NATIONAL CYBERSECURITY SYSTEM

The aim of the system is to ensure an appropriate level of security of ICT systems.
The system encompasses a wide range of entities, including:

OPERATORS OF ESSENTIAL SERVICES

Providing services in the following sectors:

- Energy
- Transport
- Banking and financial market infrastructure
- Healthcare
- Drinking water supply and distribution
- Digital infrastructure

DIGITAL SERVICE PROVIDERS

These include:

- Online marketplace
- Cloud computing providers
- Online search engines

COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

1) CSIRT GOV – organised within the Internal Security Agency
2) CSIRT NASK – organised within the Research and Academic Computer Network (NASK)
3) CSIRT MON – organised within the Ministry of National Security

The act also makes it possible to establish sector-based cybersecurity teams.

GOVERNMENT PLENIPOTENTIARY FOR CYBERSECURITY

- Coordinates governmental actions and policies for cybersecurity in Poland
- Appointed by the Prime Minister
- According to the current Regulation of the Council of Ministers of 16 March 2018, the Representative is the Secretary of the State or the Deputy Secretary of the State at the Ministry of National Security

CYBERSECURITY COUNCIL

- Operates alongside the Council of Ministers as an advisory body for matters related to cybersecurity
- Members of the Council include: the Prime Minister, selected ministers and Chief of National Security Bureau
- Meetings are also attended by, among others: the Director of the Government Centre for Security, Chief of the Internal Security Agency, Chief of the Military Counterintelligence Service and Director of NASK

SINGLE POINT OF CONTACT FOR CYBERSECURITY MATTERS

- Supervised by the Ministry of Digital Affairs
- Ensures exchange of information on incidents with other EU Member States
- Responsible for cooperation on the EU level both with the European Commission and as part of Cooperation Groups

ENTITIES PROVIDING CYBERSECURITY SERVICES

Specialised companies protecting the infrastructure of essential service providers and handling incidents in their networks on a contractual basis.

THE ACT DIVIDES SECURITY INCIDENT HANDLING IN POLAND'S CYBERSPACE BETWEEN THREE COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs):

CSIRT GOV | CSIRT NASK | CSIRT MON

POLAND'S CYBERSPACE

CSIRT NASK

- Citizens
- Companies
- Self-governmental administration
- State universities
- Other entities in the public and private sector

CSIRT MON

Entities supervised by the Ministry of Defence and companies with special economic and military significance.

CSIRT GOV

- Governmental and subordinate unit infrastructure
- Critical Infrastructure
- Infrastructure of the NBP and BGK banks, Social Insurance Institution, NHS, Supreme Audit Office, Commissioner for Human Rights, National Broadcasting Council and courts and tribunals

CLASSIFICATION OF INCIDENTS WITHIN THE NATIONAL CYBERSECURITY SYSTEM

CRITICAL INCIDENT

- An incident resulting in significant damage to public security or public order, international interests, economic interests, operation of public institutions, citizen rights and freedoms or people's lives and health
- Classified by a relevant CSIRT

SERIOUS INCIDENT

- An incident that causes or may cause a serious reductionin the quality of an essential service or a discontinuation thereof
- Classified by the operator of the essential service

SIGNIFICANT INCIDENT

- An incident that significantly affects the provision of a digital service, as defined by Article 4 of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018
- Classified by the digital service provider

THE KOSCIUSZKO INSTITUTE