ORGANISATIONAL INSTRUCTIONS ON INFORMATION SECURITY POLICY OF THE PUBLIC AGENCY FOR MEDICINAL PRODUCTS AND MEDICAL DEVICES OF THE REPUBLIC OF SLOVENIA

UNOFFICIAL TRANSLATION

ORGANISATIONAL INSTRUCTIONS ON INFORMATION SECURITY POLICY OF THE PUBLIC AGENCY FOR MEDICINAL PRODUCTS AND MEDICAL DEVICES OF THE REPUBLIC OF SLOVENIA

Pursuant to paragraph one of Article 80 of the Decree on Administrative Operations (Official Gazette of the Republic of Slovenia [*Uradni list RS*], Nos 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07, 31/08, 35/09, 58/10 and 101/10) and paragraph one of Article 19 of the Decision on the Establishment of the Public Agency for Medicinal Products and Medical Devices of the Republic of Slovenia (Official Gazette of the Republic of Slovenia [*Uradni list RS*], No. 115/06), on 13 January 2014, I, the Director of the Public Agency for Medicinal Products and Medical Devices of the Republic of Slovenia hereby adopt the following organisational regulation:

ORGANISATIONAL INSTRUCTIONS ON INFORMATION SECURITY POLICY OF THE PUBLIC AGENCY FOR MEDICINAL PRODUCTS AND MEDICAL DEVICES OF THE REPUBLIC OF SLOVENIA

I. GENERAL PROVISIONS

Article 1

These organisational instructions shall lay down the information security policy (hereinafter: ISP) of the Public Agency for Medicinal Products and Medical Devices of the Republic of Slovenia (hereinafter: the Agency), which expresses the policy by which the Agency wishes to protect the information assets it manages. Furthermore, the procedures for and establishment of an information security management system at the Agency are defined.

Article 2

These organisational instructions are a document that must be complied with by management, employees, outsourcers and anyone with access to the Agency's information assets.

Article 3

The purpose of the ISP is to determine the basic starting points for the protection of information resources against threats, internal or external, intentional or accidental. The implementation of this policy is important for ensuring information security.

Information security is defined as the protection of:

- **confidentiality**: the protection of data and information from disclosure to unauthorised persons and ensuring responsibility for their acts;
- **integrity**: the protection of data and information from unauthorised changes, and ensuring the credibility – accuracy, completeness and inalterability of information and processing procedures;
- **availability**: the protection of data, information and service from interruptions in operations and the provision of information to authorised users when they need it and in the required manner.

Article 4

The ISP shall ensure the achievement of the following main objectives:

- the protection of data and information against unauthorised access, processing and disclosure;
- maintenance of the integrity of information and the prevention of unauthorised changes;
- ensuring the availability of information and resources when needed by authorised persons;
- ensuring the preparation, maintenance and verification of business continuity plans to the extent practicable;
- ensuring information security training;
- recording and investigating infringements of the ISP and of any suspicion of such infringement;
- verification of compliance with legislation;
- ensuring compliance with recommendations regarding information security standards.

Article 5

ISP terms shall have the following meaning:

1. **digital certificate** – a certificate containing information on the identity of the holder, issuer and public key holders, which is used to verify an electronic signature;
2. **visitor log** – records in electronic or written form with information about visitors and the purpose and time of visits;
3. **event** – a condition or change that may affect information security;
4. **documentation** – all written or electronic information on equipment or procedures;
5. **electronic mail** – a service for the exchange of electronic messages;
6. **electronic mailbox** – a database in which the user's or a dedicated user group's electronic messages received or sent via the electronic mail system are stored;
7. **electronic message** – a set of data sent or received by electronic means;
8. **incident** – an event resulting in the disclosure, destruction, or unavailability of data or an information system or a breach of security policy;
9. **information system** – a complete set of equipment (communication and information) and procedures for handling Agency data;
10. **information security event** – any event that may affect the data security of the information system or the operation of the information system;
11. **infrastructure** – power and communication lines, generators, air conditioners, uninterruptible power supply systems (UPS systems), fire extinguishing systems, premises, etc.;
12. **removable media** – data carriers that can be easily removed and separated from the information system. These include CDs, DVDs, USB flash drives and disks;
13. **cryptography** – the study and use of the encryption and decryption of data or messages;
14. **cryptographic controls** – the verification, determination and management of cryptographic keys;
15. **cryptographic keys** – a set of characters that are the input data for the execution of an encryption algorithm;
16. **critical infrastructure** – equipment that is absolutely necessary for the operation of the Agency's minimum functions;

17. **local area network (LAN)** – a computer network with active and passive elements that enables connectivity and data flow between terminal equipment and resources within an individual location of the Agency;
18. **unauthorised access** – unauthorised access to premises, data and information, access without appropriate authorisation;
19. **unprotected area** – copper or optical lines passing through public spaces between buildings where the Agency has no control over this route;
20. **data carrier** – a device or means that enables data reading and/or writing (a diskette, CD, DVD, disk, USB flash drive, card, tape, cassette, paper, etc.);
21. **sensitive data** – personal data (including sensitive personal data) under the Personal Data Protection Act, classified information under the Classified Information Act and those designated as such by the Agency;
22. **data handling** – the collection, processing, display, storage, modification and deletion of data;
23. **risk assessment** – the identification of all possible risks and threats that may endanger the security and operations of the Agency;
24. **certification authority** – the issuer of qualified digital certificates, part of the public key and infrastructure that issues digital certificates;
25. **penetration test** – an intrusion test requested by the information system owner in which weaknesses in ensuring information security are identified;
26. **authorised person** – an individual or a group of people appointed on the basis of an Act or by the director to perform certain tasks;
27. **wide area network** – a wide area network, possibly a global network, or WAN, is a network of computers that extends over large geographical distances. Some connections on wide area networks take place over telephone lines or via satellites. Wide area networks often connect multiple local area networks into a single one;
28. **antivirus software** – special software designed to detect and remove viruses and other malware;
29. **administrator** – an authorised person responsible for the management of an individual system or subsystem (plans, processes, equipment, infrastructure, information security, information system, etc.);
30. **means of access to the information system** – username and password, smart cards, certificates, one-time passwords and other methods for the authentication and authorisation of information system users;
31. **World Wide Web** – the internet;
32. **encryption** – the transformation of comprehensible text into incomprehensible form by cryptographic methods;
33. **user** – a person who uses an information system or device in regular work and has an employment agreement or is employed by the Agency or is an outsourcer of the Agency;
34. **username and password** – a set of characters with which the user logs into the information system;
35. **management** – the performance of functions such as the design, installation, provision, operation, administration and maintenance of the system;
36. **backups** – copies of specific data to protect against loss, which are usually copied to an optical or magnetic medium;
37. **protected information** – personal or other non-classified information whose disclosure to unauthorised persons could cause damage to the Agency, the course of

official proceedings or the persons to whom it relates, and whose handling and processing must be subject to security measures and procedures;

38. **outsourcer** – any natural or legal person supplying equipment or providing services to the Agency under contract.

Article 6

The information system shall ensure the detection of ISP infringements and their sanctioning according to the applicable legislation or contract.

In the event of an infringement of the ISP, action may be taken against the infringer as provided by the legislation in force.

Depending on the Agency's interest, other measures may be taken. The Agency shall have the right to immediately suspend and possibly subsequently terminate service if it finds an infringement of the ISP.

Article 7

The Agency's owned and operated systems connected to the internet, intranet or extranet shall include, but not be limited to, computer hardware, software, operating systems, email user accounts, web browsing and file transfers. These systems shall only be used for the business purposes of the Agency and, in normal operation, shall exclusively serve the interests of the Agency, its clients and business partners.

Article 8

Although one of the purposes of managing the Agency’s network is to ensure a reasonable level of privacy, users should be aware that all data generated by the systems owned by the Agency are the property of the Agency. In order to protect the information environment of the Agency, the management shall not be able to guarantee the confidentiality of private information stored in any system belonging to the Agency.

Employees shall be responsible for the reasonable and acceptable use of information resources for private purposes.

II. PHYSICAL SECURITY POLICY

Physical access

Article 9

Appropriate security shall be provided for the Agency's premises.

Visitors shall report to the reception desk and tell the security guard who they have come to visit and why.

Article 10

The premises where data are processed and handled shall be protected by organisational, physical and technical measures that prevent unauthorised persons from accessing information and communication technology for data processing.

Safeguarding the means of access

Article 11

Each employee of the Agency shall safely and carefully keep, have under their control, and not lend any physical means (keys, ID cards, badges, cards, etc.) or electronic means (usernames, passwords, encryption keys, etc.) of access to premises, data and equipment.

Electronic means of access shall be considered sensitive data.

Protection of equipment

Article 12

All equipment shall be installed and protected in such a manner that environmental risks and opportunities for unauthorised access are eliminated as much as possible.

The level of protection and security shall be determined according to the sensitivity of the data and the assessed risk of data loss or damage.

Article 13

Fire protection in areas where key or ancillary equipment is installed shall be ensured in accordance with the regulations and instructions of the relevant authorised services.

Article 14

Wiring shall always be planned and installed by suitably qualified contractors and shall be carried out in accordance with applicable standards and regulations.

Wiring safety shall be planned when planning computer rooms and installing equipment. Each time the network or the devices included therein are upgraded or modified, the safety of the wiring shall be checked.

Electrical and telecommunication cables (wiring) through which data are transmitted or which support information services shall be protected against interception or damage.

Article 15

Users shall report any failure and intentional or unintentional damage to the equipment to the IT unit, which shall act in accordance with the prescribed procedures.

Article 16

The Agency shall keep records of all portable computer and storage devices allocated for use by employees and connected directly or indirectly to the Agency's information system.

The register of devices shall contain information on the type, manufacturer, model, serial number, user and date of commencement of the use of the device within the Agency's information system.

III. POLICY ON THE APPROPRIATE USE OF THE INFORMATION SYSTEMS AND SENSITIVE DATA PROTECTION

Use of information technology equipment

Article 17

Information technology equipment owned by the Agency shall be intended for the performance of work or work needs as part of the Agency's work process.

Use for private purposes shall not be permitted except for urgent matters and to a lesser extent that does not interfere with the work process and security (confidentiality, integrity and availability) of the information system, or if approved in writing by the director.

Article 18

Users shall handle the Agency's information technology equipment with due diligence in accordance with the recommendations and instructions of the manufacturer and system administrator. Interventions may only be carried out by authorised persons.

Users shall be responsible for the theft and damage of equipment. Users shall handle portable equipment with special care.

Users may not store private multimedia files (photographs, music, videos, etc.) and pirated copies of works protected by the Act governing copyright and related rights on the Agency's information technology equipment.

Article 19

Users may not install software themselves, except with the permission of information system administrators. Software installation and maintenance shall be the responsibility of information system administrators.

Information system administrators shall ensure that information systems are adequately protected against unauthorised or malicious software. At a minimum, antivirus software shall be installed. Regular updating of this software shall be ensured.

Article 20

All Agency employees shall be entitled to access a stationary workstation at the business premises of the Agency at all times.

A stationary workstation shall consist of:

- a personal computer with standard input peripherals,
- one or two monitors and
- a landline.

A workstation shall usually have one monitor connected; however, if necessary due to managing a large amount of electronic documentation, employees shall be entitled to have access to a workstation with two connected monitors.

A personal computer may be a desktop personal computer, a laptop, or an ultralight laptop. All employees, with the exceptions specified in Article 21 of these organisational instructions, shall have access to a workstation with a desktop personal computer.

Article 21

The right to use a laptop at the Agency at all times shall be granted to:

- heads of divisions,
- inspectors,
- the head of the IT unit and
- other persons ordered by the director or a person authorised by the director, if at least one of the following criteria is met: frequent business trips or work at home or substituting for a person entitled to use a laptop at all times.

The right to use an ultralight laptop at all times shall be granted to:

- the director,
- the deputy director and
- the members of the extended council of the director.

The right to use a tablet at all times shall be granted to:

- the director,
- the deputy director,
- the members of the extended council of the director,
- the business secretary of the Agency and
- the head of the IT unit.

Article 22

A desktop personal computer, a laptop and an ultralight laptop shall be equivalent workstations. Each employee shall have the right to use at least one workstation at all times.

Article 23

Employees who go on a business trip shall have the right to use a laptop while on the business trip. Employees granted the right to use a laptop during a business trip may pick up the laptop one working day before the business trip and shall be required to return it the next working day after returning from the business trip.

Article 24

All employees shall have access to all network printers in a manner that enables a reasonably short access distance from their workplace to the printer.

The following persons shall have the right to use a workstation with a printer connected at all times:

- the director,
- the deputy director and
- heads of divisions.

Inspectors shall have the right to use a portable printer.

Article 25

Each employee shall have access to at least one scanner.

Employees in the main office shall have the right to use a workstation with a scanner connected at all times.

Malware

Article 26

The installation, use or dissemination of malware shall constitute an infringement of the ISP.

The intentional installation, use and dissemination of such software shall be treated in accordance with the applicable law.

Users:

- shall immediately stop using the information system if they suspect that malware is running thereon, inform the competent person thereof, and follow their instructions;
- shall immediately inform the competent person if they suspect that malware is installed on the information system, and follow their instructions;
- shall not run executable code that is not part of their information system (e.g. from the World Wide Web, email, storage media);
- shall not run documents (e.g. from the World Wide Web, email, storage media) if they are suspicious, if they do not know what such documents or applications are intended for, or if they do not know the origin thereof;
- shall immediately stop using the information system if they suspect or find that the antivirus software is not working or has not been properly updated, notify the administrator thereof, and follow their instructions.

Information systems

Article 27

Information systems handling sensitive data shall be under surveillance.

Systems handling other data may also be under surveillance. Appropriate logs shall be included in the systems under surveillance to ensure event monitoring. The logs shall enable the identification of the user who either accessed or modified the data. The printing or export of log data shall also be monitored and unchanged. Log data may only be obtained at the written request of the director or at the request of the competent investigative body regarding suspicion of the commission of a criminal offence.

Log data shall also be used to identify errors in the information system or to improve its performance. Where logs contain sensitive data, access to and other modifications of the system shall be recorded.

Article 28

The use of private equipment in the information system of the Agency shall not be allowed.

Removable media management

Article 29

Adequate security and protection shall be provided for the management of removable media. The loss or theft of removable media shall be reported to the administrator.

Article 30

Removable media of unknown or suspicious origin may not be used. Before using the contents of a removable media device, its potential infection with malware shall always be checked.

Article 31

Users shall hand over all removable media that they no longer need or that are unusable to the administrator.

Access to information systems

Article 32

A procedure for granting, modifying and withdrawing access rights shall be established for each information system of the Agency.

Article 33

Access to individual information systems and the parts thereof may only be granted to persons who are entitled, authorised and duly qualified to access such.

Article 34

Based on business process needs, access to the information system shall be granted to the extent necessary for the performance of tasks.

Article 35

Access to the Agency's information systems shall only be possible based on appropriate authentication, at a minimum by using a username and password. Other approved authentication methods may be used to log in to the system.

System passwords shall be changed at least once every three months. User account passwords shall be changed at least once every six months.

Article 36

The means of accessing the information system shall be non-transferable. Lending shall not be allowed.

Users shall carefully safeguard the means of accessing the information system from being misappropriated or misused. Any suspicion of misuse or misappropriation shall be immediately reported to the system administrator.

Article 37

Access to services and the management of information systems and networks shall be regulated by a system of rights. These shall be assigned by the information system or network administrator.

Article 38

The right to access the information system or network may be acquired by users or administrators based on need and the approval of the application or service owner. If the need for access ceases, this right shall be revoked.

The process of managing access rights to the information system shall be documented and the assigned rights reviewed regularly.

Article 39

User and administrator rights to access the information system shall be separate.

Clear desk principle

Article 40

Users shall not leave data carriers (e.g. in paper form, electronic media) containing sensitive data on open areas of office equipment or in any other places where unauthorised persons could have access thereto. When users are not in the room, data carriers shall be stored securely. Outside working hours, all office equipment where data carriers containing non-public data are stored shall be locked or otherwise protected, and physical or software protection shall be provided for communication and information equipment.

Clear screen principle

Article 41

During the user's presence at or absence from the workplace, access to the screen or the use of information and communication equipment by unauthorised persons shall be prevented:

- workplaces shall be arranged in such a manner so as to avoid casual "looking over the shoulder";
- equipment and settings shall be used which, after a certain period of user inactivity on the workstation, switch off the screen or switch it to a password-protected screen saver;
- at the end of the work process, the user shall log out of the system and switch off the workstation, unless otherwise specified by other instructions.

Remote access

Article 42

Remote access to the information system shall be allowed only based on an approved method with an appropriate level of security for those users who need access to perform tasks, but only to a limited extent. The clear screen principle shall be observed.

After finishing work, it shall be mandatory to log out of the system and ensure that sensitive data and traces do not remain on the workstation.

Article 43

When there is a need for third-party access to the Agency's information or information system, a risk analysis shall first be carried out and the required security measures identified. Access to information or the information system by third parties shall not be permitted until the

appropriate security and control mechanisms have been implemented and an agreement defining the conditions of access has entered into force.

Third parties shall be given access only to the information and systems they urgently need in their work or to perform their contractual obligations so as to reduce the possibility of unauthorised access.

If an infringement of security regulations and instructions is suspected, access to the network shall be temporarily disabled until the actual state of the infringement is established.

Access to the World Wide Web and its services

Article 44

Access to the World Wide Web shall be provided to employees for their work, education and information.

Agency employees shall use the World Wide Web in accordance with ethical and moral norms. Agency employees shall not be allowed to disseminate or access offensive and inappropriate or illegal content.

It shall be acceptable to use the World Wide Web for private purposes only to the extent that it does not interfere with the work process and in a manner that does not compromise the security of the information system.

All users of the Agency's information systems shall be aware that they identify themselves on the internet with the Agency's network address as legal entities under public law.

Article 45

Based on the risk assessment, it shall be possible to restrict access to content in order to ensure information security and the availability of information resources, to prevent infringements of ethical and moral norms, and to ensure the smooth running of the work process.

By issuing a decision, the director may specify web addresses or content to which access shall be technically restricted.

Article 46

Sending business email addresses to external web servers shall not be allowed unless it is related to the business process of the Agency.

Article 47

For the purpose of investigating the suspicion of illegal acts, the Agency's network may record users’ access to online services and related data on assigned internal IP numbers, the time of the assignment of an internal IP number, and data on the connection between an internal and public IP number. These data may be provided by system administrators only upon a reasoned request by a body which, based on its statutory powers, deals with allegedly illegal acts.

Any data processing in violation of paragraph one of this Article shall not be allowed. The retention period of such synthesised data shall be three months, after which the data shall be destroyed or anonymised. Anonymised data may be used for system management.

Use of email

Article 48

Agency employees shall use the Agency's email and mail server as a tool to communicate with clients, employees, outsourcers and other stakeholders. In doing so, they shall adhere not only to ethical and moral norms but also to the requisite standards of etiquette. Email content shall not contain inappropriate or offensive content that would damage the reputation of the Agency.

Senders thereof shall be aware that any message sent from their work email address may be interpreted by the recipient as an opinion of the Agency.

Article 49

As a rule, the Agency's email system shall be used only for work purposes. Use for other purposes shall be permitted only exceptionally, provided that it does not interfere with the work process and security (confidentiality, integrity and availability) of the information system.

Private emails shall be unambiguously marked as such and stored separately from work emails.

Article 50

Messages on social networks whose sender's email address contains the Agency's domain shall be accompanied by a note that the content of the message represents the sender's personal opinion which may differ from that of the Agency. A note may only be omitted if the message has been sent *ex officio*.

Article 51

Users may not send chain letters and large files (music, videos, presentations, executable files and literature) by email unless they are intended for work.

Employees shall forward any suspicious email exclusively to information system administrators.

Article 52

Users may not use their work email address for marketing purposes and may not send advertising emails therefrom to known and/or unknown email addresses or create pyramid schemes.

Article 53

If users need to send emails to a large number of recipients, they shall consult with the mail system administrator before sending such and anonymise the recipients of such messages in accordance with the Act governing personal data protection.

When forwarding or replying to emails ("Forward", "Reply" and "Reply All"), users shall be especially careful to check that the email is addressed to the correct email addresses. Prior correspondence should be deleted in such cases, except in justified cases where this is strictly necessary due to the nature of the work process.

Employees shall not be allowed to sign up for advertising email or newsletters using the Agency's email addresses unless it is related to the needs of the work position.

Article 54

Users shall be careful when opening emails with attachments received from unknown senders. If they suspect that it is spam that could be harmful, they shall not open it, but shall inform the mail system administrator thereof.

Article 55

Under no circumstances shall users send sensitive data or passwords by email except in appropriately accredited systems.

Emails and attachments containing confidential information shall be encrypted when sent to an external network (outsourcers).

Article 56

Work emails shall be handled in accordance with the applicable rules on dealing with documents.

Private email addresses shall not be used to register for events or for sending messages related to the performance of work tasks. It is prohibited to forward work emails to private email addresses.

Email data rights

Article 57

All rights to the email system and all non-private emails shall belong to the Agency. Users should be aware that emails are backed up in the email system and shall remain stored even if users delete them from their email inbox.

Users should be aware that emails may be intercepted and processed by unauthorised persons, depending on the technology.

Article 58

Users shall not use an email address assigned to another user.

Article 59

If an email address is cancelled, a message regarding the unavailability of the email address shall be sent to the senders of emails to the cancelled email address. Receiving emails at a cancelled email address shall be disabled. The content of mailboxes shall be archived in accordance with the applicable legislation until the email address is cancelled. Redirecting email to another user's mailbox shall be prohibited.

Article 60

Emails received by a user to their email address may only be opened by that user or a person authorised by the user in writing, and by other users only based on an order of a competent state authority or in exceptional cases (the sudden dismissal of the worker, the death of the worker, or some other extraordinary event) by a committee based on the director's decision if this is unavoidably and absolutely necessary for work process management. In doing so, the applicable law and all regulations applicable to the handling of passwords in such cases shall be adhered to.

Article 61

The content of a public employee's email shall be inspected by a three-member committee, each time appointed by the director's decision. It shall include at least one non-managerial representative of the Agency's public employees. The committee shall write a report on the inspection.

The public employee at issue shall be informed in advance in writing of the possibility of access referred to in paragraph one of this Article, except in exceptional cases when this is not possible. Notification of a public employee by email shall be considered sufficient notification in such a manner that when sending an email the option of requesting a read receipt and delivery receipt shall be selected.

Article 62

Emails sent to single dedicated email addresses (e.g. main office, info email) shall be opened by authorised persons.

Mailbox default settings

Article 63

Users may not change the default settings of their email mailbox. In order to use additional features, they shall be required to obtain a special permit or approval from the administrator.

Email message size

Article 64

As a rule, the maximum size of messages when sending or receiving email together with an attachment between individual email systems shall be limited to 10 MB. If the limit is exceeded, the message shall be automatically rejected and the sender notified thereof.

The maximum size of an allowed attachment may be limited according to the available computer resources and the needs of the employee's workplace in order to prevent the failure of the email service. The file compression ratio and the number of recipients of an individual email may also be limited.

Article 65

If a user receives an email not intended for them, the content of that message may not be stored or used in any manner. The user shall notify the sender of this error and immediately delete or otherwise destroy the email. The user may send the email to the correct addressee before destroying it if their identity is unambiguously evident from the message.

Article 66

Users shall respect personal data, copyright and intellectual property rules, particularly by not using the email system to send personal data, copyrighted data or computer programmes.

When handling sensitive data, the legislation in force shall be strictly adhered to.

Email deletion

Article 67

Each user shall periodically delete all emails that they no longer needs from their mailbox and shall do so at the request of the administrator. When storing emails, users shall follow the principle of rationality and avoid storing documents in multimedia data formats that use significant space (videos, high-resolution images, audio recordings).

Users shall promptly delete any emails that are of a private nature.

Special authorisations

Article 68

The Agency's IT unit shall be responsible for the safe and uninterrupted operation of the email system.

In the event of the suspicion of the commission of a criminal offence using emails, the procedures shall be carried out in accordance with the applicable legislation by order of the competent state authority. Viewing emails out of curiosity or at the behest of unauthorised individuals shall not be permitted.

Access to data

Article 69

Mechanisms to prevent unauthorised access to data and organisational and technical procedures to prevent the unauthorised processing of data, including modification or destruction, shall be established.

Article 70

All sensitive databases (electronic and paper) shall have appropriate access logs in which it is recorded who accessed them and when and why, in accordance with the applicable legislation. All service and maintenance works on the server, database, application or service shall also be kept.

Access to sensitive databases in electronic form shall be protected by appropriate access rights (e.g. login name and password, certificate and password, one-time password, biometrics).

Article 71

Access rights shall be regulated in such a manner so as to enable an individual access to the minimum possible set of data necessary for the performance of their tasks.

Article 72

Usernames, passwords, access verification cards, certificates and other approved access mechanisms as well as the resulting access rights to information systems and sensitive databases shall always be issued to one person and shall be non-transferable. Lending shall not be allowed.

Article 73

The password of a system user shall be intended only for their use, thus system users shall be responsible for all activities that occur using their identity. Passwords must not be written down on paper or stored in any other way that could allow another person to access the password. A password must not contain the name and surname of the user or their family members, any form of date of birth, name, the Agency's designation or number and serial numbers.

When choosing and changing passwords, users shall be required to follow the following rules:

- the password must be at least six characters long;
- the password must consist of at least three different characters, of which at least one is a letter or symbol;
- the password may not contain the letters *č, š* or *ž;*
- the password must be changed at least once every six months;
- at least five consecutive passwords may not be used again.

Article 74

Premises in which data are processed shall be protected by organisational, physical and technical measures that prevent unauthorised persons from accessing the data and means of information technology by which the latter are processed.

In the case of electronic databases of sensitive data, it shall be required to meet the appropriate organisational and technical conditions for the maintenance of these databases and to ensure procedures for backing up and archiving these data in accordance with the legislation in force.

Article 75

Employees shall protect sensitive data that they become aware of during their employment. They shall protect them even after the termination of employment.

IV. IT EQUIPMENT AND SERVICE PROCUREMENT POLICY

Preparation of an order

Article 76

When preparing order specifications for the purchase of components or the maintenance of information systems, it shall be required to plan and define the security elements that meet the requirements of the ISP and applicable legislation.

Security features in a contract

Article 77

A contract shall specify the subject and scope of the service, the criteria, the obligations, and the related consequences affecting the quality of the performance of contractual obligations in relation to the ISP.

An outsourcing contract shall include a provision on knowledge of and acceptance of the ISP and commitment to data protection where necessary.

Outsourcers, subcontractors and their employees who are to perform the work under the contract shall be required to sign an information security policy acknowledgement form before entering into the contract.

For any valid contract concluded before the entry into force of the ISP, an appropriate annex to the contract shall be concluded with the contractors and an information security policy acknowledgement form signed where reasonable and practicable.

Article 78

In contracts under which outsourcers process sensitive data, it shall be required to specify which data are processed, how they may be processed, and who may process them.

Article 79

Access to and modification of the Agency's information systems by outsourcers shall be recorded.

V. INFORMATION SYSTEM MANAGEMENT POLICY

Article 80

A system administrator shall be responsible for the network and its security. The system administrator shall constantly check the consistency of the network and its compliance with the documentation. They shall check the physical and logical settings of its components and the network itself when making changes or at least once a year.

Article 81

The management of information systems and networks shall be divided into several tasks, which shall, if possible, be performed by different persons. The performance of tasks shall be properly monitored.

Article 82

Users shall report any security incident to the system administrator or IT unit when the antivirus software detects malicious code or the user suspects that an email is infected with a virus.

In such cases, the user shall immediately stop using the computer and may resume their work only after the incident has been resolved.

Article 83

Log records of changes and modifications to the information system shall be created regularly. The scope of the data in such logs and the retention period shall be proportionate to the purpose of the recording and shall comply with the legislation in force.

VI. LIABILITY FOR AN INFRINGEMENT OF THESE PROVISIONS

Article 84

An infringement of the provisions of these organisational instructions by employees shall mean an infringement of the obligations arising from the employment relationship, while other persons shall be liable for an infringement on the basis of their contractual obligations.

The liability referred to in the preceding paragraph shall not exclude criminal liability or liability for damage in accordance with the applicable legislation.

VII. FINAL PROVISION

Article 85

These organisational instructions shall enter into force on the day following their adoption and shall be published on the Agency's intranet, and the notice of publication shall be sent by email to all public employees of the Agency.

Ref. No.:
Date: 13 January 2014

Dr Matej BREZNIK, mag. farm.
Director