Template no. 3

ACTION PLAN FOR STRATEGY IMPLEMENTATION

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA: 1. Secure national capacities for cybersecurity.					**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024 – 2044):** **Priority area 5: Secure, safe and resilient society**		
General Objective 1.: **Ensure a resilient and secure national cyber-space.**					**Effect Indicator: Percentage reduction in the number of successful cyber incidents and attacks on national networks and information systems.**		
Specific Objective: **1.1. Clear and robust cybersecurity governance structure**					**Outcome Indicator:** **Percentage of established and operational institutional structures under the National Cybersecurity Governance Framework.** **Number of aligned cybersecurity policies and procedures for cybersecurity management among relevant stakeholders.**		
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
M 1.1.1. Development of a clear organizational schema for the Government's cybersecurity structure.	**A 1.1.1.1. Development of a clear organizational schema for the Government's cybersecurity structure.**	**National Council for Digital Transformation of Society, MDT**	**1/2025**	**4/2025**	**0**	**No financial resources required**	**No financial resources required** **Percentage of organizational chart completion:** **Initial value: 0%** **Interim value after 6 months: 50%** **Final value: 100% after 12 months, by the end of 2025.**
M 1.1.2. Establishment of clear government policies for communication and cooperation,	**A 1.1.2.1. Communication and cooperation plan.**	**MDT, National Council for Digital Transformation of Society**	**1/2025**	**4/2025**	**307.500 MKD**	**Budget of the leading activity subject**	**Percentage of completion of the communication and cooperation plan:** **Initial value: 0%** **Interim**

with defined roles and responsibilities related to cybersecurity.							**value: 70% of the plan to be prepared within 3 months Final value: 100% after 12 months, by the end of 2025.**
	A 1.1.2.2. Revision of the communication plan.	**MDT, National Council for Digital Transformation of Society**	**1/2026**	**4/2027**	**615.000 MKD**	**Budget of the leading activity subject**	**Completed annual revision. Initial value: 0 in January 2026; Interim value: 1 by the end of 2026; Final value: 2, for two revisions of the plan by the end of 2027.**
M 1.1.3. New legal framework for cybersecurity that will define the national cybersecurity framework.	**A 1.1.3.1. Cybersecurity Law**	**MDT, National Council for Digital Transformation of Society, intersectoral working group**	**1/2025**	**4/2025**	**1.230.000**	**International assistance**	**Result: Adopted cybersecurity law – The legal text to be approved by the Assembly within 12 months, by the end of 2025.**
M 1.1.4. Integration of the National Cybersecurity Council into the National Council for Digital Transformation.	**A 1.1.4.1. Amendment of the Decision on the Formation of the National Council for Digital Transformation of Society**	**MDT, National Council for Digital Transformation of Society**	**1/2025**	**4/2025**	**0**	**No financial resources required**	**Result: Adopted amendment to the decision – The amendment to be officially approved by the government or competent body during 2025.**
M 1.1.5 Formalization of existing working groups and establish-	**A 1.1.5.1. Formalization of CICWG**	**MDT, Ministry of Defence (MO), Ministry of Internal Affairs (MVR), MKD - CERT,**	**1/2025**	**4/2025**	**0**	**No financial resources required**	**Result: Formalization of CICWG – CICWG to be officially recognized**

ment of new ones related to cybersecurity protection.		National Security Agency (NSA), Army (AR), Directorate for Security of classified information, Universities, Civil Sector, Private and Public Sector Planned start: 1/2025					and formalized by the government or MDT by the end of 2025.
	A 1.1.5.2. Activities of CICWG	MDT, Ministry of Defence (MO), Ministry of Internal Affairs (MVR), MKD - CERT, National Security Agency (NSA) Intelligence Agency, Directorate for Security of classified information, Universities, Civil Sector, Private and Public Sector.	1/2025	4/2027	3,690,000ден	International assistance	Implementation of CICWG activities – Successful execution of activities contributing to increased national cybersecurity. Initial value: 70% of the annual planned activities completed in 2025; Interim value: 85% of the annual planned activities completed in 2026; Final value: 100% of the annual planned activities completed in 2027.
	A 1.1.5.3. New Working Groups	MDT National Council for Digital Transformation of Society	1/2025	4/2027	2,460,000	International assistance	At least 4 workshops/meetings held in one year for each working group.

M 1.1.6. Development of specialized training and education programs for cybersecurity for employees in the public sector.	A 1.1.6.1. Development of specialized cybersecurity training programs for employees in the public sector.	MPA, MDT, National Council for Digital Transformation of Society	1/2025	4/2027	0	No financial resources required	At least one specialized training per year, with the program reviewed at least once annually.
	A 1.1.6.2. Partnership with universities to create degree and certification programs tailored to the needs of the public sector.	MPA, MDT, National Council for Digital Transformation of Society, Universities	1/2025	4/2027	0	No financial resources required	Review of programs at least once annually.
M 1.1.7. Strengthening public-private partnerships and knowledge sharing in cybersecurity.	A 1.1.7.1. Establishment of cybersecurity hubs where public sector employees, universities, and private sector organizations will collaborate on knowledge sharing and information exchange.	MDT, Ministry of Social Policy, Demography and Youth, Chambers of Commerce and private sector organizations associations	1/2025	4/2027	3,690,000	International assistance	Number of workshops, seminars, or collaboration meetings held for each hub. Initial value: 1 per year in 2025; Interim value: 4 per year in 2026; Final value: 12 per year in 2027.
	A 1.1.7.2. Workshops for cybersecurity professionals in the public sector, focusing	MDT, MKD-CIRT	1/2025	4/2027	3,690,000	International assistance	Number of workshops organized each year. Initial value: 1 per year in 2025; Interim value: 2 per year in

	on knowledge sharing, new cyber threats, and infrastructure protection.						2026; Final value: 4 per year in 2027.
M 1.1.8. Practical workshops for public sector employees,focusing on incident response and infrastructure protection.	A 1.1.8.1. Design and implementation of practical workshops and training for incident response and infrastructure protection.	MDT, MKD-CIRT	1/2025	4/2027	3,690,000	International assistance	Evaluation of knowledge gained after the workshop/training. Initial value: In 2025, 70% of participants successfully complete the final assessment. Interim value: In 2026, 80% of participants successfully complete the final assessment. Final value: In 2027, 90% of participants successfully complete the final assessment.
M 1.1.9. Specific career pathways and career development programs for cybersecurity roles in the public sector.	A 1.1.9.1. Needs analysis and development of a plan for recruitment and retention of cybersecurity professionals in the public sector.	MДТ, Ministry of Social Policy, Demography, and Youth, Bureau for Development of Education, Center for the Development of Vocational Education, Ministry of Education,	1/2025	4/2025	1.230.000	International assistance	Development and adoption of a plan for recruitment and retention of cybersecurity professionals in the public sector by the end of 2025.

		National Council for Digital Transformation of Society, Universities					
	A 1.1.9.2. Amendments and additions to the legislation for competitive salary compensation for cybersecurity professionals in the public sector, in line with the labour market.	MDT, All relevant stakeholders	1/2025	4/2026	0	No financial resources required	Proposed legislation with competitive salary compensation for cybersecurity professionals, to be adopted within 12 months of initiating the activity.
	A 1.1.9.3. Building career development programs with clear pathways from entry-level to senior roles in cybersecurity within the public sector.	MDT, Ministry of Social Policy, Demography, and Youth, Bureau for Development of Education, Center for the Development of Vocational Education, Ministry of Education, National Council for Digital Transformation of Society	1/2025	4/2026	2.460.000	International assistance	Percentage of public sector institutions with implemented career development programs.
	A 1.1.9.4. Development of sponsored certification programs for cybersecurity professionals,	MDT, Ministry of Social Policy, Demography, and Youth, Bureau for Development of Education, Center for	1/2026	4/2027	1.230.000	International assistance	Percentage of employees who successfully obtain certification upon completion of the training/program.

	public sector employees, focused on practical skills for infrastructure protection.	the Development of Vocational Education, Ministry of Education, National Council for Digital Transformation of Society					Initial value: By September 2026, at least 70% of participating employees will successfully complete certification. Interim value: By April 2027, at least 80% of participating employees will successfully complete certification. Final value: By the end of 2027, at least 90% of participating employees will successfully complete certification.
M 1.1.10. Development of incentives for employees who retrain for cybersecurity roles in the public sector.	A 1.1.10.1. Incentive plan, such as scholarships and bonuses, for employees who retrain for cybersecurity roles.	MDT, Ministry of Education, Bureau for Development of Education, Center for the Development of Vocational Education, National Council for Digital Transformation of Society	1/2026	4/2027	1.230.000	International assistance	1: Increased motivation for retraining, measured by the percentage of employees receiving incentives who provide positive feedback on the retraining program. Initial state: In 2025, 70% of employees who received incentives report positive feedback. Interim state: In

							2026, 85% of employees who received incentives report positive feedback. Final state: In 2027, 90% of employees who received incentives report positive feedback. 2: Increased number of employees in cybersecurity – A 5% annual increase in the number of qualified employees in cybersecurity in the public sector through retraining.
M 1.1.11. International cooperation for developing cybersecurity talent.	**A 1.1.11.1. Development of exchange programs within the EU, NATO, and partner countries for training, knowledge sharing, and best practices in cybersecurity training for the public sector.**	**Ministry of European Affairs NDT, Ministry of Foreign Affairs and Foreign Trade, MPA**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**1: Increased knowledge and skills in cybersecurity, measured by the percentage of participants showing a significant increase in knowledge and skills after completing the programs. Initial state: In 2025, 80% of participants show significant improvement. Interim**

							state: In 2026, 85% of participants show significant improvement. Final state: In 2027, 90% of participants show significant improvement. 2: Enhanced international cooperation – Establishment of lasting relationships and projects with the EU, NATO, and partner countries contributing to the improvement of cybersecurity..
	M 1.1.11.2. Promoting cross-border cooperation by enabling cybersecurity professionals to gain international experience.	Ministry of Foreign Affairs and Foreign Trade, MDT	1/2025	4/2027	0	No financial resources required	More professionals with international experience – Increase in the number of professionals with international experience by 10% annually, measured from 2025.

Specific Objective: 1.2. Establishment of Cybersecurity Sector within the Ministry of Digital Transformation.	Outcome Indicator: Percentage of established and functional institutional structures within the Cybersecurity Sector at the Ministry of Digital Transformation.

Measures	Activities	Leading Subjects and other Subjects	Start date (quarter)	Planned execution date (quarter)	Estimated Required Resources	Source of Funding	Result Indicator (linked to the meas-

							ure/activ-ity)
M 1.2.1. National Authority responsible for cybersecurity and Single Point of Contact (SPOC) for cyber-security.	A 1.2.1.1. Operation-alization of the Cyber-security Sector (SSB).	MDT	1/2025	4/2027	107,625,000 MKD.	Budget of the leading activity entity	Percentage of completion of the operationalization of the Cyber-security Sector (SSB). Initial value: 0% in 2025 Interim value: 50% in 2026 Final value: 80% in 2027.
	A 1.2.1.2. Establishment of the National Authority Responsible for Cyber-security	MDT	1/2025	4/2027	0	No financial resources required	Time to establish the authority – The National Authority should be established and operational within 6 months from the initiation, by the end of 2025.
	A 1.2.1.3. National Single Point of Contact for Cyber-security (SPOC)	МДТ	1/2025	4/2027	0	No financial resources required	Time to establish SPOC – SPOC should be established and operational within 6 months from initiation, by the end of 2025.

M 1.2.2. Government Security Operations Center (SOC) for preventive monitoring and care of cybersecurity for the networks, systems, and services of MDT and the Government	**A 1.2.2.1. Security monitoring of government networks, systems, and services**	**MDT, National Council for Digital Transformation of Society, MKD-CIRT**	**1/2026**	**4/2027**	**24,600, MKD.**	**Budget of the leading subject of the activity**	**Average time to resolve 90% of security issues within the SOC Initial value: 12 hours by September 2026; Transitional value: 6 hours by April 2027; Final value: Resolve 90% of identified issues within 3 hours by the end of 2027.**
	A 1.2.2.2. Government team for responding to computer security incidents – Government CSIRT, as part of the Government SOC;	**MDT**	**1/2026**	**4/2027**	**0**	**No financial resources required**	**Incident response time The response time for significant incidents, from the moment of notification, should not exceed: Initial value: 24 hours by September 2026; Transitional value: 8 hours by April 2027; Final value: 2 hours by the end of 2027.**

	A 1.2.2.3. Cooperation with the national CSIRT and other government institutions and organizations in the country	**MDT MKD-CIRT, Military CIRT**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**1. Frequency of coordination between government institutions – Minimum of 4 meetings per year for coordination and information sharing between government institutions. 2. Percentage of timely shared incident information – 100% of cyber incident information to be shared within 12 hours after identification.**
M 1.2.3. International cooperation and building strategic partnerships	**A 1.2.3.1. Cooperation with the European Union organizations and networks responsible for managing large-scale incidents and crises (EU-CyCLONe)**	**MDT, MEA**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**1.Frequency of communication with EU-CyCLONe – Regular communication with European Union networks, at least once per quarter. 2.Frequency of par-**

							ticipation in crisis simulations and exercises – Participation in at least 1 simulation or crisis exercise organized by EU-CyCLONe per year.
M 1.2.4. National authority for coordination and management of large-scale computer security incidents and crises	**A 1.2.4.1. National authority for coordination and management of large-scale computer security incidents and crises**	**MDT MKD-CIRT, Military CIRT, National Council for Digital Transformation of Society**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Time for establishing the national authority – The authority must be fully functional by the end of 2027. Initial value: 0 in 2025 Transitional value: 1 in 2026 (established) Final value: 2 in 2027 (fully functional)**
M 1.2.5. Preparation of strategic documents and policies and monitoring the implementation of the Cybersecurity Strategy and Action Plan, and other strategic documents	**A 1.2.5.1. Preparation of strategic documents and policies and monitoring the implementation of the Cybersecurity Strategy and Action Plan, and other stra-**	**MDT, National Council for Digital Transformation of Society**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Number of Strategy revisions (successful implementation) – Carrying out at least 1 revision annually to update and monitor pro-**

	tegic documents						**gress.**
M 1.2.6. Establishing standards, measures, and controls for cybersecurity for government networks, systems, and services, and for the public sector	**A 1.2.6.1. Establishing standards, measures, and controls for cybersecurity for government networks, systems, and services, and for the public sector**	**MDT National Council for Digital Transformation of Society, MKD-CIRT**	**1/2025**	**4/2027**	**2,460,000 MKD**	**Budget of the leading activity subject**	**Percentage of government institutions that have implemented the standards – Initial value: 35% in 2025; Transitional value: 50% in 2026; Final value: 75% in 2027.**
M 1.2.7. Supervision of public sector institutions' compliance with prescribed standards, measures, and controls	**A 1.2.7.1. Supervision of public sector institutions' compliance with prescribed standards, measures, and controls**	**MDT Inspection Council**	**1/2025**	**4/2027**	**1.230.000 MKD**	**Budget of the leading activity subject**	**1. Number of annual supervisions of public sector institutions – Perform at least: Initial value: 0 in 2025; Transitional value: at least 5 in 2026; Final value: minimum 10 supervisions in 2027.**
<u>Specific Objective:</u> 1.3. Increased capacities for defence operations in cyberspace			**Outcome Indicator: Operational capacities for cyber defence within the Army of the Republic of North Macedonia**				

M 1.3.1. Enhancement of capacities for military cyber operations through the development of a comprehensive strategy for improving the cyber operations capacities of the military, including the formation of a military team for responding to cybersecurity incidents	**A 1.3.1.1. Cyber defence strategy**	**MoD ARM**	**1/2025**	**4/2025**	**1.230.000 MKD.**	**Budget of the leading activity subject**	**Adopted cybersecurity defence strategy by the end of 2025.**
	A 1.3.1.2. Formation of a military team for responding to cybersecurity incidents	**MD Stakeholders**	**1/2025**	**4/2027**	**18,204,000 MKD.**	**Budget of the leading activity subject**	**Operational team by 2027.**
M 1.3.2. Development of cybersecurity defence capabilities for national and military needs through the creation of a solid framework for the deployment of cybersecurity defence capabilities as needed for the protection of national security and military operations;	**A 1.3.2.1. Development of cybersecurity defence capabilities for national and military needs through the creation of a solid framework for the deployment of cybersecurity defence capabilities as needed for the protection of national security and military operations**	**ARM MoD**	**1/2025**	**4/2027**	**4,305,000ден.**	**Budget of the leading activity subject**	**Established framework for deploying cybersecurity defence capabilities for national security protection.**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: Secure, safe and resilient society -**			
General Objective: **Ensuring the security, confidentiality, and resilience of critical networks, information systems, and essential and important entities.**				**Effect Indicator:** **Level of improvement in the security, confidentiality, and resilience of critical networks and information systems, measured through the success of developed national risk management frameworks, implemented protection measures, and the effectiveness of public-private cooperation.**			
<u>Specific Objective 2.1:</u> Risk and threat management and monitoring				**Outcome Indicator:** **Level of effectiveness in risk and threat management, measured through the degree of identification, assessment, and management of cyber risks and threats at the national level.**			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
M 2.1.1 National Framework for Risk Assessment Related to Cybersecurity	**A 2.1.1.1 Preparation and Adoption of a National Framework for Cybersecurity Risk Management with Methodology:**	**MDT, Essential and Important Entities**	**1/2025**	**4/2025**	**1.537.500**	**Budget of leading institution**	**Indicator: Full implementation of the framework at the national level. Initial value: 0%, Intermediate value after 6 months: 50%, Final value: 100% after 12 months, by the end of 2025.**
M 2.1.1 National Framework for Risk Assessment Related to Cybersecurity	**A 2.1.1.2 Revision of the National Framework for Cybersecurity Risk Management:**	**MDT, Essential and Important Entities**	**1/2026**	**4/2027**	**922,500 MKD**	**Budget of the leading institution of the activity.**	**Improved efficiency of the framework after the revision. Initial value: 0%; Transition value by the end of 2027: 35%; Final value: 70% of institutions to report improved effectiveness in risk manage-**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: Secure, safe and resilient society -				
							ment after the revision by the end of 2027.
M 2.1.1 National framework for risk assessment related to cybersecurity	A.2.1.1.3. Training for essential and important entities on risk assessment	MDT, MKD CIRCT, Essential and important entities	1/2026	4/2027	2,460,000 MKD	Budget of the leading institution for the activity	Increased preparedness of institutions for risk assessment – Measurable improvement in the ability of institutions to identify and assess risks within 1 year after the training is completed.
M 2.1.1 National Framework for Cybersecurity Risk Assessment	A.2.1.1.4. Supervision of public sector institutions' compliance with prescribed risk assessments	MDT, MKD CIRT, Essential and Important Entities	1/2027	4/2027	1.230.000	Budget of the leading institution for the activity	1. Full compliance of institutions with risk assessments. Initial value: 0% – Transitional value: 50% of institutions to be compliant with risk assessments within 2 years. Final value: 70% of institutions to be compliant with risk assessments within 3 years. 2
M.2.1.2 Operational and Organizational Measures for Managing Risks Related to the Security of Network and Information Sys-	A.2.1.2.1 Operational and Organizational Measures for Managing Risks Related to the Security of Network and Inform-	MKD-CIRT, National Council for Digital Transformation of Society	1/2025	4/2027	1,845,000 MKD	Budget of the leading institution for the activity	, Achieved full compliance with the prescribed measures – 100% compliance of essential and important entities with the implemented meas-

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: Secure, safe and resilient society -**				
tems for Essential and Important Entities;	**ation Systems for Essential and Important Entities;**						**ures within 4 years. Initial value: 0% in 2025. Transitional value: 35% in 2026. Final value: 70% in 2027.**
M.2.1.3 Supervision of Essential and Important Entities in the Implementation of Prescribed Measures, Controls, and Risk Assessment	**A.2.1.3.1 Establishment of Supervision over Essential and Important Entities in the Implementation of Prescribed Measures, Controls, and Risk Assessment**	**MDT, MKD-CIRT, National Council for Digital Transformation of Society**	**1/2026**	**4/2026**	**1.230.000**	**Budget of the leading institution for the activity**	**Functional supervisory system – Established and operational supervisory system that is regularly applied to all relevant entities.**
M.2.1.3 Supervision of Essential and Important Entities in the Implementation of Prescribed Measures, Controls, and Risk Assessment	**A.2.1.3.2 Implementation of Supervision over Essential and Important Entities in the Implementation of Prescribed Measures, Controls, and Risk Assessment**	**MDT, MKD-CIRT, National Council for Digital Transformation of Society**	**1/2026**	**4/2027**	**0**	**No financial resources required**	**Effective risk reduction due to supervision – 30% reduction in risks related to non-compliance within one year after the implementation of supervisory activities. Achieved continuous compliance – 70% of entities to achieve full compliance after the second round of supervision.**
M.2.1.4 Vulnerability Management, Including the Promotion	**A.2.1.4.1 Policy for Vulnerability Management, Including the**	**MDT, MKD-CIRT,**	**1/2026**	**4/2027**	**615.000**	**Budget of the leading institution for the**	**1. Reduction in the number of critical vulnerabilities in network and information**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: Secure, safe and resilient society -**				
and Facilitation of Coordinated Vulnerability Disclosure	**Promotion and Facilitation of Coordinated Vulnerability Disclosure**					**activity**	**systems on a quarterly, semi-annual, and annual basis.**
M.2.1.4 Vulnerability Management, Including the Promotion and Facilitation of Coordinated Vulnerability Disclosure	**A.2.1.4.2 Training for Essential and Important Entities on Vulnerability Management**	**MDT, MKD-CIRT,**	**1/2026**	**4/2027**	**2,460,000 MKD**	**Budget of the Leading Institution for the Activity**	**1. Increased Vulnerability Management Capability – 85% of participants to report improved ability to identify and manage vulnerabilities after completing the training.**
M.2.1.4 Vulnerability Management, Including the Promotion and Facilitation of Coordinated Vulnerability Disclosure;	**A.2.1.4.3 Information Sharing on Vulnerabilities**	**MDT, MKD-CIRT,**	**1/2026**	**4/2026**	**0**	**No financial resources required**	**Timely Information Sharing Within 24 Hours**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
General Objective: Ensuring the security, confidentiality, and resilience of critical networks, information systems, and essential and important entities.				**Effect Indicator:** Level of improvement in the security, confidentiality, and resilience of critical networks and information systems, measured through the success of developed national risk management frameworks, implemented protection measures, and the effectiveness of public-private cooperation.			
Specific Objective 2.2: Secure and resilient essential and important entities				**Outcome Indicator:** Level of security and resilience of essential and important entities, measured through the implementation of protection measures and their ability to withstand cyberattacks and threats.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
M.2.2.1. Improving the Resilience of Essential and Important Entities	**A.2.2.1.1. Establishing Policies for Risk Analysis and Security of Information Systems**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2025**	**4/2027**	**3,690,000 MKD**	**Budget of the leading institution for the activity**	**Reduction of risks by 30% – Reduction of identified risks in the current period compared to the previous year.**
M.2.2.1. Improving the Resilience of Essential and Important Entities	**A.2.2.1.2. Development, review, and updating of Business Continuity Plans and Crisis Management Plans.**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2025**	**4/2027**	**2,767,500 MKD**	**Budget of the leading institution for the activity**	**Improvement of crisis resilience. Starting value: 0% in 2025, Transitional value: 35% in 2026, Final value: 70% in 2027. 70% of institutions should demonstrate improvement in crisis scenarios, through reports on conducted exercises and tests.**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**				
M.2.2.1. Improvement of resilience of essential and important entities	**A.2.2.1.3. Implementation of Supply Chain Security Measures**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2025**	**4/2027**	**922,500 MKD**	**Budget of the leading institution for the activity**	**1. Reduction of supply chain-related risks – Reduction of supply chain incidents by 30% annually.**
M.2.2.1. Improvement of resilience of essential and important entities	**A.2.2.1.4. Assessment of cybersecurity risk management measures**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Reduction of risks by 30% - Reduction of identified cybersecurity risks annually.**
M.2.2.1. Improvement of resilience of essential and important entities	**A.2.2.1.5. Basic Cyber Hygiene Practices and Cybersecurity Training**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2026**	**4/2027**	**3,075,000 MKD**	**Budget of the leading institution for the activity**	**1: Increased awareness of cyber hygiene – More than 85% of participants should report an increased understanding of cyber hygiene after completing the annual training. 2: Reduction in incidents related to human factors annually.**
M.2.2.1. Improvement of resilience of essential and important entities	**A.2.2.1.6. Policies and Procedures Regarding the Use of Cryptography and, Where Appropriate, Encryption**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2026**	**4/2027**	**922,500 MKD**	**Budget of the leading institution for the** activity	**1. Increased data protection – Reduction in reported incidents related to encryption on an annual basis.**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**				
M.2.2.1. Improvement of resilience of essential and important entities	**A.2.2.1.7. Human Resources Security, Access Control Policies, and Asset Management**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2026**	**4/2027**	**922,500 MKD**	**Budget of the leading institution for the activity**	**1. Reduction in reported incidents related to human resources on an annual basis.**
M.2.2.1. Improvement of resilience of essential and important entities	**A.2.2.1.8. Use of Multi-factor Authentication or Continuous Authentication Solutions**	**MDT, MKD-CIRT, Essential and Important Entities**	**1/2026**	**4/2027**	**24,600,000 MKD**	**Budget of the leading institution for the activity**	**1 Improved access security – Reduction in compromised access to critical systems on an annual basis. 2. Full implementation of authentication – 100% of entities to apply Multi-Factor Authentication (MFA) for critical systems and services within 4 years.**
M.2.2.2. Government Security Operations Center (SOC) for preventive monitoring and care of cybersecurity for the networks, systems, and services of MDT and the Govern-	**A.2.2.2.1. Creation of sectoral CSIRT and SOC structures for essential and important entities.**	**MDT, Essential and Important Entities,**	**1/2025**	**4/2027**	**196,800,000 MKD**	**Budget of the leading institution for the activity**	**1. Increased speed and efficiency in incident response – At least 90% of entities to report improvement in the time and quality of incident response.**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**				
ment							
M.2.2.2. Government Security Operations Center (SOC) for preventive monitoring and care of cybersecurity for the networks, systems, and services of MDT and the Government	**A.2.2.2.2. Procedures for handling cybersecurity incidents;**	**MDT, Essential and Important Entities,**	**1/2025**	**4/2027**	**3,075,000 MKD**	**Budget of the leading institution for the activity**	**1. Improved incident response – Reduction in incident response time on an annual basis.**
M.2.2.2. Government Security Operations Center (SOC) for preventive monitoring and care of cybersecurity for the networks, systems, and services of MDT and the Government	**A.2.2.2.3. Security in the use, development, and maintenance of networks and information systems, including vulnerability management and detection.**	**Essential and Important Entities,**	**1/2025**	**4/2027**	**36,900,000 MKD**	**Budget of the leading institution for the activity**	**1. Increased protection of networks and systems – Decrease in the number of successful cyberattacks due to vulnerabilities on an annual basis.**
ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5 "Secure, safe and resilient society"**				

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
General Objective: Ensuring the security, confidentiality, and resilience of critical networks, information systems, and essential and important entities.				**Effect Indicator:** Level of improvement in the security, confidentiality, and resilience of critical networks and information systems, measured through the success of developed national risk management frameworks, implemented protection measures, and the effectiveness of public-private cooperation.			
Specific Objective 2.3: Improved security of national networks and information systems				**Outcome Indicator:** Level of security and resilience of essential and important entities, measured through the implementation of protection measures and their ability to withstand cyberattacks and threats.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
M.2.3.1. Minimum set of technological and organizational measures for cybersecurity	**A.2.3.1.1. Defining the minimum set of technological and organizational measures for cybersecurity**	**MDT, Essential and Important Entities**	**1/2025**	**4/2027**	**1,230,000 MKD**	**Budget of the leading institution for the activity**	**1 Risk reduction due to the implementation of measures – A 30% reduction in identified technological and organizational risks after implementation.**
M.2.3.1. Minimum set of technological and organizational measures for cybersecurity	**A.2.3.1.2. Revision of the minimum set of technological and organizational measures for cybersecurity**	**MDT, Essential and Important Entities**	**1/2027**	**4/2027**	**615.000**	**International Assistance**	**At least 70% of institutions should be compliant with the revised measures and international standards.**
M.2.3.2. Support for implementation and oversight of compliance with the minimum	**A.2.3.2.1 Support for implementation and oversight of compliance with the minimum**	**MDT, Essential and Important Entities**	**1/2027**	**4/2027**	**0**	**No financial resources needed**	**1. Full compliance with technological and organizational measures – 95% of all relevant in-**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**				
set of technological and organizational measures for cybersecurity	**set of technological and organizational measures for cybersecurity**						**stitutions should achieve compliance with technological and organizational measures within 4 years.**
M.2.3.3. Security accreditation of communication and information systems through which classified information is processed.	**A.2.3.3.1. Procurement of equipment for TEMPEST zoning of facilities.**	**Directorate for security of classified information**	**1/2025**	**4/2025**	**12.300.000**	**Budget of the leading institution for the activity**	**Implementation of procurement and training for the use of equipment.**
M.2.3.3. Security accreditation of communication and information systems through which classified information is processed.	**A.2.3.3.2. Training for specialized personnel.**	**Directorate for security of classified information**	**1/2025**	**4/2027**	**1,845,000 MKD**	**Budget of the leading institution for the activity**	**Successful completion of training for a minimum of 80% of specialized personnel on an annual basis.**
M.2.3.3. Security accreditation of communication and information systems through which classified information is processed.	**A.2.3.3.3. Procurement of cryptographic equipment and software**	**Directorate for security of classified information, Stakeholders**	**1/2025**	**4/2027**	**18,450,000 MKD**	**Budget of the leading institution for the activity**	**Increased security of classified information handled in Information and Communication Systems (ICS) on an annual basis.**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems			**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**				
M.2.3.3. Security accreditation of communication and information systems through which classified information is processed.	**A.2.3.3.4. Procurement of TEMPEST equipment**	**Directorate for security of classified information, Stakeholders**	**1/2025**	**4/2027**	**3,690,000 MKD**	**Budget of the leading institution for the activity**	**Increased security of classified information handled in Information and Communication Systems (ICS) on an annual basis.**
M.2.3.3. Security accreditation of communication and information systems through which classified information is processed.	**A.2.3.3.4. Construction of security zones**	**Directorate for security of classified information, Stakeholders**	**1/2025**	**4/2027**	**3,690,000 MKD**	**Budget of the leading institution for the activity**	**Increased security of classified information handled in Information and Communication Systems (ICS) on an annual basis.**
M.2.3.3. Security accreditation of communication and information systems through which classified information is processed.	**A.2.3.3.5. Development of a new Regulation for cryptographic protection**	**Ministry of Defence, ARM, Ministry of Interior, Ministry of Foreign Affairs and Foreign Trade, Directorate for security of classified information Intelligence Agency, National Security Agency, Crisis Manage-**	**1/2025**	**4/2025**	**123.000**	**Budget of the leading institution for the activity**	**The regulation adopted by the Government of the Republic of North Macedonia.**

ACTION PLAN (2025-2027) FOR 2025-2028 CYBERSECURITY STRATEGY IMPLEMENTATION							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
		ment Centre					

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
General Objective: Ensuring the security, confidentiality, and resilience of critical networks, information systems, and essential and important entities.			**Effect Indicator:** Level of improvement in the security, confidentiality, and resilience of critical networks and information systems, measured through the success of developed national risk management frameworks, implemented protection measures, and the effectiveness of public-private cooperation.				
Specific Objective 2.4: Recommendations for the use of security technology in society				**Outcome Indicator:** The level of implementation of security technologies and alignment with recommendations, as well as the degree of awareness and acceptance of security technologies by various entities in society.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
M.2.4.1. Policy for Inclusion and Specification of Cybersecurity Requirements for	**A.2.4.1.1. Policy for Including and Specifying Cybersecurity Requirements for ICT**	**MDT, MKD-CIRT, National Council for Digital Transformation of Society**	**1/2026**	**4/2027**	**922,500 MKD**	**International Assistance**	**1Improved Cybersecurity of Procured ICT Products and Services – Institutions should incorporate cybersecurity requirements in**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
ICT Products and ICT Services in Public Procurement	**Products and ICT Services in Public Procurement**						**ICT procurements.**
M.2.4.2. Registry of Secure New Technologies	**A.2.4.2.1. Registry of Secure New Technologies**	**MDT, MKD-CIRT, National Council for Digital Transformation of Society**	**1/2026**	**4/2027**	**922,500 MKD**	**International Assistance**	**Reduction in incidents and problems caused by insecure technologies after the implementation of the registry.**
M.2.4.3. Register of Technologies Representing High Security Risks	**A.2.4.3.1. Register of Technologies Representing High Security Risks**	**MDT, MKD-CIRT, National Council for Digital Transformation of Society**	**1/2026**	**4/2027**	**922,500 MKD**	**International Assistance**	**1. Reduction in the use of high-risk technologies on an annual basis after the registry implementation.**
M.2.4.4. Permanent inter-ministerial working group for monitoring new technologies	**A.2.4.4.1. Permanent inter-ministerial working group for monitoring new technologies.**	**MDT, MKD-CIRT, National Council for Digital Transformation of Society**	**1/2026**	**4/2027**	**922,500 MKD**	**International Assistance**	**Operational working group by the end of 2026.**

ACTION PLAN (2025-2027) FOR THE IMPLEMENTATION OF THE 2025-2028 CYBERSECURITY STRATEGY	
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems	**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**
General Objective: Ensuring the security, confidentiality, and resilience of critical networks, information systems, and essential and import-	**Effect Indicator:** Level of improvement in the security, confidentiality, and resilience of critical networks and information systems, measured through the success of developed national risk management frameworks, implemented protection

ACTION PLAN (2025-2027) FOR THE IMPLEMENTATION OF THE 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
ant entities.				measures, and the effectiveness of public-private cooperation.			
Specific Objective 2.5: Public-private sector partnership and collaboration				**Outcome Indicator:** Level of public-private cooperation in the implementation of cybersecurity measures and the effectiveness of partnerships in protecting against cyber threats.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
M.2.5.1. Multisectoral Working Group	**A.2.5.1.1. Establishment of a National Platform for Multisectoral Cooperation**	**MDT, Private Sector, Chambers of Commerce**	**1/2025**	**4/2027**	**5,535,000 MKD**	**International Assistance**	**1. Improved coordination between sectors – By 2027, 90% of users should report improved communication and cooperation through the platform.**
M.2.5.1. Multisectoral Working Group	**A.2.5.1.2. Development and Monitoring of Legal Framework: Legal solutions that will facilitate public-private partnerships, outsourcing contracts, and support from business chambers**	**MDT, Private Sector, Chambers of Commerce**	**1/2025**	**4/2027**	**615.000**	**International assistance**	**1Increased legal support for public-private partnerships – institutions (including subjects using these mechanisms) to report that the legal framework has facilitated the partnership.**
M.2.5.1. Multisectoral Working Group	**A.2.5.1.3. Encouraging Outsourcing Solutions: Creating programs**	**MDT, Private Sector, Chambers of Commerce**	**1/2026**	**4/2027**	**0**	**No financial resources needed**	**1. Increased use of outsourcing solutions in cybersecurity on an annual basis. 2. Improved**

ACTION PLAN (2025-2027) FOR THE IMPLEMENTATION OF THE 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 2: Security and Resilience of Essential and Important Entities, Networks, and Information and Communication Systems				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
	that will promote outsourcing in cybersecurity						**cybersecurity through outsourcing solutions – Reduction in security incidents after the introduction of outsourcing solutions on an annual basis.**
M.2.5.1. Multisectoral Working Group	**A.2.5.1.4. Strategic Plan for Public-Private Partnerships (PPP)**	**MDT, Private Sector, Chambers of Commerce**	**1/2026**	**4/2027**	**615.000**	**International Assistance**	**2. Increased investment through PPP projects on an annual basis.**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028CYBERSECURITY STRATEGY	
PRIORITY AREA 3: Cyber-Resilient Society	**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**
General Objective: Create a cybersecurity-resilient and society	**Effect Indicator:** Percentage of increased awareness and behavioural change in society regarding cybersecurity, the protection of children and young people on the internet, and critical thinking concerning cyber risks and disinformation.
Specific Objective 3.1: Raise awareness on cybersecurity and disinformation in cyberspace	**Outcome Indicator:** Percentage of increased awareness and understanding of cybersecurity and disinformation in cyberspace, measured through changes in behaviour and knowledge of the target group.

Measures	Activities	Leading Subjects and other Subjects	Start date (quarter)	Planned execution date (quarter)	Estimated Required Resources	Source of Funding	Result Indicator (linked to the measure/activity)
M.3.1.1. Plan for Improving General Cybersecurity Awareness, Including at Least the Necessary Measures	**A.3.1.1.1. Preparation and Adoption of a Plan for Improving General Cybersecurity Awareness, Including at Least the Necessary Measures**	**MDT, ME, Bureau for Development of Education, Center for the Development of Vocational Education, National Council for Digital Transformation of Society, MKD-CIRT**	**1/2026**	**4/2027**	**1.230.000**	**International Assistance**	**Adopted plan, reviewed annually.**
M.3.1.1. Plan for Improving General Cybersecurity Awareness, Including at Least the Necessary Measures	**A.3.1.1.2. Implementation of campaigns, creation of educational content.**	**MDT, ME, Bureau for Development of Education, Center for the Development of Vocational Education, National Council for Digital Transformation of Society, MKD-CIRT**	**1/2026**	**4/2027**	**1,230,000**	**International Assistance**	**1. Increased public awareness of cybersecurity – More than 75% of campaign participants to report a higher level of awareness (measured through surveys).**
M.3.1.1. Plan for improving the general level of cybersecurity awareness, including at least	**A.3.1.1.3. National platform for cybersecurity education**	**MDT, ME, Bureau for Development of Education,**	**1/2025**	**4/2027**	**9,225,000**	**International Assistance**	**Increased cybersecurity awareness and knowledge –**

the necessary measures		Center for the Development of Vocational Education, National Council for Digital Transformation of Society, MKD-CIRT					85% of platform users to report a higher level of cybersecurity awareness and knowledge after completing training and programs.
M.3.1.2. Plan for improving education in primary and secondary schools on critical thinking and protection against disinformation in cyberspace	A.3.1.2.1. Preparation and adoption of a Plan for improving the general level of cybersecurity awareness, including at least the necessary measures	Bureau for Development of Education, MDT, ME, Center for the Development of Vocational Education, Civil Sector	1/2026	4/2026	1.230.000	Budget of the leading institution for the activity	Adopted plan
M.3.1.2. Plan for improving education in primary and secondary schools on critical thinking and protection against disinformation in cyberspace	A.3.1.2.2. Implementation of the activities from the plan	Bureau for Development of Education, MDT, ME, Center for the Development of Vocational Education, Civil Sector	1/2026	4/2027	12,300,000	Budget of the leading institution for the activity	Implementation of the plan
M.3.1.2. Plan for improving education in primary and secondary schools on critical thinking and protection against disinformation in cyberspace	A.3.1.2.3. Revision and updating of the plan	Bureau for Development of Education (BDE), Ministry of Digital Transformation (MDT), Ministry of Education and Science (ME), Center for the Development of Vocational Education (CRVE), National Council for Digital Transform-	1/2027	4/2027	615.000	Budget of the leading institution for the activity	1.mplementation of the recommendations from the revision 2.Updated plan

		ation of Society (NSDTS), Civil Sector					
M. 3.1.3. Raise awareness and education on cybersecurity in primary and secondary education	A.3.1.3.1. Incorporation of cybersecurity concepts and thematic units into the curricula in primary and secondary education.	Bureau for Development of Education, MDT, ME, Center for the Development of Vocational Education, National Council for Digital Transformation of Society, Civil Sector	1/2026	4/2026	3.382.500	Budget of the leading institution for the activity	1.Percentage of curricula that include cybersecurity 2.Development of curricula and programs for cybersecurity 3.Number of students participating in cybersecurity training and programs 4.Creation of lessons on data protection and privacy 5.Assessment of knowledge and awareness of cybersecurity
M. 3.1.3. Raise awareness and education on cybersecurity in primary and secondary education	A.3.1.3.2. Educating and training teaching staff in primary and secondary schools in the field of cybersecurity and providing appropriate and up-to-date materials for students.	Bureau for Development of Education, MDT, ME, Center for the Development of Vocational Education, National Council for Digital Transformation of Society, Civil Sector	1/2026	4/2027	6,457,500	Budget of the leading institution for the activity	1.Percentage of teachers trained in cybersecurity Starting value: 0% in 2025, Target value: 50% in 2026, Final value: 85% in 2027. 2.Percentage of teachers who successfully apply cybersecur-

							ity in their teaching on an annual basis.
M. 3.1.3. Raise awareness and education on cybersecurity in primary and secondary education	**A.3.1.4.1. Acquiring knowledge and skills in cybersecurity concepts through study programs at higher education institutions.**	**Agency for Quality of Higher Education, Universities**	**1/2026**	**4/2026**	**3.075.000**	**Budget of the leading institution for the activity**	**1.Percentage of students with basic and advanced understanding of cybersecurity. 2.Percentage of graduates who start a career in cybersecurity. 3.Percentage of institutions offering accredited cybersecurity programs.**
M.3.1.5. Raising awareness and education on cybersecurity for employees in the public and private sectors	**A.3.1.5.1. Promotional activities**	**MDT, MKD-CIRT**	**1/2025**	**4/2027**	**922.500 MKD**	**Budget of the leading institution for the activity**	**Increased cybersecurity awareness – At least 80% of participants in the campaigns should report improved awareness and understanding of cybersecurity on an annual basis.**

M.3.1.5. Raising awareness and education on cybersecurity for employees in the public and private sectors	**A.3.1.5.2. Update of materials**	**МДТ, MKD-CIRT**	**1/2025**	**4/2027**	**922,500**	**Budget of the leading institution for the activity**	**Compliance with the latest cybersecurity standards on an annual basis – 100% of updated materials should be aligned with the latest cybersecurity practices.**
M.3.1.6. Mandatory cybersecurity training for all employees in the public sector.	**A.3.1.6.1. Implementing mandatory training for employees in the public sector**	**MDT, AA,**	**1/2025**	**4/2027**	**922,500**	**Budget of the leading institution for the activity**	**Successfully completed training: Starting value in 2025: 25%, Transition value in 2026: 50%, Final value in 2027: 80%**
M.3.1.6. Mandatory cybersecurity training for all employees in the public sector.	**A.3.1.6.2. Development and updating of cybersecurity training for employees in the public sector.**	**MDT, AA, National Council for Digital Transformation of Society , MKD-CIRT**	**1/2025**	**4/2027**	**922,500**	**Budget of the leading institution for the activity**	**Successfully completed training: Initial value in 2025: 25%, Transitional value in 2026: 50%, Final value in 2027: 80%.**

M.3.1.7. Raising awareness and education on cybersecurity for citizens.	**A.3.1.7.1. Creation of publicly available courses, multimedia campaigns, and media coverage for cybersecurity for citizens.**	**MDT, MKD-CIRT, Civil Sector**	**1/2025**	**4/2027**	**1,845,000**	**Budget of the leading institution for the activity**	**Increased awareness of cybersecurity among citizens – More than 70% of citizens who participated in the campaigns and courses to report increased awareness of cybersecurity through surveys.**
M.3.1.8. Coordination of activities for the development and implementation of education and training programs for cyber professionals	**A.3.1.8.1. Coordination of activities for the development and implementation of education and training programs for cyber professionals**	**MES, MDT, Universities**	**1/2025**	**4/2027**	**0**	**No financial resources needed**	**1.Percentage of success of the training based on the number of certified professionals. 2.Level of feedback from the industry on the quality of trained professionals.**
M.3.1.9. Development and equipping of the Cybersecurity and Digital Forensics Institute	**A.3.1.9.1 Development and implementation of education and training programs for cyber professionals**	**Military Academy, MDT, Ministry of Defence, MoI, MKD-CIRT, and other relevant stakeholders**	**1/2025**	**4/2027**	**4,612,500**	**Budget of the leading institution for the activity**	**1.Accredited 2 (two) second-cycle programs, and 1 (one) first-cycle program 2.Development of at least 10 courses 3.Implementation of at least 3 second-cycle studies during the period 4.At least**

							6 courses annually 5.Training of at least 30 professionals annually
M.3.1.9. Development and equipping of the Cybersecurity and Digital Forensics Institute	**A.3.1.9.2 Procurement and maintenance of equipment, services, and platforms for training, and other educational licenses.**	**Military Academy, MDT, Ministry of Defence, MoI, MKD-CIRT, and other relevant stakeholders**	**1/2025**	**4/2027**	**5,842,500**	**Budget of the leading institution for the activity**	**Renewal and maintenance of equipment to meet the standards for delivering appropriate training and education at the highest level.**
M.3.1.9. Development and equipping of the Cybersecurity and Digital Forensics Institute	**A.3.1.9.3 Training and licensing of teaching staff**	**Military Academy, MDT, Ministry of Defence, MoI, MKD-CIRT, and other relevant stakeholders**	**1/2025**	**4/2027**	**2,152,500**	**Budget of the leading institution for the activity**	**1.Five trainings conducted annually 2.Development of 7 trainers to be permanently employed, and up to 15 external trainers**
M.3.1.9. Development and equipping of the Cybersecurity and Digital Forensics Institute	**A.3.1.9.4 Organizing and participating in projects, conferences, exercises, professional debates, expert meetings, forums, initiatives, etc.**	**Military Academy, MDT, Ministry of Defence, MoI, MKD-CIRT, and other relevant stakeholders**	**1/2025**	**4/2027**	**2,460,000**	**Budget of the leading institution for the activity**	**1.One conference per year 2.One major exercise during the given period 3.Organization and participation in at least 2**

							profes-sional de-bates, ex-pert meet-ings, for-ums, and initiatives annually 4. Min-imum of 5 projects completed during the given period 5.At least 20 pub-lished pa-pers an-nually
M. 3.1.10. Devel-opment and up-grading of exist-ing institutes/cen-ters/laboratories for cybersecurity and digital forensics at rel-evant Macedonian universities.	**A. 3.1.10.1 Pro-curement of equipment, software, soft-ware licenses, and educa-tional licenses.**	**Universit-ies**	**1/202 5**	**4/2027**	**16,605, 000**	**Budget of the leading institu-tion for the activity**	**1.Percent-age of laborat-ories op-erating with the latest technolo-gies in cyberse-curity and forensics. 2.Student satisfac-tion as-sessment regarding resources and infra-structure in the laborat-ories3.Per-centage of activities supported by in-dustry partners.**
M. 3.1.10. Devel-opment and up-grading of exist-ing institutes/cen-ters/laboratories for cybersecurity and digital forensics at rel-evant Macedonian universities.	**A. 3.1.10.2 Training and certification of employees with internationally recognized cer-tificates in the field of cyber-security and digital forensics.**	**Universit-ies**	**1/202 5**	**4/2027**	**5,535,0 00**	**Budget of the leading institu-tion for the activity**	**1.Assess-ment of the effect-iveness of laborat-ories in delivering results for research projects. 2.Percent-age of laborat-**

							ories participating in international research networks. 3.Number of industry or academic events organized in the laboratories4.Success rate of students using laboratory resources for final and diploma projects.
M. 3.1.11. Continuous improvement of existing study programs at all cycles of higher education related to cybersecurity, creation of new ones, and accompanying activities related to cybersecurity and students.	**A. 3.1.11.1. Formation of professional studies in cybersecurity and digital forensics.**	**Universities, Ministry of Education**	**1/2026**	**4/2027**	**0**	**No financial resources needed**	**1.Evaluation of student satisfaction with cybersecurity study programs. 2.Percentage of successful projects and competitions in the field of cybersecurity. 3.Evaluation of the improvement of teaching staff in the field of cybersecurity.**

M. 3.1.11. Continuous improvement of existing study programs across all cycles of higher education related to cybersecurity, creation of new and supporting activities related to cybersecurity and students.	**A.3.1.11.2. Formation of additional professional master's programs in cybersecurity, digital forensics, and cybercrime.**	**Universities, Ministry of Education**	**1/2026**	**4/2027**	**0**	**No financial resources needed**	**1.Assessment of student satisfaction with cybersecurity study programs. 2.Percentage of successful projects and competitions in the field of cybersecurity. 3.Assessment of the advancement of faculty in the field of cybersecurity.**
M.3.1.11. Continuous improvement of existing study programs in all cycles of higher education related to cybersecurity, creation of new and complementary activities related to cybersecurity and students.	**A.3.1.11.3. Enhancement of existing studies in all cycles with topics related to cybersecurity**	**Universities, Ministry of Education, MDT**	**1/2025**	**4/2027**	**0**	**No financial resources needed**	**1.Assessment of student satisfaction with cybersecurity study programs 2.Percentage of successful projects and competitions in the field of cybersecurity 3.Evaluation of faculty advancement in the field of cybersecurity.**
M.3.1.11. Continuous improvement of existing study programs in all cycles of higher education related to cybersecurity, creation of new and complementary activities re-	**A.3.1.11.4. Improvement of technical capacities for the implementation of educational programs for cybersecurity**	**Universities, Ministry of Education, MDT**	**1/2025**	**4/2027**	**7,380,000**	**Budget of the leading institution for the activity**	**Percentage decrease in incidents on an annual basis**

lated to cybersecurity and students.							
M.3.1.11. Continuous improvement of existing study programs in all cycles of higher education related to cybersecurity, creation of new and complementary activities related to cybersecurity and students.	**A.3.1.11.5. Organization of national hackathons/competitions for students in cybersecurity**	**Universities, Ministry of Education, MDT**	**1/2025**	**4/2027**	**1,845,000**	**Budget of the leading institution for the activity**	**Number of organized hackathons, number of participants in the hackathons on an annual basis.**
M.3.1.11. Continuous improvement of existing study programs in all cycles of higher education related to cybersecurity, creation of new and complementary activities related to cybersecurity and students.	**A.3.1.11.6. Development and implementation of cybersecurity training, as well as recognized programs for the education of cybersecurity professionals**	**Universities, Ministry of Education, MDT**	**1/2025**	**4/2027**	**5,535,000**	**Budget of the leading institution for the activity**	**Number of conducted trainings, number of participants annually.**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 3: Cyber-resilient society				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
General objective: Create a cybersecurity-aware and resilient society				**Effect indicator:** Percentage of increased awareness and behavioral change in society regarding cybersecurity, protection of children and youth on the internet, and critical thinking about cyber risks and disinformation.			
Specific objective 3.2: Protection of children and youth online				**Outcome indicator:** Percentage of children and youth protected from online risks and trained to recognize and avoid potential internet threats.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**

M.3.2.1. Plan for protection of children and youth online	**A.3.2.1. 1 Development, adoption, implementation, monitoring, and revision of the plan.**	**MDT, Civil Sector**	**1/2025**	**4/2027**	**3,075,000**	**Budget of the leading institution for the activity**	**1. Improved awareness and knowledge due to the strategy – At least 80% of the affected groups (citizens, schools, employees in the public sector) should report increased knowledge about cybersecurity and internet risks.**
M.3.2.2. Mechanisms for reporting and monitoring online crimes against children.	**A.3.2.2. 1. Introduction and promotion of reporting mechanisms.**	**MoI, MDT, MKD-CIRT, Civil sector**	**1/2025**	**4/2027**	**0**	**No financial resources required.**	1.Percentage of reports that lead to the initiation of an investigation. 2. Percentage of cases that result in final judgments. 3. Evaluation of the effectiveness of the reporting platform. 4.Number of reported cases by types of online crime (sexual exploitation, manipulation, trafficking, etc.).
M.3.2.3. MDT initiative with internet providers for the promotion of filters to block harmful content for children.	**A.3.2.3. 1. Collaboration between MDT and Internet providers.**	**MoI, MDT, MKD-CIRT, Internet Providers**	**1/2026**	**4/2027**	**0**	**No financial resources required.**	**1.Reduction of access to harmful content for children – 50% reduction in access to harmful content for children within the first year of introducing filters, based on blocking statistics. 2.Increased use of protective filters by families – 80% of parents with internet access to use filters to block harmful content for children.**

M.3.2.4. Tools for parental control and safe internet browsing for younger users.	**A.3.2.4. 1 Collaboration between MDT and Internet providers.**	**MDT, MKD-CIRT, Internet Providers, Civil sector**	**1/2026**	**4/2027**	**4,305,000**	**International assistance**	**1.Increased protection for children during internet browsing – 50% reduction in exposure to harmful content for younger users within the first year after the implementation of the tools, based on tool statistics.**
M.3.2.5. National Center for a Safer Internet MK-SafeNet	**A.3.2.5. 1. Establishment of MK-SafeNet**	**MDT, Civil sector**	**1/2025**	**4/2027**	**17.183.961**	**Budget of the leading institution for the activity**	**1.Percentage of users receiving fast and effective assistance 2.Number of published educational resources (videos, articles, guides) 3.Percentage of active users of security tools and resources 4.User satisfaction level with MKSafeNet services**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 4: Minimizing the Impact of Cyber Incidents				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY (2024-2044): Priority Area 5: "Secure, safe and resilient society"**			
General Objective: Ensure timely and coordinated response to cyber incidents and crises				**Effect Indicator:** Percentage reduction in the number of cyber incidents affecting critical infrastructure and key services following the implementation of risk management measures and coordination.			
Specific Objective 4.1: Timely identification, reporting, and appropriate response to cyberattacks and significant incidents related to cyberspace.				**Outcome Indicator**: Percentage of affected entities (governmental and private) regularly reporting cyber incidents to the National CSIRT and other relevant authorities.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Result Indicator (linked to the measure/activity)**
M.4.1.1. Monitoring of networks and information sys-	**A.4.1.1.1. System for monitoring, detection, and response to**	**MKD-CIRT**	**1/2025**	**4/2027**	**64,575,000 MKD**	**Budget of the leading institution for the activity**	**Number of organizations/entities connected to the system (10 per year) Initial value**

tems of critical and important entities by MKD-CIRT and the Government CSIRT for government networks and systems	cyberattacks and incidents on infrastructure and endpoints of critical and important entities by MKD-CIRT.						(2025): 10 organizations Transition value after 1 year (2026): 20 organizations Final value after 3 years (2027): 40 organizations
	A.4.1.1.2. System for monitoring government networks, systems, and endpoints by the Government CSIRT	MKD-CIRT	1/2026	4/2027	30,750,000 MKD	Budget of the leading institution for the activity	Implementation time for the monitoring system: 12 months Indicator: Percentage of government networks covered (100% by the fifth year).
M.4.1.2. System for cooperation and information exchange, support for response and coordination in handling incidents	A.4.1.2.1. Development and implementation of systems and services for the exchange and sharing of information, knowledge, and experiences between the public, private, and defence-security sectors in the field of cybersecurity, aimed at protecting critical ICT systems and services.	MKD-CIRT MDT, Ministry of Defence, MoI, Ministry of Foreign Affairs and Foreign Trade , other stakeholders	1/2025	4/2027	11,070,000 MKD	Budget of the leading institution for the activity	Operational system in 2025 Measurement: System uptime with a target of 99.99% availability on an annual basis.
M.4.1.3. Establishment of a single point for reporting incidents and cybercrime, and further cooperation between the National CSIRT and	A.4.1.3.1. Memorandum of Cooperation between the Ministry of Interior (MVR), MKD-CIRT, and Government CSIRT	MKD-CIRT, MDT, MoI	1/2025	4/2025	0	No financial resources required	A memorandum of cooperation signed between the Ministry of Interior, MKD-CIRT, and the Government CSIRT, which includes defined obligations and procedures for coordination and information exchange in managing cyber incidents.

the Ministry of Interior, Computer Crime Department.	A.4.1.3.2 Development and Adoption of a Cooperation Procedure	MKD-CIRT, MDT, MoI	1/2025	4/2025	0	No financial resources required	Development within 3 months
	A.4.1.3.3 Working Group	MKD-CIRT, MDT, MoI	1/2025	4/2026	0	No financial resources required	A working group for cooperation between the Ministry of Interior (MVR), MKD-CIRT, and Government CSIRT has been formed and is operational. This group meets regularly and has defined procedures for coordination and response to cyber incidents.
	A.4.1.3.4. Promotion of reporting and communication channels.	MKD-CIRT, MDT, MoI	1/2025	4/2027	8,610,000 MKD	Budget of the leading institution for the activity	The initial value in 2025 is three promotions per year to launch a campaign for reporting incidents. The transitional value from 2026 onward is five promotions per year to increase awareness. The final value in 2027 is seven promotions per year to achieve high awareness and participation in incident reporting.
M.4.1.4. National categorization and classification of cyber incidents and attacks, and prioritization in their resolution.	A.4.1.4.1. Preparation and adoption of a proposal for the categorization and classification of cyber incidents, with developed procedures for initiation, coordination, and handling of different categories of incidents.	MKD-CIRT, MDT	1/2025	4/2026	922.500 MKD	International assistance	The initial value in 2025 is 0%, as the project begins and the communication and cooperation plan is in the design phase. After three months, 70% of the plan is expected to be prepared, with progress in defining key communication strategies and collaborations. By 2026, the final value should reach 90%, with a

							largely completed communication and cooperation plan, though some details may still need finalization.
	A.4.1.4.2. Workshops and exercises for educating involved stakeholders.	**MKD-CIRT, MDT,**	**1/2025**	**4/2027**	**369,000 MKD**	**Budget of the leading institution for the activity**	**Number of conducted workshops and exercises. The initial value for 2025 is four workshops per year to initiate organization. The transitional value for 2026 is six workshops annually, involving relevant institutions and private partners. The final value for 2027 is eight workshops per year, with expanded participation and advanced topics. Percentage of employees completing the training. The initial value for 2025 is 60% of employees starting the training. The transitional value for 2026 is 80% of employees completing the training. The final value for 2027 is 85% of employees completing the training with a high level of knowledge. Online workshops for educating stakeholders and exercises. The initial value for 2025 is one online workshop organized. The transitional value for 2026 is two online workshops annually for stakeholder education, with the promotion of incident report-**

							ing channels. The final value for 2027 is four online workshops per year, promoting the entire incident reporting process and the use of reporting forms.
M.4.1.5. Support for the establishment of well-equipped, staffed, and operational CSIRT teams in highly critical sectors and other critical sectors.	**A.4.1.5.1. Workshops for establishing CSIRT, SOC, and ISAC functions.**	**MKD-CIRT, MDT**	**1/2025**	**4/2026**	**1.845.000 MKD**	**Budget of the leading institution for the activity**	**Initial Value (2025): Successfully conducted one workshop on establishing CSIRT (Computer Security Incident Response Team), SOC (Security Operations Center), and ISAC (Information Sharing and Analysis Center) functions as an initial step for capacity building and preparation. Transitional Value (2025-2026): Two workshops. Final Value (2026): Three workshops.**
	A.4.1.5.2. Training for CIRT teams	**MKD-CIRT, MDT**	**1/2025**	**4/2026**	**0**	**No financial resources required**	**The initial value for 2025 includes the organization of one training session for CSIRT teams, with at least 60% of participants successfully completing the program and obtaining certification in cyber incident response. The transitional value for 2025-2026 entails the organization of two training sessions per year, with 70% of participants successfully completing the program and earning certification,**

							thereby increasing team preparedness. The final value for 2026 involves the organization of three training sessions per year, with 80% of participants successfully completing the program and obtaining certification in cyber incident response, ensuring enhanced readiness and efficiency of teams in handling cyber incidents.
M.4.1.6. Standardized operational procedures, rules, and obligations for cooperation and information exchange, support in response, and coordination in handling incidents between the National CSIRT team, the Government CSIRT, sectoral CSIRT teams, and other relevant stakeholders	**A.4.1.6.1. Development of procedures and rules for cooperation and information exchange, support in response, and coordination in handling incidents between the National CSIRT team, the Government CSIRT team, sectoral CSIRT teams, and other relevant stakeholders.**	**MKD-CIRT, MDT, Essential and Important Entities**	**1/2025**	**4/2026**	**1.230.000 MKD**	**Budget of the leading institution for the activity**	**Formal adoption of the procedure and rules by the National CSIRT team and sectoral CSIRT teams – Adoption of the procedure within six months.**

M.4.1.7. Mechanisms for detection and response to cyberattacks and incidents in organizations – essential and important entities	**A.4.1.7.1. Training for establishing mechanisms for detection and response to cyberattacks and incidents in essential and important entities.**	**MKD-CIRT, MDT, Essential and Important Entities**	**1/2025**	**4/2027**	**1,845,000 MKD**	**Budget of the leading institution for the activity**	**Initial value (2025): 10 organizations/entities connected to the monitoring systems of MKD-CIRT and the Government CSIRT. Transitional value (2026): 20 organizations/entities connected, with the continued process of including new entities into the monitoring system. Final value (2027): 40 organizations/entities connected to the monitoring systems of MKD-CIRT and Government CSIRT, with full progress achieved in ensuring security and cooperation in the field of cybersecurity.**
	A. 4.1.7.2. Reporting and information sharing	**MKD-CIRT, MDT**	**1/2026**	**4/2027**	**0**	**No financial resources required**	**Preparation of strategic and tactical information and reports**

M.4.1.8. Rapid Response Teams for Cyber Attacks and Incidents of National Importance	**A.4.1.8.1. Establishment of Rapid Response Teams for Cyber Attacks and Incidents**	**MKD-CIRT, MDT**	**1/2025**	**4/2026**	**0**	**No financial resources required**	**Number of reported cyber incidents. Number of rapid responses to incidents.**
	A.4.1.8.2 Quick response to incidents	**MKD-CIRT, MDT**	**1/2025**	**4/2027**	**46,125,000 MKD**	**Budget of the leading institution for the activity**	**Achieving rapid response by measuring the response time with 1 hour distance and 3 hours on-site.**
M. 4.1.9. National register of cyber-resources	**A.4.1.9.1 Establishing a National Register of Cyber-Resources**	**MDT, MKD-CIRT**	**1/2026**	**4/2027**	**10,455,000 MKD**	**Budget of the leading institution for the activity**	**1.Time for establishing the register – The national register should be established and functional within 12 months.** **2.Percentage of cyber-resources (personnel, equipment, services...) entered in the register – 80% of critical cyber-resources at the national level should be registered and documented within the first 12 months.** **Number of institutions using and updating data in the re-**

							gister – 100% of relevant government institutions and private partners should use and update the register on a regular basis within three years of its availability.

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 4: Minimizing the Impact of Cyber Incidents in Cyberspace				**ALIGNMENT WITH THE NATIONAL DEVELOPMENT STRATEGY: "A Secure, Safe, and Resilient Society"**			
GENERAL OBJECTIVE: Ensure timely and coordinated response to cyber incidents and crises				**Effect Indicator:** Percentage decrease in the number of cyber incidents affecting critical infrastructure and key services after the implementation of risk management and coordination measures.			
Specific objective 4.2: Timely and appropriate handling of large-scale incidents and crises				**Outcome Indicator:** Percentage of affected entities (governmental and private) that regularly report incidents of significant scope and crises to the National CSIRT and other relevant authorities, enabling timely and effective management and coordination in responding to such incidents.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Result Indicator (linked to the measure/activity)**
M.4.2.1. MDT as the Coordinating and Managing Body for Large-Scale Incidents and Crises	**A.4.2.1.1. Identification of MDT as the Coordinating and Managing Body for Large-Scale Incidents and Crises through the Cybersecurity Law**	**MDT, National Council for Digital Transformation of Society, Ministry of Defence, MKD-CIRT**	**1/2026**	**4/2027**	**2,460,000 MKD**	**International assistance**	**1.Time for Formal Identification of MDT Starting Value (2026): MDT initiates the process of formal identification through the Cybersecurity Law. Transitional Value (2026-2027): Six months after the initiation of the process, MDT is identified as the body responsible for coordinating**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 4: Minimizing the Impact of Cyber Incidents in Cyberspace				**ALIGNMENT WITH THE NATIONAL DEVELOPMENT STRATEGY: "A Secure, Safe, and Resilient Society"**			
GENERAL OBJECTIVE: Ensure timely and coordinated response to cyber incidents and crises				**Effect Indicator:** Percentage decrease in the number of cyber incidents affecting critical infrastructure and key services after the implementation of risk management and coordination measures.			
Specific objective 4.2: Timely and appropriate handling of large-scale incidents and crises				**Outcome Indicator:** Percentage of affected entities (governmental and private) that regularly report incidents of significant scope and crises to the National CSIRT and other relevant authorities, enabling timely and effective management and coordination in responding to such incidents.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Result Indicator (linked to the measure/activity)**
							and managing incidents and crises. **Final Value (2027): MDT is fully formally identified through the Cybersecurity Law and begins the implementation of its role.** **2.Percentage of Compliance with Legal Requirements** **Starting Value (2026): 50% compliance with legal and regulatory requirements for defining MDT's role.** **Transitional Value (Early 2027): 80% compliance with all legal and regulatory requirements.** **Final Value (End of 2027): 100% compliance with**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 4: Minimizing the Impact of Cyber Incidents in Cyberspace				**ALIGNMENT WITH THE NATIONAL DEVELOPMENT STRATEGY: "A Secure, Safe, and Resilient Society"**			
GENERAL OBJECTIVE: Ensure timely and coordinated response to cyber incidents and crises				**Effect Indicator:** Percentage decrease in the number of cyber incidents affecting critical infrastructure and key services after the implementation of risk management and coordination measures.			
Specific objective 4.2: Timely and appropriate handling of large-scale incidents and crises				**Outcome Indicator:** Percentage of affected entities (governmental and private) that regularly report incidents of significant scope and crises to the National CSIRT and other relevant authorities, enabling timely and effective management and coordination in responding to such incidents.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Result Indicator (linked to the measure/activity)**
							legal and regulatory requirements for defining MDT's role, with full implementation of the law.
M.4.2.2. Plan for Coordinated Response to Major Incidents and Crises, Including Crisis Management Procedures	**A.4.2.2.1. Adoption and Implementation of a Coordinated Response Plan for Major Incidents and Crises, Including Crisis Management Procedures**	**MDT, Ministry of Defence, National Council for Digital Transformation of Society**	**1/2026**	**4/2026**	**1.845.000 MKD**	**International assistance**	**1.Time for Adoption and Implementation – The plan should be adopted and implemented within 12 months. 2.Percentage of Relevant Institutions Following the Plan – 90% of relevant institutions should adopt and follow the coordinated response plan for incidents and crises.**
	A.4.2.2.2. Regular testing of the Coordinated Response Plan for large incidents	**MDT, Ministry of Defence, National Council for Digital Transformation of Society,**	**1/2026**	**4/2027**	**4,920,000 ден**	**Budget of the leading institution for the activity**	**At least one testing of the Coordinated Response Plan for large incidents and crises will be conducted**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 4: Minimizing the Impact of Cyber Incidents in Cyberspace				**ALIGNMENT WITH THE NATIONAL DEVELOPMENT STRATEGY: "A Secure, Safe, and Resilient Society"**			
GENERAL OBJECTIVE: Ensure timely and coordinated response to cyber incidents and crises				**Effect Indicator:** Percentage decrease in the number of cyber incidents affecting critical infrastructure and key services after the implementation of risk management and coordination measures.			
Specific objective 4.2: Timely and appropriate handling of large-scale incidents and crises				**Outcome Indicator:** Percentage of affected entities (governmental and private) that regularly report incidents of significant scope and crises to the National CSIRT and other relevant authorities, enabling timely and effective management and coordination in responding to such incidents.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Result Indicator (linked to the measure/activity)**
	and crises, including procedures for crisis management.	**Civil Sector**					**annually, with all participants in the testing demonstrating 90% or more success in implementing the crisis management procedures.**
	A.4.2.2.3. Adoption and implementation of a Strategic Communication Plan with the public, which will include procedures for crisis management.	**MDT, Ministry of Defence, National Council for Digital Transformation of Society, Civil Sector**	**1/2026**	**4/2026**	**1.845.000 MKD**	**Budget of the leading institution for the activity**	**Adopted and implemented Strategic Communication Plan with the public by the end of 2026.**
	A.4.2.2.4. Regular testing of the Strategic Communication Plan with the public, which will include procedures for crisis management.	**MDT, Ministry of Defence, National Council for Digital Transformation of Society, Civil Sector**	**1/2026**	**4/2027**	**4,920,000 MKD**	**International assistance**	**1.Frequency of testing – The plan should be tested at least twice a year with the participation of all relevant institutions. 2.Percentage of successful tests – 80% of tests should**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 4: Minimizing the Impact of Cyber Incidents in Cyberspace				**ALIGNMENT WITH THE NATIONAL DEVELOPMENT STRATEGY: "A Secure, Safe, and Resilient Society"**			
GENERAL OBJECTIVE: Ensure timely and coordinated response to cyber incidents and crises				**Effect Indicator:** Percentage decrease in the number of cyber incidents affecting critical infrastructure and key services after the implementation of risk management and coordination measures.			
Specific objective 4.2: Timely and appropriate handling of large-scale incidents and crises				**Outcome Indicator:** Percentage of affected entities (governmental and private) that regularly report incidents of significant scope and crises to the National CSIRT and other relevant authorities, enabling timely and effective management and coordination in responding to such incidents.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Result Indicator (linked to the measure/activity)**
							demonstrate full preparedness and functionality of the procedures in the second year.

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028 CYBERSECURITY STRATEGY							
PRIORITY AREA 4: Minimizing the Impact of Cyber Incidents in Cyberspace				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY: "Secure, Safe, and Resilient Society"**			
General Objective: Ensure timely and coordinated response to cyber incidents and crises.				**Effect Indicator:** Percentage reduction in the number of cyber incidents affecting critical infrastructure and key services after implementing risk management and coordination measures.			
Specific Objective 4.3: Timely and appropriate handling of cybercrime				**Outcome Indicator:** Percentage of successfully investigated and processed cases of cybercrime through a joint platform for reporting incidents and cooperation between the Ministry of Interior (MoI), the National CSIRT, the Government CSIRT, and international partners (Interpol, Europol), with a focus on legal actions and sanctions.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
M.4.3.1. Improving Capacities for Dealing with Cybercrime.	**A.4.3.1.1. Analysis of Current Capacities for Dealing with Computer Crime in the Republic of North Macedonia.**	**MoI MDT, MKD-CIRT**	**1/2025**	**4/2026**	**0**	**No financial resources required**	**The analysis of the current capacities for dealing with computer crime has been completed.**
	A.4.3.1.2. Identification of All Relevant Institutions in the Republic of North Macedonia with Competencies and Capacities for Addressing Computer Crime.	**MoI, MDT, MKD-CIRT**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**The identification and mapping of all relevant institutions in the Republic of North Macedonia with the authority and capacity to handle cybercrime will be completed in 2025, with regular annual updates in 2026 and 2027. A report will be prepared and delivered to the responsible institutions.**
	A.4.3.1.3. Development of Procedures and Recommendations for Cooperation Between All Institutions	**MoI, MDT, MKD-CIRT**	**1/2025**	**4/2027**	**922.500 MKD**	**Budget of the leading institution for the activity**	**In 2025, procedures and recommendations for cooperation between all competent institutions**

	Involved in the Fight Against Cybercrime						**involved in the fight against cybercrime will be developed and adopted, aiming to strengthen coordination and communication, and delivered to all relevant institutions. A revision will be made in 2027.**
	A.4.3.1.4. Study on the need for training and development of programs and courses for handling cybercrime and digital forensics for all relevant institutions.	**MoI, MDT, MKD-CIRT**	**1/2025**	**4/2027**	**1,537,500 MKD**	**Budget of the leading institution for the activity**	**A study has been developed, training conducted, and computer equipment and software tools provided.**
	A.4.3.1.5 Establishing a framework for collaboration with the private sector, internet service providers, and the academic community.	**MoI, MDT, MKD-CIRT**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Official cooperation with ISPs and other relevant stakeholders will be formalized. The goal is to establish direct contact and facilitate information sharing between the Ministry of Interior (MVR), ISPs, and other relevant parties.**
M.4.3.2 Harmonization of national policies with international ones related to cybercrime.	**A.4.3.2.1 Analysis of the current methodology, procedures, and cooperation for dealing with cybercrime at the national level.**	**MoI, MDT, MKD-CIRT**	**1/2025**	**4/2026**	**0**	**No financial resources required**	**Completed analysis**
	A.4.3.2.2 Proposal for new or suggested changes to existing methodologies and procedures for handling cy-	**MoI, MDT, MKD-CIRT**	**1/2025**	**4/2026**	**1.230.000 MKD**	**Budget of the leading institution for the activity**	**New updated Standard Operating Procedures (SOPs)**

	bercrime and electronic evidence.						
M.4.3.3 Establishing efficient procedures for reporting and investigating cybercrime.	**A.4.3.3.1. Establishment of a system/platform for reporting cybercrime and information related to criminal activities in the field of cybercrime. Establishment of procedures for involving the private sector and academia in the process of providing information related to cybercrime. Establishment of procedures for sharing collected information from the system with all institutions that have authority in the field of cybercrime.**	**MoI, MDT, MKD-CIRT**	**1/2025**	**4/2027**	**5,535,000 MKD**	**Budget of the leading institution for the activity**	**Development of a case management system for reports received by the Ministry of Interior (e.g., terrorism, violent crime, etc.).**
M.4.3.4. Providing specialized education and training for individuals working in the field of identification and investigation of cybercrime.	**A.4.3.4.1 Identification of existing and relevant specialized education and training programs at the national and international level.**	**MoI, MDT**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Identified existing and relevant programs for specialized education and training at the national and international level.**

	A.4.3.4.2 Development of a plan and procedures for the participation of representatives from all institutions with responsibilities in combating cybercrime in specialized training programs at the national and international level.	**MoI, MDT**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Developed and approved plan and procedures for participation in specialized training programs at the national and international level, with annual updates.**
M.4.3.5. Continuous assessment of the adequacy and effectiveness of national cybercrime regulations.	**A.4.3.5.1. Analysis and assessment of the adequacy and effectiveness of the existing legal regulations for combating cybercrime.**	**MoI MDT, MoJ**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**An analysis and assessment of the suitability and effectiveness of the existing legal framework for cybercrime has been completed, with recommendations for necessary amendments or additions.**
	A.4.3.5.2. Development of proposals for amendments and changes to the national legal regulations regarding the identification and investigation of cybercrime.	**MoI, MDT, MoJ**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Proposals have been made for the supplementation and amendment of the national legal framework regarding the identification and investigation of cybercrime.**

M.4.3.6. Continuous education of judicial authorities in the field of cybersecurity, cybercrime, and electronic evidence.	**A.4.3.6.1. Analysis of the educational and training needs of judicial authorities in the field of computer crime investigation and electronic evidence.**	**Academy for Judges and Public Prosecutors, MoI, MoJ, PP, Courts**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**The analysis of the needs for education and training of judicial authorities in the field of computer crime investigation and electronic evidence has been completed.**
	A.4.3.6.2. Preparation of a Curriculum for Judicial Authorities	**Academy for Judges and Public Prosecutors, MoI, MoJ, PP, Courts**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**The curriculum for judicial authorities, covering training on the investigation of computer crime and electronic evidence, has been approved.**
	A plan for the implementation of education and training for judicial authorities on the investigation of computer crime and electronic evidence has been prepared.	**Academy for Judges and Public Prosecutors, MoI, MoJ, PP, Courts**	**1/2025**	**4/2026**	**0**	**No financial resources required**	**A developed and approved plan for the education and training of judicial authorities on the investigation of computer crime and electronic evidence, which includes clear timelines, resources, and methodologies for conducting the training, has been delivered to all relevant institutions.**

M. 4.3.7. New Strategy for Cybercrime	**A.4.3.7.1 Developed Strategy for Cybercrime**	**MoI, MoJ, PP**	**1/2025**	**4/2026**	**0**	**No financial resources required**	**Developed and adopted Strategy for Cybercrime.**
M. 4.3.8. Implementation of cybersecurity campaigns related to computer crime.	**A.4.3.8.1 Implementation of online campaigns, posters, and visual materials to raise cybersecurity awareness.**	**MoI, PP**	**1/2025**	**4/2027**	**922,500 MKD**	**Budget of the leading institution for the activity**	**Initial Value (2025): 1 campaign, 2 visual materials. Transitional Value (2026): 2 campaigns, 3 visual materials. Final Value (2027): 3 campaigns annually, 5 visual materials.**
M. 4.3.9. International partnerships for monitoring and prosecuting online crimes against children.	**A.4.3.9.1 Building international partnerships for monitoring and prosecuting online crimes against children.**	**MoI, MoJ, PP, Courts**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Establishment of 1 new international partnership for monitoring and prosecuting online child crime. Transitional Value (2026): Formation of 2 new international partnerships and initiation of joint activities. Final Value (2027): Establishment of 3 new international partnerships and successful implementation of 2 international actions or legal collaborations. Final Value (2027): Establishment of 3 new interna-**

							tional partnerships and successful implementation of 2 international actions or legal collaborations.

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028CYBERSECURITY STRATEGY	
PRIORITY AREA 5: national and International Cooperation	**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY: 'A Secure, Safe, and Resilient Society'"**
General Objective: Strengthen national capacities and build trust in cyberspace	**Effect Indicator:** Percentage of increased cooperation and information exchange in the field of cybersecurity at international, regional, and national levels, measured by the number of new partners, established partnerships, and successful international actions implemented into national policy, as well as the number of joint projects and initiatives involving the country's participation.
Specific Objective 5.1: Cooperation in cybersecurity at national, regional and international level	**Outcome Indicator:** Number of established and functional international cybersecurity cooperation partnerships with NATO, the EU, and regional countries. Percentage of successful joint platforms and initiatives for coordinating collaboration in the fight against cyber threats.

Measures	Activities	Leading Subjects and other Subjects	Start date (quarter)	Planned execution date (quarter)	Estimated Required Resources	Source of Funding	Result Indicator (linked to the measure/activity)
M.5.1.1. Cooperation within NATO and the EU, regional countries, other countries, and relevant international organizations.	**A.5.1.1.1. Signing cooperation agreements with bodies responsible for cybersecurity in other countries. Establishing cooperation initiatives in areas related to information systems security, cybercrime,**	**Agency for national Security, Intelligence Agency, Ministry of Foreign Affairs and Foreign trade, MDT**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Bilateral agreements, initiatives, cyber dialogues, exercises, and technical information exchange.**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028CYBERSECURITY STRATEGY	
PRIORITY AREA 5: national and International Cooperation	**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY: 'A Secure, Safe, and Resilient Society'"**
General Objective: Strengthen national capacities and build trust in cyberspace	**Effect Indicator:** Percentage of increased cooperation and information exchange in the field of cybersecurity at international, regional, and national levels, measured by the number of new partners, established partnerships, and successful international actions implemented into national policy, as well as the number of joint projects and initiatives involving the country's participation.
Specific Objective 5.1: Cooperation in cybersecurity at national, regional and international level	**Outcome Indicator:** Number of established and functional international cybersecurity cooperation partnerships with NATO, the EU, and regional countries. Percentage of successful joint platforms and initiatives for coordinating collaboration in the fight against cyber threats.

Measures	Activities	Leading Subjects and other Subjects	Start date (quarter)	Planned execution date (quarter)	Estimated Required Resources	Source of Funding	Result Indicator (linked to the measure/activity)
	cyber defence, cyber terrorism, cyber espionage, and cyber diplomacy.						
	A.5.1.1.2. Improving coordination of all types of international cooperation of institutions in the Republic of North Macedonia in the field of cybersecurity. Systematic coordination through the Ministry of Interior as the central institution where all information should be consolidated.	**MDT, Ministry of Foreign Affairs and Foreign Trade**	**1/2025**	**4/2027**	**0**	**No financial resources required**	**Number of held coordination meetings. Inclusion of a representative from the Ministry of Interior in the coordinating bodies for cybersecurity at the national level.**

ACTION PLAN (2025-2027) FOR IMPLEMENTATION OF 2025-2028CYBERSECURITY STRATEGY							
PRIORITY AREA 5: national and International Cooperation				**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY: 'A Secure, Safe, and Resilient Society'"**			
General Objective: Strengthen national capacities and build trust in cyberspace				**Effect Indicator:** Percentage of increased cooperation and information exchange in the field of cybersecurity at international, regional, and national levels, measured by the number of new partners, established partnerships, and successful international actions implemented into national policy, as well as the number of joint projects and initiatives involving the country's participation.			
Specific Objective 5.1: Cooperation in cybersecurity at national, regional and international level				**Outcome Indicator:** Number of established and functional international cybersecurity cooperation partnerships with NATO, the EU, and regional countries. Percentage of successful joint platforms and initiatives for coordinating collaboration in the fight against cyber threats.			
Measures	**Activities**	**Leading Subjects and other Subjects**	**Start date (quarter)**	**Planned execution date (quarter)**	**Estimated Required Resources**	**Source of Funding**	**Result Indicator (linked to the measure/activity)**
	A.5.1.1.3. Participation in and organization of conferences, exercises, and other events.	**MDT, Ministry of Foreign Affairs and Foreign Trade, MoD, Agency for National Security, Intelligence Agency and other stakeholders**	**1/2025**	**4/2027**	**1,845,000 MKD**	**Budget of the leading institution for the activity**	**Participation in annual conferences of NATO, the EU, and organization of conferences in the Republic of North Macedonia.**

ACTION PLAN (2025-2027) FOR THE IMPLEMENTATION OF 2025-2028 CYBERSECURITY STATEGY	
PRIORITY AREA 5: National and International Cooperation	**ALIGNMENT TO THE NATIONAL DEVELOPMENT STRATEGY: „Secure, safe and resilient society “**
General Objective: Strengthen national capacities and build trust in cyberspace	**Effect Indicator:** Percentage of increased cooperation and information exchange in the field of cybersecurity at international, regional, and national levels, measured by the number of new partners, established partnerships, and successful international actions implemented into national policy, as well as the number of joint projects and initiatives involving the country's participation.
Specific Objective 5.2: Responsible state behaviour and measures to build trust in cyberspace	**Outcome Indicator:** Percentage of successful implementation of national policies for responsible behaviour in cyberspace, measured through the effective alignment of legal and regulatory measures with international standards and norms, as well as increased awareness and engagement of domestic and international stakeholders regarding the protection of personal data and cybersecurity.

Measures	Activities	Leading Subjects and other Subjects	Start date (quarter)	Planned execution date (quarter)	Estimated Required Resources	Source of Funding	Result Indicator (linked to the measure/activity)
M.5.2.1. Promoting norms, rules, and principles of responsible behaviour by the state, in accordance with the established principles at the international level.	**A.5.2.1.1. Promoting norms, rules, and principles of responsible behaviour by the state, in accordance with the established principles at the international level.**	**Ministry of Foreign Affairs and Foreign Trade, MDT, MKD-CIRT**	**- 1/2025**	**4/2027**	**0**	**No financial resources required**	**Conferences/trainings on cyber diplomacy for representatives from state institutions and private companies.**
M.5.2.2. Protection of national interests through participation in the definition of interna-	**A.5.2.2.1. Participation in the activities/working bodies of the EU, NATO, UN, OSCE, and other international organizations and sending**	**Ministry of Foreign Affairs and Foreign Trade**	**1/2025**	**4/2027**	**1.845.000 MKD**	**Budget of the leading institution for the activity**	**Participation of the Republic of North Macedonia in the activities and working bodies of international organizations (EU, NATO, UN, OSCE, and others), with the involvement of**

tional legal acts related to behaviour in cyberspace, freedom of expression, protection of personal data, privacy rights, and fundamental human rights and freedoms.	experts from the field to important meetings.						experts in the field of cybersecurity and computer crime at important international meetings and forums.
	A.5.2.2.2. Building competent cyber diplomats for participation in the working bodies of the mentioned international organizations through regular training.	Ministry of Foreign Affairs and Foreign Trade	1/2025	4/2027	738.000 MKD	Budget of the leading institution for the activity	Development of a plan for additional training of diplomats assigned to these working positions.

	A.5.2.2.3. Strengthening the capacities for cyber diplomacy within the Ministry of Foreign Affairs.	**Ministry of Foreign Affairs and Foreign Trade**	**1/2025**	**4/2027**	**1.845.000 MKD**	**Budget of the leading institution for the activity**	**Initial Value (2025): Number of employees in the Ministry of Foreign Affairs who begin work on cyber diplomacy. Start of regular coordination meetings.** **Transitional Value (2026): Increase in the number of employees and organization of at least two coordination meetings per month.** **Final Value (2027): A team of employees in the Ministry of Foreign Affairs and regular holding of at least three coordination meetings per month.**