partners of the Czech Republic, or within the structures of the EU and NATO.	NÚKIB in cooperation with: MD MFA	Continuously
	65.	Actively participate in the international coordination and response to cybersecurity initiatives (mainly within the structures of the EU and NATO) and promote the Czech Republic's position in coalitions with countries that share the same values.	MFA NÚKIB	Continuously

	66.	Actively cooperate with partner states and allied states in coordinating attribution of and response to severe cyberattacks and incidents.	Intelligence services MD MFA NÚKIB PCR	Continuously
	67.	Actively participate in organising, preparing, and implementing international training programs, and actively strengthen the network of important cybersecurity partners through joint cybersecurity exercises.	ACR MD MFA NÚKIB	Continuously
INTERNATIONAL LAW, INTERNET GOVERNANCE, AND HUMAN RIGHTS ONLINE	68.	Create a comprehensive Czech Republic national position on the interpretation of international law on cybersecurity and cyber protection.	MFA in cooperation with: Intelligence services MD MJ NÚKIB PGO	Q4 2021
	69.	Compile an overview of the implementation of non-compulsory standards of responsible cyberspace conduct for states, and actively participate in the promotion of compliance therewith. Prevent their fragmentation and weakening in the area of respect for human rights, among others.	MFA in cooperation with: NÚKIB	Q4 2021 and then continuously
	70.	Promote existing international law and non-compulsory standards of responsible cyberspace conduct for states through active cyber diplomacy.	MFA in cooperation with: MJ NÚKIB	Continuously
	71.	Actively help shape international discussions at the UN on improving cyberspace security and stability, especially within the scope of the first and third committees of the General Assembly in New York and negotiations organised by the UNODC in Vienna. Focus on interpreting international law and non-compulsory cyberspace standards of responsible conduct of individual states, as well as measures to increase trust and cooperation in the development of digital capacities.	MFA in cooperation with: MJ NÚKIB	Continuously
	72.	Become involved in the international discussion on Internet governance, including the Internet Governance Forum, and promote private and academic sector participation.	MFA MTI NÚKIB	Continuously

	73.	Monitor the preparation of harmonised EU standards, as well as technical and non-technical standards within the scope of international standardisation organisations with outreach to cybersecurity and Internet governance (such as the International Telecommunication Union), and with regards to capacities participate in their creation and implementation.	CTU MFA MTI NÚKIB	Continuously
SHARING CAPABILITIES AND EXPERTISE	74.	Create and organise cybersecurity exercises for foreign partners of the Czech Republic in coordination and synergy with other CR international activities.	NÚKIB in cooperation with: MFA	Continuously
	75.	Share experience with good practices in various cybersecurity areas with foreign partners, states, international organisations, and non-governmental organisations.	NÚKIB in cooperation with: MFA	Continuously
	76.	Organise international cybersecurity conferences, training programs, courses, seminars, and educational projects.	NÚKIB in cooperation with: Intelligence services MD MFA MoI	Continuously
	77.	Actively contribute to the activities of NATO CCD COE using national means and expertise, and participate in the Centre's research and training activities.	MD NÚKIB	Continuously
	78.	Strengthen the cybersecurity capacities of third countries through the use of foreign development cooperation instruments and economic diplomacy in compliance with the " <i>Cross-Border Development Cooperation Policy</i> " and the " <i>Concept of Foreign Policy of the Czech Republic</i> ". Carry out both bilateral and multilateral projects within the scope of platforms such as the Global Forum on Cyber Expertise (GFCE), the United Nations Development Programme (UNDP), the International Telecommunication Union (ITU), the United Nations Conference on Trade and Development (UNCTAD) or the Freedom Online Coalition (FOC).	MFA in cooperation with: CzDA MJ MoI MTI NÚKIB	Continuously

C. RESILIENT SOCIETY 4.0

	Code	Task	Responsible body	Timeframe
SECURING DIGITAL PUBLIC ADMINISTRATION	79.	Design procedures to secure e-Government systems according to the “ <i>security by design</i> ” approach; i.e., from the conception and implementation of each individual element.	Government agent for IT and digitalisation MoI NÚKIB	Q4 2021
	80.	Ensure compliance with procedures designed and intended to ensure the cybersecurity of individual e-Government systems from the very beginning of their implementation.	Government MoI NÚKIB Plenipotentiary for IT and Digitalisation	From Q1 2022, continuously
	81.	Formulate a safe code methodology for public administration to support the development of secure software.	MoI in cooperation with: NÚKIB	Q4 2021
	82.	Ensure development of the e-Government surveillance centre to create a single Government surveillance centre that provides common monitoring and surveillance for e-Government and other applicable systems.	MoI in cooperation with: Intelligence services MD MFA NÚKIB OG CR	Q4 2023
	83.	Draft a concept for the protection of non-confidential information of a sensitive nature.	NÚKIB in cooperation with: Intelligence services MD MFA MoI NSA	Q4 2023
	84.	Formulate and set a state administration-wide framework to secure information confidentiality in e-mail communications via encryption.	NÚKIB	Q3 2022
	85.	Set the IROP 2021–2027 calls effectively for the area of the e-Government and cybersecurity to ensure the cybersecurity of selected information systems of the Czech Republic.	MRD in cooperation with: MoI NÚKIB	Continuously

	86.	Share experience, know-how, methodological materials, and examples of good practices in the management of cybersecurity ICT projects across the state public administration, emphasising projects co-funded by the EU and the future IROP II call.	NÚKIB in cooperation with: MRD	Continuously
	87.	Make the best use of the EU funds in the EU 2021+ programme period for projects that increase the resilience of the CII/IIS/OES against cyber threats.	NÚKIB	Continuously
	88.	Participate in the safe development of Smart Cities in the Czech Republic in line with the “ <i>SMART Cities Concept- Resilience by SMART Solutions for Municipalities and Regions</i> ”, utilising, for example, methodological guidance and consultations.	NÚKIB in cooperation with: MRD	Continuously
QUALITY EDUCATION SYSTEM	89.	Prepare a national education plan in the field of cybersecurity.	NÚKIB in cooperation with: MD MEYS MFA MH MJ MLSA MoI OG CR PCR	Q4 2022
	90.	Actively offer an e-learning cybersecurity course to all officers and include it in their mandatory initial training. Offer e-learning courses to other interested parties from both the public and private sectors.	NÚKIB in cooperation with: MoI OG CR	Continuously
	91.	Continue to modernise primary and secondary school curricula to promote cybersecurity topics and digital competencies.	MEYS in cooperation with: NÚKIB	Q4 2023
	92.	Cooperate with universities, higher vocational schools, and secondary schools (including support to Junior Centres of Excellence programs) to create and introduce new study programmes, fields, curricula, and innovative elements in teaching cybersecurity.	NÚKIB in cooperation with: MEYS	Continuously

	93.	Raise the cybersecurity education level of teachers and students using modern teaching methods and technologies.	MEYS in cooperation with: Mol NÚKIB	Continuously
	94.	Prepare supporting materials to ensure and secure distance learning at primary and secondary schools.	MEYS in cooperation with: NÚKIB	Q3 2021
AWARENESS- ENHANCING AND TRAINING ACTIVITIES	95.	Directly participate in teaching cybersecurity disciplines, programmes, subjects and related topics, especially at universities, but also at designated higher vocational schools and secondary schools.	NÚKIB	Continuously
	96.	Provide supervision and consultations on university and higher vocational school theses dealing with cybersecurity and information security topics to students from such institutions.	NÚKIB	Continuously
	97.	Develop and maintain an educational e-learning platform focused upon the following target groups: public administration officers, teaching staff, IT administrators, cybersecurity managers, and other professionals performing ACS-affected roles, as well as vulnerable population groups such as children, young people, and seniors.	NÚKIB in cooperation with: MEYS MJ MLSA Mol OG CR	Continuously
	98.	Use the current education and prevention system, including cybersecurity platforms (such as the Digikoalice advisory group and Safer Internet Board), for cybersecurity education, prevention, and enhanced public awareness.	NÚKIB in cooperation with: MEYS MJ Mol PCR	Continuously
	99.	Analyse the current state of the labour market in order to identify fundamental requirements for cybersecurity specialists and ensure they are reflected in the respective state policies.	MLSA in cooperation with: MTI NÚKIB	Q2 2022
	100.	Educate both professionals and the general public in cybersecurity via training sessions, conferences, workshops, and other activities.	NÚKIB	Continuously

VOCATIONAL TRAINING AND STRENGTHENING EXPERTISE LEVELS	101.	Train both new and current public administration employees in cybersecurity, including public authorities and persons subject to ACS.	NÚKIB	Continuously
	102.	Create and prepare awareness-raising and educational materials, e-learning courses, and other training activities for both new and current members of the armed forces and public security forces.	NÚKIB in cooperation with: ACR Administration Customs DG FRS GIBS Intelligence services Mol PCR Prison Service	Continuously
	103.	Implement professional educational activities for judges and public prosecutors in the field of cyber criminality.	PCR in cooperation with: Judicial Academy	Continuously
	104.	Integrate cybersecurity training programs into the training of specialists and expert members of the public security forces.	NÚKIB in cooperation with: Administration Customs DG FRS GIBS Mol PCR Prison Service	Continuously
	105.	Extend and improve training provided to public authorities and persons subject to ACS relating to their duties, as per the security measures pursuant to DCS provisions.	NÚKIB	Continuously

LIST OF ABBREVIATIONS

ACR - Army of the Czech Republic

ACS - Act No. 181/2014 Coll., on Cyber Security and change of related acts (Act on Cyber Security), as amended

AI - artificial intelligence

BIS - Security Information Service

CAA - Civil Aviation Authority

CAI - Czech Accreditation Institute

CCD COE - NATO Cooperative Cyber Defence Centre of Excellence

CECSP - Central European Cyber Security Platform

CERT - Computer Emergency Response Team

CII - critical information infrastructure

CNB - Czech National Bank

CR - Czech Republic

CSIRT - Computer Security Incident Response Team

CTU - Czech Telecommunication Office

CzDA - Czech Development Agency

DCS - Decree No. 82/2018 Coll. on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (Cybersecurity Decree)

DG FRS - Directorate General of the Czech Republic Fire Rescue Service

ENISA - European Union Agency for Cybersecurity

EU - European Union

FIRST - Forum of Incident Response and Security Teams

FOC - Freedom Online Coalition

GFCE - Global Forum on Cyber Expertise

GIBS - Inspectorate General of the Czech Republic Security Forces

HPPO - High Public Prosecutor's Office



ICT - information and communication technology
IIS - important information system
IROP - Integrated Regional Operational Programme
IT - information technology
ITU - International Telecommunication Union
MD - Ministry of Transport
MEYS - Ministry of Education, Youth and Sports
MF - Ministry of Finance
MFA - Ministry of Foreign Affairs
MH - Ministry of Health
MI - Military Intelligence
MJ - Ministry of Justice
MLSA - Ministry of Labour and Social Affairs
MO - Ministry of Defence
MoI - Ministry of the Interior
MPO - Ministry of Industry and Trade
MRD - Ministry of Regional Development
NATO - North Atlantic Treaty Organization
NCOC - National Cyber Operations Centre
NIS - Network and Information Systems
NSA - National Security Authority
NÚKIB - National Cyber and Information Security Agency
OECD - Organisation for Economic Co-operation and Development
OES - operator of an essential service
OFRI - Office for Foreign Relations and Information
OG CR - Office of the Government of the Czech Republic

OSCE- Organization for Security and Cooperation in Europe

PGO - Office of the Prosecutor General

PCR - Czech Republic police force

SONS - State Office for Nuclear Safety

TA CR - Technology Agency of the Czech Republic

TC CAS - Technology Centre of the Czech Academy of Sciences

TF-CSIRT - Task Force on Computer Security Incident Response Teams

UN - United Nations

UNCTAD - United Nations Conference on Trade and Development

UNDP - United Nations Development Programme

UNODC - United Nations Office on Drugs and Crime

USA - United States of America

