INFORMATION SECURITY GUIDELINES FOR THE CONTRACTORS

VERSION: 5.0

Approved by
Deputy Director
of the Audit and Information Security Office
on 11 January 2017

This document is drawn-up pursuant to the Ordinance of the President of the Agricultural Market Agency (AMA) No. 224/2016/W of 27 October 2016 on the implementation of the "Information security management principles" in the Agricultural Market Agency, as amended.
Any motions aiming at improving information security should be submitted to the Audit and Information Security Office (AISO).

1. The *Information security guidelines for the contractors* constitute the set of rules obligatory for the contractors performing the supplies or providing services for the AMA and the persons outside AMA having access to information resources under the separate regulations or contracts. The Guidelines are enclosed to the contracts made with the contractors, who shall familiarize with the Guidelines content and oblige to follow them. Updating and approving of the document shall be the responsibility of the Deputy Director of AISO, being the document owner.
2. Any infringement to information security rules by the intern may effect in prompt termination of the internship and dissolution of the contract. In such case the internship is not completed.
3. Any infringement to the information security rules by the trainee may effect in prompt termination of the on-the-job training and dissolution of the contract. In such case the on-the-job training is not completed.
4. Any infringement to the information security rules by any natural person employed under the contract of commission or contract for specific work may effect in prompt dissolution of the contract and constitutes the basis to claim for damages or payment of contractual penalty, if the concluded contract so specifies.
5. Any infringement to the information security rules by a contractor shall constitute the basis for withdrawal of AMA from the contract and claim for potential damages or payment of contractual penalty, if the concluded contract so specifies.
6. Liability for AMA information security shall cover the AMA head office and any cases of processing AMA activity-related information outside its head office. This includes in particular remote access to AMA IT network.

Physical and environmental safety

1. AMA establishes the following secured areas:
   a) administrative zones,
   b) security zones.
2. Administrative zone is the area used by AMA.
3. The borders of administrative zone are provided with operating electronic access control.
4. Access to warehouse premises is supervised, with personnel and material traffic control operating.
5. Security zone is the separated part of administrative zone equipped with additional, independent security systems.

6. Access to the security zones is restricted only to the persons who obtained the applicable authorisations. Entrance and exit from the security zones is recorded. ID of the persons and time of entry/exit are recorded..
7. Carrying in and out of electronic data carriers into and from the security zones is supervised.
8. Using cameras, video cameras, audio devices or any other recording devices e.g. cameras in mobile devices to record image or sound in the security zones without authorisation of the IT Office (ITO) is prohibited.
9. Presence of persons holding no right of access to the security zones is permissible only in exceptional cases and for specific purposes, in the Head Office and upon issuing the authorisation of the persons responsible for supervision over the individual zones, in the Regional Branches (RB) of the AMA – Director of the Regional Branch of AMA. Presence of persons holding no right of access to the security zones is permissible only when supervised by the persons holding the access rights to the given zone.
10. Presence of the person holding no right of access to the security zone subject to the RB Director must be recorded by the introducing person in the register, pursuant to the Procedure Record IT Management [PR_ITM].
11. Passageways of the facilities are provided with the boards informing on the direction of evacuation route and, if possible, equipped in emergency lighting system. Fire instructions are drawn-up as provided in the laws and regulations in force.

Access to IT system resources

1. Access to the IT system (ITS) may be provided only to the authorised users.
2. The persons being not the AMA employees cannot obtain the user profile or authorisations to use the ITS without prior consent of the administrator in writing. The above shall not apply to legally authorised authorities.
3. The rights of the users being not the AMA employees cannot be assigned for an indefinite period of time and must be updated every 90 days.
4. The terms and conditions of use the internal AMA network and external ITSs are regulated by the concluded agreements, specifying the technical and functional conditions of the connection in details. The agreement must contain the clause concerning the observance of the AMA's informational system security rules.
5. The persons holding access to the ITS and being not the AMA employees must sign the statement on observing the rules specified in the Information security guidelines for the contractors. This statement arises when signing the contract, appendix to which these Guidelines are the appendix.

Access to AMA resources from the networks of the other institutions

1. AMA may provide access to the IT network to the persons and entities authorised under the laws and regulations.
2. The application for access to the AMA network should contain information on the purpose of connection, estimated number of connected work places and users, method of security against unauthorised access.
3. Prior to issuing the decision on consent to access to the AMA network, the President of AMA shall consult the Steering Committee for Information Security (SCIS).
4. Technical specification of the connection must form an appendix to the agreement or contract made between the AMA and institutions. The specification should contain in particular the following arrangements:

   a) connection should be encrypted and secured with applicable certificate;

   b) connection should be established only between strictly defined IP addresses of the connected network of the AMA's internal network and for strictly defined ports allocated to the addresses in the AMA's network;

   c) each establishing of the connection between the connected network and AMA's network should be authorised with password or certificate and logged-on;

   d) resources provided to the users from the other institutions include only access to applications. File servers or mailbox are not enabled.
5. The users from the other institutions cannot hold the administrator rights.

Security against malware and mobile code

1. All electronic data carriers externally supplied to AMA cannot be used without prior scanning with anti-virus programme.
2. All files, before sending or transferring to any third parties (persons being not the AMA employees), are tested with anti-virus software.

System acceptance

1. Prior to handover for use of the software developed for AMA, the developers must delete all special access paths to enable access only with the use of AMA security rules. This means that any undocumented functions enabling security system bypass must be deleted. All system rights established for the purposes of software development however unnecessary in the production environment must be also deleted.
2. In the case of making a decision on storage of source code developed on request of AMA outside the AMA's head office, entering into deposit agreement on such source code with the entities independent from the software supplier is necessary. These agreements should specify the independent entity, to which the software developer shall provide the source code along with all updates thereof. They should also specify the circumstances in which the source code is to be

enabled to AMA, including among others bankruptcy or liquidation of the software supplier or its non-performance from the contractual obligations on software updates.

Infringement of information security

1. The employees, contractors and users representing the third party and using the informational systems are obliged to report the events indicating or proving the infringement of information security to the AMA employee supervising their operations.
2. Infringement of information safety (incident) shall be understood as, in particular:

   a) infringement or attempted infringement of the information processing system integrity;

   b) infringement or attempted infringement of integrity of information in the processing system – any and all modifications (adding, changing, deleting), damage or attempted modifications by any unauthorised persons or authorised persons acting in bad faith or as an error or authorised person (e.g. change of data content, loss of all or part of data);

   c) infringement of confidentiality by purposeful or unaware transfer of information to any person not authorised to receive it;

   d) infringement of security protection in the ITS (e.g. unauthorised logging-on to the system or any other symptom indicating the attempt or activity related to illegal external access into the ITS effecting in access to information, access to which should be impossible);

   e) unauthorised access or attempted access to ITS (e.g. unauthorised operation on the user's account);

   f) enabling access to information to any unauthorised person; e.g. leaving data copy (in printer, xero machine, on the table), failing to block access to ITS (during absence of authorised person), no supervision over the service workers and other unauthorised persons;

   g) unauthorised access or attempted access to premises in which information is processed;

   h) revealing individual users' access passwords (or password hashes) to ITS;

   i) unauthorised copying of information or printouts;

   j) creating no backup copies;

   k) change or deleting information stored on backup or archive copies;

   l) intended or unintended loss of data confidentiality by loss of: mobile device, e-signature key, backup copy, data carrier or any other component of the AMA's informational system (including in effect of theft) and failing to undertake appropriate neutralising activities in due time;

   m) no data carrier – theft or loss of printout, backup copy, disc or any other data carrier;

   n) improper destruction of data carriers containing sensitive or statutorily protected data, preventing their readout – disposal of non-destructed carriers (e.g. printouts, CD/DVDs);

o) erroneous (excessive) granting of rights to information processing or granting of rights to the persons not meeting the requirements;

p) any other events indicating or proving infringement of information security.

Intellectual property right

When creating intellectual property on request of AMA, the contract made with the contractor contains the provision on transfer of copyrights to the work.