HUNGARIAN CENTRAL STATISTICAL OFFICE

INFORMATION SECURITY POLICY OF THE HUNGARIAN CENTRAL STATISTICAL OFFICE

The Hungarian Central Statistical Office (hereinafter referred to as HCSO) has one of the largest statistical data assets in Hungary, and due to its activities, the protection of data and IT infrastructure is of high priority. HCSO's data processing operations are carried out in an appropriately protected operational and electronic information infrastructure in accordance with the information security principles and with the security classification.

HCSO's information security principles are established in its information security policy detailed below in compliance with the Regulation of the European Parliament and of the Council on European statistics, the GDPR, the principles of the European Statistics Code of Practice, Act CXII of 2011 (Privacy Act), Act CLV of 2016 on Official Statistics and Act L of 2013 on Electronic Security of State and Local Government Bodies.

HCSO shall apply the following principles in the field of information security:

1. **Confidentiality**: the data and information stored in the electronic information system can be known and used, and their use can be disposed of only by those authorised to do so and only according to the level of their authorisation.
2. **Integrity**: the content and characteristics of the stored data shall be as expected, including the certainty that these are from the expected source (credibility) and that their origin can be verified and stated (undeniability), as well as the characteristic of the elements of the electronic information system that each element of the electronic information system can be used as intended.
3. **Availability**: electronic information systems shall be available to the authorised person and the data managed therein can be used.
4. **Completeness of protection:** in the field of physical, logical and administrative protection the principle of completeness shall be applied in the following three dimensions:
    a) for all system components;
    b) for all layers of the architecture of the systems, at the levels of both the IT infrastructure and applications;
    c) for central as well as end-point IT tools and their environment.
5. **Closed nature of protection:** preventive protection measures against all probable threats shall be implemented, and taken as a whole they shall form a regulated and integral whole.
6. **Risk proportionality of protection:** the extent and costs of protection shall be proportionate to assessed risks. The aim is the maximum protection capability reached with the necessary and sufficient security costs.
7. **Continuity of protection:** the established security measures, along with the security environment and conditions constantly changing over time, shall persist without interruption during the entire life cycle of the system.

HCSO, by designing, implementing, managing and maintaining an information security management system, ensures the confidentiality, integrity and availability of data, and, by implementing logical, physical, and administrative measures, ensures that the electronic information systems are secure by default and implements a risk proportionate and overall security strategy against threats to their integrity and availability on a continuous basis.

The management of HCSO is greatly concerned with the protection of its electronic information systems and the data stored therein, and is committed to continuously providing resources required for implementing appropriate state of the art technical protection measures. HCSO improves its security level by establishing monitoring procedures, introducing regular controls and by integrating them into the information security processes.

The management of HCSO is committed to ensuring that the requirements for data processing are defined in accordance with the information security principles and that data processing activities are in compliance with the requirements for state of the art protection methods. HCSO takes into account the requirements for data quality and data confidentiality, regular data transfers and data protection, adopts protective measures to comply with these requirements and allocates the required resources.

All executives, employees and third parties of HCSO are responsible for complying with the data protection principles and requirements, receive regular training about the principles and requirements and ensure the protection of data in accordance with these principles and requirements.

Budapest, 1 March 2019

Dr. Gabriella Vukovich
President of HCSO