(Version of Order No BR1-207 of 4 June 2025, effective from 4 June 2025)

Annex 4
to the Information Security Policy
of the National Paying Agency
under the Ministry of Agriculture

SUMMARY OF THE INFORMATION SECURITY POLICY OF THE NATIONAL PAYING AGENCY UNDER THE MINISTRY OF AGRICULTURE

SECTION I
GENERAL PROVISIONS

1. The Information Security Policy of the National Paying Agency under the Ministry of Agriculture (hereinafter referred to as – the Information Security Policy) is a document regulating the main provisions of information security within the National Paying Agency under the Ministry of Agriculture.

2. The Information Security Policy is approved by order of the Director of the National Paying Agency under the Ministry of Agriculture. Parts of this document may be disseminated to parties related to the information of the National Paying Agency under the Ministry of Agriculture in a form accessible and comprehensible to them.

3. The purpose of the Information Security Policy is to present the position of the management of the National Paying Agency under the Ministry of Agriculture regarding information security.

4. Information is a strategically important asset for the activities of the National Paying Agency under the Ministry of Agriculture; therefore, its loss, unlawful alteration, damage, or interruption of information processing may cause disruptions to the activities of the National Paying Agency under the Ministry of Agriculture. Given this, the Information Security Policy sets out the main guidelines that must be followed by all civil servants and employees of the National Paying Agency under the Ministry of Agriculture working under employment contracts, contractors, and related parties in order to protect the information of the National Paying Agency under the Ministry of Agriculture. The Information Security Policy is approved by the management of the National Paying Agency under the Ministry of Agriculture.

5. ***(Version of Order No BR1-141 of 1 June 2018, effective from 1 June 2018)***

The Information Security Policy applies to all operational processes of the National Paying Agency under the Ministry of Agriculture and covers oral and written information, information systems, computer networks, the physical environment, civil servants and employees working under employment contracts, related parties, contractors, including remote workers or other persons working at the National Paying Agency under the Ministry of Agriculture, including employees working for third parties who lawfully process the information of the National Paying Agency under the Ministry of Agriculture.

6. Information security includes three main aspects:

6.1. information confidentiality – protection of information from unauthorised disclosure;

6.2. integrity – protection of information from unauthorised or accidental alteration;

6.3. availability – ensuring that information is accessible when needed for the proper functioning of the National Paying Agency under the Ministry of Agriculture.

7. The Information Security Policy:

7.1. describes the policy of the National Paying Agency under the Ministry of Agriculture intended to protect the confidentiality, integrity and availability of its information assets, i.e., technical equipment, software, premises, and information;

7.2. establishes liability for information security;

7.3. provides references to security documents that constitute the information security management system.

8. The summary of the Information Security Policy must be reviewed at least once a year.

SECTION II
TERMS AND ABBREVIATIONS

9. The following terms are used in this Summary of the Information Security Policy:

9.1. ***(Version of Order No. BR1-280 of 23 July 2020, effective from 1 August 2020)***

Data Protection Officer – a civil servant or employee of the Information Security Division of the Prevention and Security Department of the National Paying Agency under the Ministry of Agriculture, appointed by order of the Director, who performs the functions of a Data Protection Officer;

9.2. **Information Security** – includes the preservation of the confidentiality, integrity and availability of information. Additional criteria may be included, such as authenticity, accountability, non-repudiation and reliability;

9.3. ***(Version of Order No. BR1-117 of 8 May 2018, effective from 8 May 2018)***

Information Security Incident – one or more undesirable and unexpected information security events that are likely to harm activities and pose a threat to information security;

9.4. ***(Version of Order No. BR1-117 of 8 May 2018, effective from 8 May 2018)***

Information Security Event – an identified system, service or network event indicating a possible gap in the information security policy or a failure of information security measures, or the emergence of an unforeseen situation that may be related to information security;

9.5. ***(Version of Order No. BR1-280 of 23 July 2020, effective from 1 August 2020)***

Information Security Officer – a civil servant or employee of the Information Security Division of the Prevention and Security Department of the National Paying Agency under the Ministry of Agriculture, appointed by order of the Director, responsible for implementing and maintaining information security management within the National Paying Agency under the Ministry of Agriculture.

9.6. **Malicious Software** – software designed with harmful intent or having a negative effect, e.g., viruses, worms, Trojan horses, spyware, etc.;

9.7. **Confidential Information** – information that is accessible and disclosed only to authorised persons;

9.8. **Confidentiality** – a property that ensures information is not accessible or disclosed to unauthorised natural or legal persons or processes;

9.9. **User** – a civil servant or employee of the National Paying Agency under the Ministry of Agriculture working under an employment contract, a contractor, a temporary consultant, or any other person working at the National Paying Agency under the Ministry of Agriculture, including employees working for third parties who lawfully process the Agency's information and who have been granted the right to access the information and/or information systems of the National Paying Agency under the Ministry of Agriculture and to use the resources of the information system for the performance of assigned functions;

9.10. **Software** – application software, system software, development tools and service programmes;

9.10[1]. ***(Version of Order No. BR1-207 of 4 June 2025, effective from 4 June 2025)***

Endpoint Device – a device or part of a device intended for receiving and/or transmitting information, which is directly or indirectly connected by any means to the internal electronic communications networks of the NPA;

9.11. **Encryption** – a process of converting data from its original state into a state in which the data cannot be read (used) without tools/information (an encryption key) that enable the data to be returned to their original state;

9.12. **Third Party** – a person or organisation recognised as independent from the persons involved when assessing the matter under consideration;

9.13. **Assets** – anything that has value to the National Paying Agency under the Ministry of Agriculture. In Annex 11 "Description of the Procedure for Information Security Risk Management" of the Management Systems Manual of the National Paying Agency under the Ministry of Agriculture, approved by Order No BR1-1404 of 30 December 2013 "On the Approval of the Management Systems Manual of the National Paying Agency under the Ministry of Agriculture," assets are defined as information resources;

9.14. ***(Version of Order No BR1-17 of 22 January 2024, effective from 22 January 2024)***

Management – the Director of the National Paying Agency under the Ministry of Agriculture and the Deputy Directors.

10. The following abbreviations are used in this Information Security Policy Summary:

10.1. **Agency** – the National Paying Agency under the Ministry of Agriculture;

10.2. **EU** – the European Union;

10.3. **IT** – information technology;

10.4. **Officials** – the Agency's civil servants and employees working under employment contracts.

SECTION III
ORGANISATION OF INFORMATION SECURITY

11. The Management ensures the Agency's Information Security by providing clear leadership in this process, assuming commitments, and clearly allocating responsibility for Information Security.

12. Representatives of related parties and contractors must:

12.1. comply with the Agency's Information Security Policy and the requirements of related documents;

12.2. ***(Version of Order No. BR1-207 of 4 June 2025, effective from 4 June 2025)***

protect the Agency's entrusted technical equipment, Software, endpoint devices, and information;

12.3. prevent the installation of Malicious Software in the Agency's information systems;

12.4. report all suspected or actual Information Security incidents in accordance with the established procedure;

12.5. notify the Agency on the same day they become aware that a contractor's employee holding access rights to the Agency's information or information systems is being dismissed, but no later than the contractor employee's last working day.

SECTION IV
RULES FOR THE USE OF THE INFORMATION SYSTEM

13. The purpose of the Information System use rules is to protect the Agency, its Officials, and its partners from unlawful and/or harmful actions carried out intentionally or unintentionally by persons, and from the consequences of such actions. These rules (hereinafter referred to as – the User Standard) establish the rules for acceptable use of information and communication technologies in the workplace during working hours, as well as the rules and scope of User monitoring and control in the workplace.

14. ***(Version of Order No. BR1-207 of 4 June 2025, effective from 4 June 2025)***

The Agency's Information System – including (but not limited to) electronic information, the internet, intranet, the internal computer network, hardware (servers, endpoint devices), operating systems, data media, information system accounts, email, and internet browsing (hereinafter referred to as – the Information System) – is the property of the Agency.

15. The Information System must be used solely for the performance of operational functions.

16. The Agency's Information Security depends on the efforts of all Officials and related third parties who in any way use the Agency's information; therefore, each User must familiarise himself/herself with this User Standard and act in accordance with its provisions.

17. The provisions of this User Standard are mandatory for all Users.

18. General principles of Information System use:

18.1. Users must use the Information System only for work-related purposes, in accordance with approved work procedures and Information System user instructions;

18.2. For the purposes of ensuring Information Security and maintaining the Information System, authorised Officials may at any time inspect the operation of hardware or Software, network traffic, and User activity within the Information System;

18.3. The Agency reserves the right to audit the Information System and activities carried out within it in order to ensure compliance with the User Standard;

18.4. Users have the right to consult the Officials of the Information Technology Department on matters related to the use of hardware and Software;

18.5. Users must protect their Information System passwords. It is prohibited to share Information System usernames, or to log into the Information System using another User's login credentials;

18.6. Under no circumstances may Users, when using the Information System, engage in activities that are illegal, criminal, or otherwise violate the legislation of the Republic of Lithuania or international law;

18.7. ***(Version of Order No. BR1-141 of 1 June 2018, effective from 1 June 2018)***

On matters related to EU and Republic of Lithuania legislation regulating personal data protection, Users shall be advised and provided with recommendations by the Data Protection Officer, whose contact details are available at the "Personal Data Protection" section of the website www.nma.lt.

19. The actions listed below are prohibited. Exceptions may be applied to those Users who must perform the specified actions for the performance of lawful operational functions (e.g.: maintenance of the Information System, investigation of information security incidents, etc.). The list of prohibited actions provided below is not exhaustive; it is of an informative nature, enabling the User to understand the boundaries of potentially unauthorised actions:

19.1. to disclose the Agency's Confidential information on the internet;

19.2. to infringe the rights of individuals protected by trademarks, trade secrets, patents or other intellectual property or related rights, including (but not limited to) installing, storing, using, copying or distributing illegal Software (or other Software for which the Agency does not hold usage rights);

19.3. to unlawfully copy copyright-protected content, including (but not limited to) scanning images or text in part or in full from books, magazines or other sources, copying music recordings, Software, etc.;

19.4. to export Software or hardware, Encryption technologies or Encryption methods in breach of the export restriction requirements of the Republic of Lithuania or the EU (in case of doubt, the Information Security Officer must be consulted);

19.5. to download or distribute graphic, audio and video materials, games and Software that are not directly related to work, or to send data infected with viruses or containing other harmful

programme code, or files that may disrupt the functioning and security of computer or telecommunication devices and Software;

19.6. ***(Version of Order No. BR1-207 of 4 June 2025, effective from 4 June 2025)*** to independently modify or repair Endpoint Devices (IT and telecommunications equipment) and Software;

19.7. to disclose Information System login credentials to other persons (including family members when working from home);

19.8. to use the Information System for activities prohibited by law, or for information of a defamatory, insulting, threatening nature, or information contrary to the principles of public decency and morality, or for sending computer viruses, mass malicious information (spam), or for any other purposes that may infringe the legitimate interests of the Agency or other persons;

19.9. to use the Information System for creating or transmitting information containing disturbing, offensive, pornographic or similar content, or content that may be construed as sexual harassment;

19.10. to discriminate or harass in any form when using email, telephone or any other means, for example by the frequency or size of messages, etc.;

19.11. to use email and internet access for personal or commercial purposes, or to offer goods or services not provided by the Agency, using the Agency's name;

19.12. ***(Version of Order No. BR1-207 of 4 June 2025, effective from 4 June 2025)*** to use Software and/or Endpoint Devices for unauthorised access to the Information System or for checking its data security, scanning, or monitoring computer network traffic;

19.13. to collect data or fragments of data transmitted over computer networks, or to analyse their nature, quantity, etc., unless this is necessary for performing lawful operational functions (e.g.: Information System maintenance, investigation of information security incidents, etc.);

19.14. to attempt to bypass the User authentication mechanisms of the Information System;

19.15. to perform denial-of-service attacks or otherwise disrupt the work of other Users within the Information System;

19.16. ***(Version of Order No. BR1-207 of 4 June 2025, effective from 4 June 2025)*** to transfer Endpoint Devices (IT and telecommunications equipment) and Software belonging to the Agency to Third Parties, if such transfer is not related to the performance of work functions or may in any way harm the interests of the Agency;

19.17. to provide information about Users or to provide User lists to non-Officials;

19.18. to exploit vulnerabilities of the Information System, including (but not limited to) access to data not intended for the User to log into the Information System or part thereof, unless required for performing lawful operational functions (e.g.: Information System maintenance, investigation of information security incidents, etc.);

19.19. to alter or otherwise misuse e-mail headers;

19.20. to use another User's e-mail address;

19.21. to create or forward chain e-mails encouraging recipients to forward the e-mail to friends, etc.;

19.22. to perform other actions unrelated to work functions or in violation of applicable laws.

20. Furthermore, without the approval of the Agency's Director or authorised Officials, it is prohibited to send emails containing information on the functioning principles of the Information System and their regulation, as well as measures for ensuring and controlling Information Security.

21. When Users use email and internet resources for personal purposes, the Agency does not guarantee the confidentiality of personal information.

22. Identification and authentication. The User shall:

22.1. comply with the established password usage requirements:

22.1.1. keep the password confidential and not disclose it to any person under any circumstances;

22.1.2. ***(Version of Order No. BR1-100 of 25 March 2021, effective from 25 March 2021)*** change the password at least once every 2 months (this requirement applies without exception to administrators as well);

22.1.3. use a password containing at least 8 characters;

22.1.4. use a unique password that cannot be reused from the previous 6 passwords;

22.1.5. use a password composed of letters, numbers and special characters;

22.1.6. when creating a password, not use personal information, widely known words or names (e.g., Vilnius).

22.2. comply with additional password usage requirements established by the Information System administrators:

22.2.1. ***(Version of Order No. BR1-100 of 25 March 2021, effective from 25 March 2021) No longer in force***

22.2.2. to use a password consisting of at least 12 characters;

22.2.3. not to reuse a password identical to the previous 3 passwords;

22.2.4. to store the password in a safe;

22.2.5. ***(Version of Order No BR1-449 of 30 December 2022, effective from 30 December 2022)*** if passwords are stored on an electronic medium, it must be encrypted with a password.

23. A User's access to the Information System is blocked if the password is entered incorrectly 3 times consecutively. In such cases, the User must contact the Agency's Help Desk and may only log in again with the administrator's permission.

24. Without the permission of an Official of the Systems Administration Division of the Information Technology Department, the User must refrain from:

24.1. installing and using any software obtained from the Internet or provided on disks or in any other form without authorisation;

24.2. changing the configuration of computer hardware or operating systems;

24.3. using unlicensed or unauthorised Software.

25. The User must ensure that Confidential Information is used and processed in accordance with the terms of the contract.

26. ***(Version of Order No. BR1-207 of 4 June 2025, effective from 4 June 2025)*** A User who notices disruptions in the operation of the Information System must immediately report them to the Agency's Help Desk (by email pagalba@nma.lt or by phone +370 5 252 688) and to the Official responsible for the contract (if the relationship is based on a contract between the Agency and a third party). The User must immediately inform the Information Security Officer (by email saugos.igaliotinis@nma.lt or by phone +370 5 252 6909) and his/her direct supervisor about any Information Security incident.

27. The liability of representatives of related parties and contractors for the use of all information processing resources, whether used by themselves or by other authorised persons, is defined in the contracts.

28. To protect: the Agency's Confidential Information, the personal data of clients and Users from disclosure to Third Parties; the Information System from cyber-attacks, intrusions and data theft, viruses, dangerous websites, and Malicious Software; the Agency's Assets and to ensure security within the Agency's premises and territory; the Agency's interests and to ensure compliance with work duties and internal regulations, and in accordance with the principles of necessity, expediency, transparency, proportionality, accuracy, and data retention and security, to the extent necessary to achieve the intended objectives, the Agency carries out User monitoring and control at the workplace.

_____