

INTRODUCTION CSC-H AND NCZI CSIRT



**CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO**

<NCZI>



TLP: CLEAR

25.9.2026

Peter Spörer

HISTORY OF ORIGIN



THE ORIGIN AND MISSION OF NHIC



Establishment of the NHIC

Effective August 1, 2004, the Ministry of Health of the Slovak Republic establishes a state-funded organization with legal personality.

Name of the organization: Institute of Health Information and Statistics

Primary purpose:

The primary purpose of establishing the organization is to build the material and professional foundation necessary to foster the development of health informatics and health statistics in the Slovak Republic. The Institute will serve as the national center for health information and statistics and act as a partner to similar institutions within the European Union and abroad.

Act No. 153/2013 Coll. on **the National Health Information System** and on Amendments and Supplements to Certain Acts

§ 1 Subject Matter

h) the status and tasks of **the National Health Information Center**

§ 12 The National Center

(2) **The National Center** performs tasks in the areas of healthcare informatization, administration of the national health information system, standardization of health informatics, health statistics, and the provision of library and information services in the fields of medical sciences and healthcare.

ESTABLISHMENT OF THE SECURITY SECTION



Year 2022

Creation of an independent security section within the organizational structure NHIC.

TLP: CLEAR

INSTITUTIONAL ANCHORING



EUROPEAN COMMISSION, Brussels,
15.1.2025 COM (2025) 10 final

4. National Actions

The capacity of this Action Plan to improve cybersecurity in the health sector hinges on the active involvement and commitment of Member States. To successfully implement the Action Plan, Member States could designate **National Cybersecurity Support Centre specifically for hospitals and healthcare providers.**

These centres would act as the primary points of contact for the health sector at national level, collaborating closely with the ENISA Support Centre. Where possible and relevant, Member States should designate existing bodies, such as **national health CSIRTs** or relevant authorities, as **National Cybersecurity Support Centres.**

AMENDMENT TO THE FOUNDING CHARTER National Health Information Centre from May 23, 2025

In Article I, letter z), the operation of an accredited **Cyber Security Incident Response Team (CSIRT)** for the healthcare sector, which performs the tasks and fulfils the obligations of an accredited CSIRT in accordance with the provisions of Act No. 69/2018 Coll. on Cybersecurity and on Amendments and Supplements to Certain Acts, and Decree No. 166/2018 Coll. of the National Security Authority on the details of the technical, technological and personnel equipment of the Cyber Security Incident Response Team, governing the establishment, security and operation of the CSIRT.

AMENDMENT TO THE FOUNDING CHARTER National Health Information Centre from October 15, 2025

In Article I, letter aa), performing the role of **the National Centre for supporting cybersecurity for hospitals and healthcare providers** as the main contact point for the healthcare sector at the national level, including the implementation of measures arising from the European Action Plan for Cybersecurity for Hospitals and Healthcare Providers, and close cooperation with the European Union Agency for Cybersecurity (ENISA), which acts as the main coordinator, provider of methodological support, and developer of a European-wide cybersecurity centre for the healthcare sector.

INTERNATIONAL ACCREDITATION



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>



NCZI CSIRT (SK)

has been accredited by
TF-CSIRT Trusted Introducer since

11 December 2024

Valid for

2024

on behalf of
Trusted Introducer

on behalf of
TF-CSIRT

Dr. Klaus-Peter Kossakowski
TI Service Manager



S. Oertli
Silvio Oertli
TF-CSIRT Chair

TLP: CLEAR

§ 14 Conditions for CSIRT unit accreditation (law n.69/2018 about Cybersecurity)

An applicant for CSIRT unit accreditation pursuant to § 13 shall demonstrate through documentation that the CSIRT unit

a)

possesses the required technical, technological, and personnel resources in accordance with a generally binding legal regulation issued by the Authority,

b)

has established conditions enabling the protected transmission and processing of data in the manner prescribed by a special regulation,

c)

protects information and data obtained and processed in connection with the fulfillment of obligations under this Act in such a way that their availability, confidentiality, authenticity, and integrity are not compromised,

d)

houses its documentation, information systems, and other information and communication technologies in a secure area in such a way that their confidentiality, authenticity, and integrity are not compromised.

NATIONAL ACCREDITATION NCZI CSIRT UNIT



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>



NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

Č: 00590/2026/SAC/OA-014

V Bratislave 22.06.2026

Rozhodnutie o akreditácii jednotky CSIRT

uznáva akreditáciu jednotky CSIRT

názov jednotky CSIRT:	NCZI CSIRT
prevádzkovateľ jednotky CSIRT:	Národné centrum zdravotníckych informácií
so sídlom:	Lazaretská 26, 811 09 Bratislava 1

s platnosťou do 21.06.2031.

TLP: CLEAR

VISION AND STRATEGY

NCZI CSIRT



TLP: CLEAR

To become a specialized sectoral unit for protecting the healthcare sector against cyber threats.



Systematic capacity building for cyber incident detection and response in the sector.

Supporting the continuity of healthcare provision and the resilience of digital services in the healthcare sector.

Strengthening cooperation, exchange, and information sharing among national and international CSIRT units, as well as specialized state entities.

Support for the targeted implementation of uniform safety standards in accordance with national and European frameworks and technical standards.

VISION AND STRATEGY

Cyber Support Centre



TLP: CLEAR

To become the central coordinating and expert support body for cybersecurity in the Slovak healthcare sector.



Systematic capacity building for prevention and deterrence in the health sector.

The center's role as an expert, professional, and coordinating pillar for enhancing the level of cybersecurity and protecting sensitive medical and patient data.

Strengthening cooperation, exchange, and information sharing among hospitals, healthcare providers, state authorities, the private sector, and international entities.

Support for targeted professional training and raising safety awareness in the healthcare sector.

ROAD MAP



TLP: CLEAR

WHERE WE ARE AND WHAT IS AHEAD



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>

2026



NHIC begins fulfilling the tasks of
THE CYBER SUPPORT CENTRE FOR HEALTHCARE

TLP: CLEAR

WHERE WE ARE AND WHAT IS AHEAD



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>

2026



NHIC begins fulfilling the tasks of
NCZI CSIRT UNIT for Healthcare.

TLP: CLEAR

WHAT AWAITS US IN NCZI CSIRT UNIT



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>

2027



Connecting



Connection of entities into SOC



Oversee



NCZI CSIRT operates in the sector

Evaluating



Preparation of an evaluation report on the status, scope, and content for future activities and the provision of support.

TLP: CLEAR

WHAT AWAITS US IN CYBER SUPPORT CENTRE

2027



Evaluating



Report on the fulfillment of the Support Center's tasks for the year 2026



Progress



Adjustment of the scope of work to streamline operations based on analysis

Providing
Information



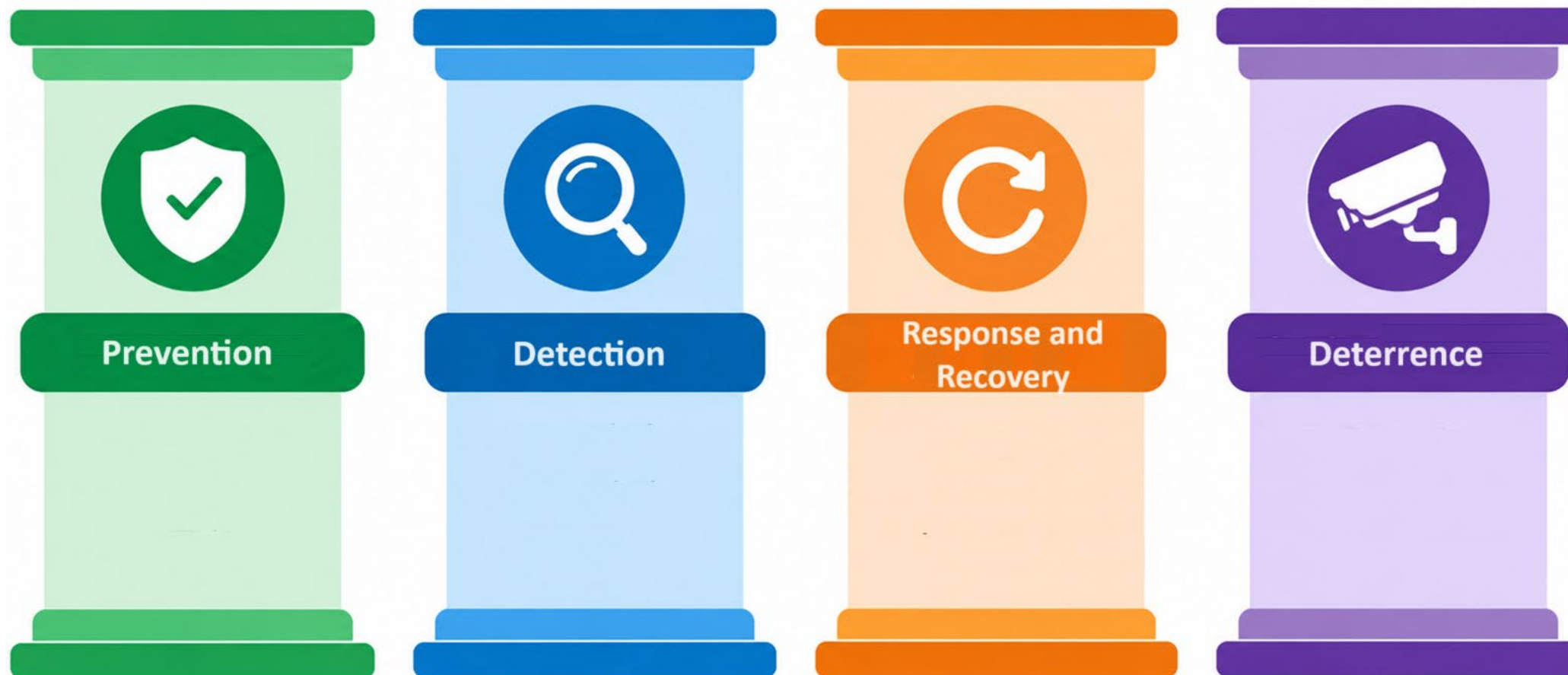
Dissemination of acquired and evaluated information to entities in the sector

PRIORITIES

Priorities of the European Commission's action plan



PRIORITIES BASED ON FOUR PILLARS



PREVENTION

Stopping an attack before it even begins. How to set up the system right from the start.

DETECTION

Minimize impacts and damage, detect threats early and respond quickly.

RESPONSE AND RECOVERY

Reduce the impact of an attack and recover quickly, ensure faster recovery following an incident.

DETERRENCE

Making the healthcare system less attractive to cybercriminal, making them think twice before attacking.



**CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO**

<nczi>

PRIORITIES FOR THE CYBER SUPPORT CENTER



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>



Prevention



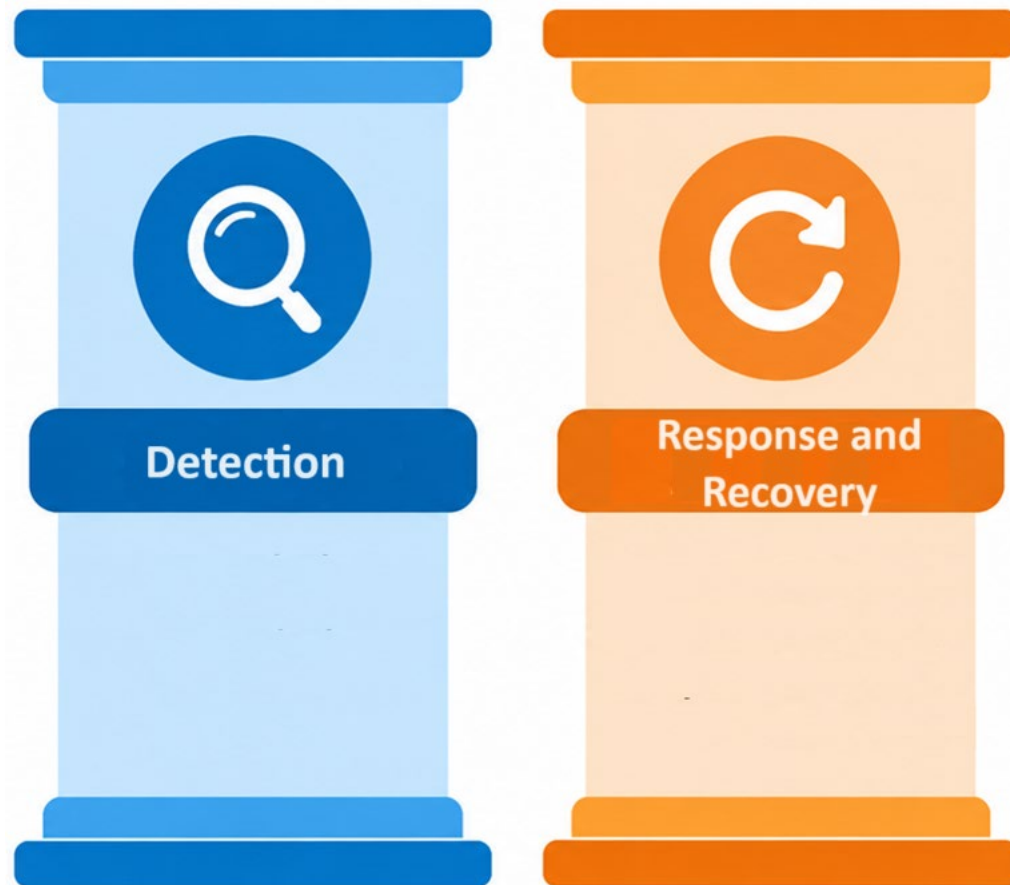
Deterrence

TLP: CLEAR

PRIORITIES FOR THE UNIT NCZI CSIRT



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>



TLP: CLEAR

Personalized horizontal communication line.

TWO WAY-DIRECTION

"Discover, share, respond and evaluate."

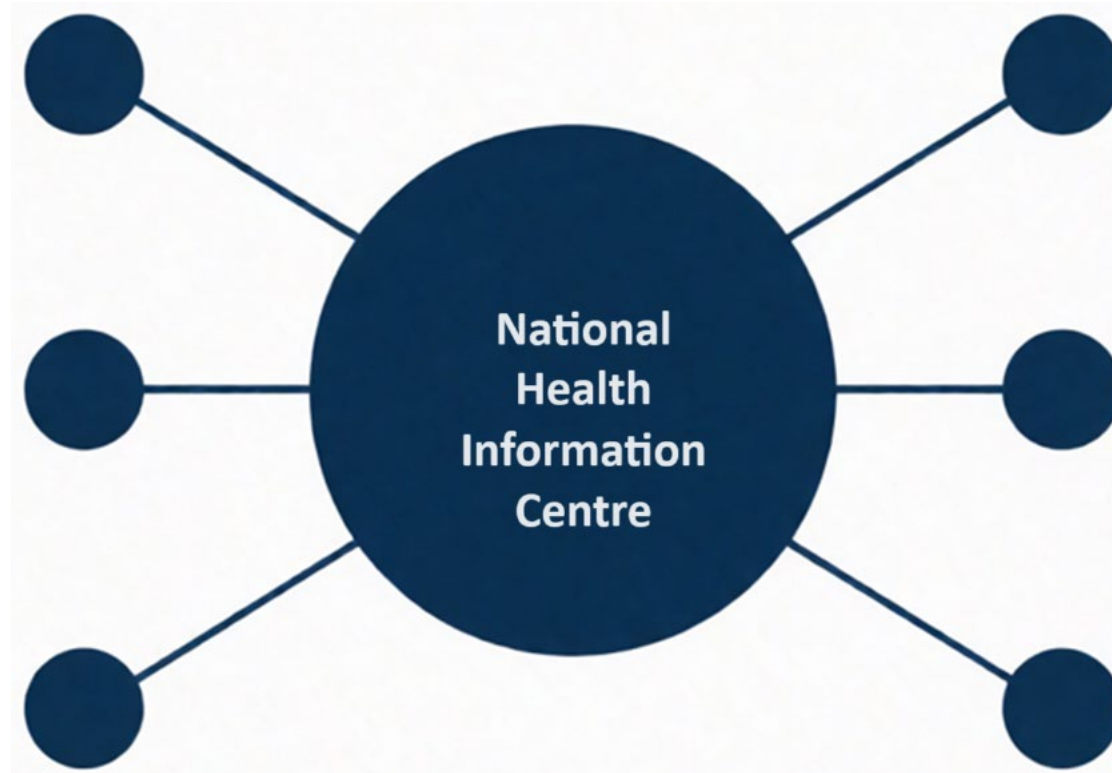


HEALTHCARE SECTOR COOPERATION

**Universities and
Secondary medical
schools**

**State and Public
administration**

Suppliers



Hospitals

Healthcare providers

Laboratories

and other entities as needed

PRINCIPLES AND FOCUS OF ACTIVITIES



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>



TLP: CLEAR

NATIONAL ACTION PLAN



TLP: CLEAR

NATIONAL ACTION PLAN FOR THE YEARS 2026 AND 2027

National Action Plan developed in accordance with the European Action Plan

Content: comprises 17 tasks

Main focus:

1. Long-term activities to raise security awareness and preparedness
2. Regular measurement and assessment of cybersecurity maturity
3. Active identification of threats and vulnerabilities affecting the sector and its stakeholders
4. Periodic risk analysis for the sector regarding ICT and OT
5. Establishing communication between the sector and its stakeholders, authorities, and organizations
6. Exchange of information and knowledge on a regular or as-needed basis



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>

NATIONAL ACTION PLAN FOR THE YEARS 2026 AND 2027

National Action Plan developed in accordance with the European Action Plan

Evaluation: Every January of the following calendar year.

Format: Activity report of the Cyber Support Centre for Healthcare

Content: Implementation of the National Action Plan



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>

DOMESTIC COOPERATION AS PART OF ACTION PLAN

Domestic cooperation is integral part of our activity due to the effectiveness of action which is not separate, but national wide impact.

TLP: CLEAR



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>

DOMESTIC COOPERATION



National Security Authority: [SK-CERT](#)



Ministry of Investment, Regional Development and Informatization
of the Slovak Republic: [CSIRT.SK](#)



Centre for Cyber Defence of the Slovak Republic: [CSIRT.MIL.SK](#)

TLP: CLEAR

DOMESTIC COOPERATION

1. University and Medical Secondary Schools
 - education, awareness and research
2. Hospitals and healthcare facilities
 - information exchange, expert cooperation and technical support
3. Healthcare providers
 - information and technical support, education and awareness

INTERNATIONAL COOPERATION



TLP: CLEAR

INTERNATIONAL COOPERATION



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>



TLP: CLEAR

INTERNATIONAL COOPERATION



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>



EUROPEAN
HEALTH ISAC

TLP: CLEAR

INTERNATIONAL COOPERATION

Our actual ongoing activity is to open the communication and cooperation with our close neighbors.

Austria

and

Hungaria

„ Knowing is not enough; we must apply.
Wanting is not enough either; we must act“

Thank you for your attention.



**CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO**

<nczi>