Directive on Identification and Removal of Sensitive Information from Documents which are to be Made Available to Public

Article 1
Purpose of Directive

Purpose of the Directive is to define the manner for identification of sensitive information in documents that are to be made available to:

a) Public pursuant to Act No. 211/2000 Coll. on Free Access to Information and on Amendments and Supplements to Certain Acts (Freedom of Information Act); or
b) Parties to the proceedings pursuant to Act No. 50/1976 Coll. on Territorial Planning and Building Order (Building Act) as amended or Act No. 541/2004 Coll. on Peaceful Use of Nuclear Energy (Atomic Act) and on Amendments and Supplements to Certain Acts as amended defined under Art. 8 (2) of the Atomic Act

and its subsequent removal in these documents including identification of indicators and arguments supporting the decision making that a particular information is a sensitive one.

Article 2
Application Area

The Directive is valid for all employees of the Authority participating in identification and subsequent removal of information in documents defined in Article 1 hereof.

Article 3
General Part, Definition of Terms

1. With regard to the global security situation, the Authority likewise other supervisory bodies worldwide considers necessary to determine pieces of information which cannot be made available to public in order to avoid their use for malevolent activities.

   Sensitive information is defined in Act No. 350/2011 Coll. amending Act No. 541/2004 Coll. on Peaceful Use of Nuclear Energy (Atomic Act) and on Amendments and Supplements to Certain Acts as amended, in Art. 3 (14) as follows: "The documentation containing sensitive information is the documentation whose publication could be used for planning and execution of activities in order to cause the disturbance or destruction of the nuclear installation and thus unfavourably influencing the security of the public[1)] and causing ecological or financial damage. This documentation shall not be published pursuant to the special regulation.[2)]".
2. The Directive defines conditions used for determination of a sensitive piece of information which will not be made available to entities stipulated in Article 1 hereof in order to avoid unwanted providing of information to those who would like to misuse them for malevolent

[1)] Art. 4 (4) Convention on Access to Information, Public Participation in Decision-making and Acess to Justice in Environmental Matters (Notification No. 43/2006 Coll.)

[2)] Art. 11 (1) (i) of Act on Information Freedom as amended.

activities targeted against nuclear facilities or nuclear materials or to a possible origination of an terrorist attack.

3. Sensitive pieces of information relate to all range of information, the loss, misuse, alternation or unauthorised access to which may jeopardize nuclear safety and physical protection and thus also the public interest.
4. Information is sensitive if their publishing could have a clear and signification contribution to violators and possible attack.
5. The scope of the mentioned sensitive information was determined in co-operation with ALFA Security Technologies, a.s. with the registered seat at Dúbravská cesta 3, 841 04 Bratislava, Company ID No.: 31 402 836 based on analysis and assessment included in the document titled: "Analysis of Possible Source of Leakage of Sensitive Information about Nuclear Facilities with Regard to Nuclear Facilities Physical Protection", 2013 that particular knowledge of these detailed information can be decisive in planning of malevolent activity towards the nuclear facility or nuclear materials /4/. And contrary to this, an absence of such information complicates significantly such malevolent activity or even excludes it.
6. The subsequent project of ALFA Security Technologies, a.s. continues by opposing and editing of the existing "Directive on Identification and Removal of Sensitive Information in Documents that are to be Made Public", No. 2290/2014, Ref. No. S 330 006:14 and elaborates so called "Argumentation Lines" justifying why a particular piece of information may be considered the sensitive one /5/.
7. An Argumentation Line represents a causal chain related to all arguments supporting decision making about the fact that a particular information is a sensitive one. The causal chain consists of the facts stated in respective annexes of the Directive related to a particular type of the sensitive information according to the catalogue.
8. Physical Protection (hereinafter only "PP") shall mean a set of technical, administrative or organisational measures needed to prevent and identify unauthorised activities concerning nuclear installations, nuclear material, special materials and equipment, management of radioactive waste, spent fuel, shipment of radioactive material, as well as an unauthorised entering nuclear installations and perpetrating of sabotage.[3)]
9. Security Protection System (hereinafter only "SeSy") shall mean a set of technical means, technological rules, organisational directives and way of human behaviour (Security Culture) that by its synergy effect provides for a safe and designed operation of a nuclear facility or storage, use and handling of nuclear materials.
10. Breaking efficiency of physical protection (PP) and/or efficiency of safety systems (technology protection) (SeSy) – "Breaking" shall be such an activity of the violator providing for unnoticed manipulation without clear damage to barriers and protective mechanisms. Detection systems do not have to record any activity as it is legal and performed by an authorised person. Most probably, it will be an internal perpetrator authorised to perform certain activity that he/she will however misuse against the protected interest. Breaking includes also a possible manipulation with operational instructions aimed at subsequent (e.g. in the future) initiation of a crisis situation.
11. Elimination of human resources of PP and/or SeSy - "Elimination" means control or restriction by the means of (blackmailing, threat of violation, violation or murder) of the activity of a person – employee, service personnel, PP member and other employee.
12. Elimination of PP and SeSy systems – "Elimination" shall be such a behaviour of the perpetrator which is aimed at elimination of PP and/or SeSy technical means from

[3] Art. 2 (b) of Act No. No. 541/2004 Coll. on Peaceful Use of Nuclear Energy (Atomic Act) and on Amendments and Supplementations to Certain Acts as amended.

operation or prevention of functioning of PP and/or SeSy processes and the perpetrator overcomes protective measures in an apparent manner, i.e. there is an information about his/her activity.

13. Restriction of efficiency of PP and/or SeSy – "Restriction" shall mean a particular disruption of functionality of both the PP and/or SeSy means and process. Activity of a violator can be detected.
14. Sensitive information will be removed from documents that is going to be made public in a way that the mentioned information will remain in the documents and will be removed in such a manner so that they are made illegible.

3.1 Documentation including sensitive information pursuant to the Atomic Act

Pursuant to Art. (3) (15) of the Atomic Act, the documentation including sensitive information is the documentation listed in Annex No. 1 Section A item c), Section B items a), b), i), m), Section C items a), d), i), j), s), w) and Annex No. 2 Section A item b) of the Atomic Act which is:

1. Design intention for physical and technical solution of nuclear installation at the level of initial design;
2. Preliminary safety report providing evidence for meeting the legal requirements on nuclear safety based on data considered in the design;
3. Design documentation necessary for the building proceedings;
4. Preliminary limiting conditions of the safe operation;
5. Documentation in line with Art. 6 (2) (j) of Act No. 541/2004 Coll. as amended;
6. Limiting conditions of the safe operation;
7. Nuclear facility commissioning programme divided into phases;
8. Pre-operation safety report specifying in detail the report mentioned in Section B item a);
9. For a nuclear installation with a nuclear reactor, a probabilistic safety assessment of operation for shut down reactor and for low power levels, as well as for the reactor full power;
10. Documents about preparation of the nuclear facility for commissioning, for testing operation and report assessing the nuclear facility commissioning and preparation for permanent operation, report about assessment of the testing operation;
11. Type and amount of radioactive material for transportation;
12. Type and amount of radioactive material to be imported or exported, type and amount of special material that are supposed to be exported.

3.2 Sensitive Information

Typical sensitive information which are not made public, e.g. during the building proceedings, administrative proceedings, etc. in line with provisions of Art. 4 (4) of the Aarhus Convention about exemptions from information provisioning due to possible adverse impact on the public safety can be divided into the following groups:

1) Mentioned information about:
   a) Physical protection which are not kept confidential pursuant to Act No. 215/2004 Coll.;
   b) Transportation of nuclear materials which are not kept confidential pursuant to Act No. 215/2004 Coll. /6/;
   c) Transportation of nuclear waste which are not kept confidential pursuant to Act No. 215/2004 Coll. /6/;

d) Layout of HW means, instrumentation and control of safety systems, instrumentation and control systems with regard to safety;
e) SW versions which is part of classified equipment (e.g. I&C);
f) Safety systems;
g) Graphic parts of lists of classified equipment and lists of seismically classified equipment;
h) Operative diagrams of nuclear equipment systems.

2) Information about equipment of:
   a) Emergency power supply system – category I. and II.

3) Information about analysis, calculations, results of:
   a) Probabilistic analysis (PSA);
   b) Stress calculations;
   c) Risks analysis.

4) Information about functioning of:
   a) Emergency power supply system – category I. and II. of own consumption,
   b) Instrumentation and control system of safety systems;
   c) Control system of safety systems;
   d) Connection of the nuclear facility operation staff with emergency teams.

5) Information about location of:
   a) Equipment;
   b) Buildings;
   c) Equipment for bringing raw water to the power plant;
   d) Nuclear materials
   e) Radioactive waste;
   f) Air-conditioning systems and potable water connections;
   g) Entrances into the premises (including their number);
   h) Chemical substances;
   i) Safety systems;
   j) Own consumption supply and connection to the grid.

6) Information about description, labelling of:
   a) Buildings;
   b) Rooms;
   c) Pipeline channels;
   d) Surroundings of buildings;
   e) Number of buildings, floors;
   f) Main Control Room layouts;
   g) Detailed description of IT systems;
   h) Detailed description of functions of safety systems;
   i) Detailed description of control, management systems, etc.;
   j) ES marking;
   k) Emergency power supply system – category I. and II.;
   l) Own consumption and connection to the grid;

m) Safety systems;
n) Air-conditioning and potable water system,
o) Systems of fire signalling and extinguishing.

7) Information about lists and declarations of amount of:
   a) Nuclear materials;
   b) Radioactive materials;
   c) Air-conditioning equipment and potable water connections;
   d) Chemical substances;
   e) Emergency power supply system – category I. and II.

8) Information indirectly identifying persons – employees of nuclear facilities and persons performing physical protection of the nuclear facility on the contractor´s basis:

a) Personal data not being in the scope of power of the Act on Personal Data Protection providing for identification of a person with including the job position (congratulations in the company printouts, articles about a person during various occasions, lists of participants, records, etc.);
b) Job positions and their responsibilities in particular during a non-standard operation of the nuclear facility;
c) List of participants of security shifts being on duty for protection of the nuclear facility (distribution of utensils, holiday plans, meal vouchers records, etc.).

3.2.1 Indicators of information sensitivity

Different indicators may impact safety of nuclear facilities and materials. The main and decisive ones are physical protection and safety systems (set of technical means, technological rules and organisations directives and the manner of human behaviour (Security Culture) which by the means of synergy provide for a safe and designed operation of the nuclear facility or storage, use and handling with the nuclear material).

The physical protection provides for both physical and building protection, i.e. in particular an isolation of premises in which nuclear industry processes take place (nuclear facilities, nuclear material warehouses, etc.).

Safety systems provide for functioning of technological elements and nodes in designed parameters in order to ensure the main functionality of the nuclear industry facility (run of the nuclear reactor, storage, processing and re-processing of nuclear material, etc.).

A categorical detriment in the nuclear industry circumstances is:

a) Radioactivity leakage;
b) Theft of radioactive material.

From the viewpoint of time and material development of the situation that may potentially lead to the described detriment, it is necessary analyse respective phases of development of the emergency situation.

A perpetrator needs three components to complete his/her intention: a motivation (Want), conditions (Can) and he/she must be Able, i.e. have certain abilities (skills, knowledge) and information area.

Depending on potential – and ability of the perpetrator, this information area can be used for committing a crime, the perpetrator can generate a danger or to increase an existing danger and thus naturally he/she can immediately or potentially increase a risk for the protected interest.

3.2.2 Arguments

In order to exactly define that the assessed information may be or is a sensitive one, we need a set of arguments supporting this decision.

Based on previous indicators analysis, the process of looking for arguments may be divided into three phases:

a) Find justification why is a piece of information indicated as a sensitive one, important for the perpetrator – what value does it have for him/her and his/her behaviour;
b) What impact an information in question have on decision making or behaviour of the perpetrator, i.e. what consequence its use (misuse) may have;
c) What detriment may happen in the case the information in question will be used in a due way by the perpetrator.

Given arguments are used for justification of legitimacy to declare certain pieces of information included herein in clause 3.2 as sensitive ones.

3.2.2.1 Value for perpetrator

The parameter "Value for perpetrator" expresses a morphological (content), syntactic and semantic value of a piece of information which the perpetrator reached by various means. A value can originate, it can be a supplement or confirmation of a piece of information obtained earlier.

Using association, integration, deduction and induction, the perpetrator may get a new content of knowledge even from a piece of information representing separately an absolutely "nothing to disclose" content.

Such information can provide the perpetrator in particular with:

1. Knowledge of parameters of PP and SeSy technical equipment

Even though a majority of information about physical protection is under the classified information regime, there is not the zero risk that the perpetrator can obtain these pieces of information from not classified information by the means of deduction

and physical protection. The same rule applies also to information about the security system. Knowledge of processes and parameters can allow the perpetrator to effectively plan and perform an attack using weak points or misusing information about designed parameters. It allows him/her to plan type of tools, instruments and other utensils he/she will need for breaking the resistance.

2. Knowledge of technical equipment functioning

Knowledge of technical equipment functioning allows the perpetrator to plan and execute an attack against technical equipment, failure of which can cause so called a "domino effect", i.e. series of technical failures and accidents causing a crisis situation increasing the risk of radioactivity leakage or theft of the radioactive material. This type of attack would have a nature of the technical failure or accident and under certain circumstances it could hide the fact that it was a planned attack.

3. Knowledge of PP and SeSy technical equipment functioning

Information allows for planning an effective attack by avoiding or breaking barriers formed by the both PP and SeSy elements.

4. Knowledge of both PP and SeSy procedures

Information allows for planning an effective attack by avoiding or breaking barriers formed by the both PP and SeSy procedures.

5. Knowledge of the blackmailing target (person)

This information can be created by e.g. "innocent" articles in the company printouts where there is published a congratulation at the occasion of the anniversary and a person is identified by his/her name and work position. Furthermore, that can be information without mentioning the name of a particular person including however the information that a particular process consists of identification of the job position.

6. Knowledge of the current status of technical equipment, process, people

Typical information of this type is periodicity of inspections, in particular of redundant systems. Information that "regular inspections of equipment takes place once in six month" in combination with the information about the currently performed inspection, gives the perpetrator information about the date when the given equipment will be again under the attention of the service personel and how much time he/she thus have for an uninterrupted preparation of, e.g. sabotage. Sensitive information are also information about upgrading of a particular equipment and that it will be fully operation at the particular time only.

7. Information about layout of buildings, equipment and buildings

Information of this type allows the perpetrator´s orientation in the premises where a protected interest is being located. Typical examples are orientation maps and labels for visitors. Sensitive information is also labelling of buildings and equipment including their function in the system. Moreover, it can be evidence about existence (non-existence) and manner of protection of the building or equipment in question.

8. Knowledge of the amount of material, equipment and their location

Information specifies the situation and conditions to perpetrator for committing its intention.

3.2.2.2 Manner of misuse of obtained information

Information obtained by the perpetrator, after processing (assessment, supplement and verification of the information obtained earlier) may have an impact on preparation or execution of the attack, in particular the attack tactics, its immediate behaviour or attack preparation. Components significantly impacting tactics of an attack are as follows:

1. Estimation of efficiency of equipment and process

Information about efficiency of equipment and process allow the perpetrator to estimate intensity of the resistance to overcome or factors helpful to him/her to perform the attack.

2. Enhancement of motivation, determination to perform the act

Systematic assessment of obtained information and assessment of own forces and means with regard to estimated safety and security measures can significantly impact decision of the perpetrator to perform the act and at the same time his/her courage he will use.

3. Selection of tools, transportation, transportation of material and robbery

4. Estimation of the time available to perform the attack

5. Verification or confirmation of information obtained by another manner.

3.2.2.3 Types of consequences – detriment

Limiting to conditions of the nuclear power industry, we can talk about the following types of detriment:

a) Overcoming of efficiency of physical protection (PP) and/or efficiency of safety systems (protection of technology) (SeSy);
b) Elimination of human resources PP and/or SeSy;
c) Elimination of PP and/or SeSy means;
d) Limiting of efficiency of PP and/or SeSy.

3.3 Risk analysis pursuant to respective items mentioned in chapter 3.2

All items mentioned in chapter 3.2 were subject of subsequent risk analysis. The risk analysis was performed in the following structure:

a) Group of information (according to chapter 3.2),
b) Description of information content (respective elements included in chapter 3.2),
c) Detailed specification,

d) Example. This part of the analysis was introduced with the aim to better understand the content and detailed specification;
e) Value for a perpetrator. Value for the perpetrator was identified with the aim to detect respective types of danger and was performed according to the model (Picture No. 2):

   - Knowledge of parameters of PP technical equipment;
   - Knowledge of parameters of SeSy technical equipment;
   - Knowledge of functions of PP technical equipment;
   - Knowledge of functions of SeSy technical equipment;
   - Knowledge of PP procedures;
   - Knowledge of SeSy procedures;
   - Knowledge of blackmailing target;
   - Knowledge of current status of technical equipment;
   - Knowledge of current status of process;
   - Knowledge of current status of human resources;
   - Knowledge of layout of buildings, equipment and civil structures;
   - Knowledge of the amount of material, number of equipment and their location;
   - Combination of information.

f) Manner of misuse (Can impact) (we looked for the manner of misuse of information by the attacker) (**Chyba! Nenašiel sa žiaden zdroj odkazov.**):
   - Tactics of attack,
   - Estimation of efficiency of equipment and process;
   - Enhancement of determination to act;
   - Selection of a tool,
   - Selection of manner of transportation;
   - Selection of manner of transportation for material and robbery,
   - Estimation of the time available for performance of attack;
   - Verification or confirmation of information obtained by another manner.

g) Consequence (**Chyba! Nenašiel sa žiaden zdroj odkazov.**) – detriment in line with the Causality Pyramid **Chyba! Nenašiel sa žiaden zdroj odkazov.**:
   - Overcoming of PP efficiency;
   - Overcoming of SeSy efficiency;
   - Elimination of PP human resources;
   - Elimination of SeSy human resources;
   - Elimination of PP technical means from functioning;
   - Elimination of SeSy technical means from functioning;
   - Limiting of efficiency of PP technical means;

- Limiting of efficiency of SeSy technical means;
- Combination of consequences.

Results of the risk analysis of respective items from clause 3.2 are included in Annex No.2.

Performed risk analysis confirmed legitimacy of respective items of the Directive included in clause 3.2.

3.4 Elaboration of the argumentation apparatus

With regard to respective items included under clause 3.2, there is an argumentation apparatus elaborated to confirm legitimacy to consider respective information to be sensitive one.

This algorithm is being followed:

a) Elaboration of the list of groups of sensitive information in the field of technology, processes and human factor,
b) Elaboration of the risk analysis for respective groups of sensitive information,
c) Elaboration of argumentation lines and their reduction to a practically applicable scope.

3.4.1 Elaboration of categories of sensitive information groups

Categories of groups of sensitive information in the following areas:

a) Technology – sensitive information describing those parts and parameters of technology that may lead to increase of the risk.
b) Processes – sensitive information about existence and content of processes that may lead to increase of the risk.

c) Human factor – information that seems to be harmless but that are by its content and in particular in context with other information form sensitive information.

3.4.2 Elaboration of the risk analysis for respective groups of sensitive information

For respective groups of sensitive information there was elaborated the risk analysis in the following composition:

a) Category (technological, processes, human factor);
b) Code (an identification that can be practically used in the further processing of the work objective);
c) Group of sensitive information (relatively precise specification of the content of sensitive information);
d) Value for the perpetrator – risk carrier. It means the benefit which the obtained information give to the perpetrator for planning and performing an attack;
e) Use from the perpetrator´s viewpoint;

f) Negative consequence – description what may be the consequence of misuse of the sensitive information by the perpetrator;
g) Risk (an estimation in the scale "High – Medium – Low". It is an expert but a subjective estimation.

Complete results of the risk analysis for respective groups of information is mentioned in Annex No.3. By the means of the risk analysis, there was a catalogue of sensitive information created divided into categories.

3.4.3 Elaboration of argumentation lines and their reduction to a practically applicable scope

The last part of argumentation is elaboration of argumentation lines for their practical application to prove legitimacy when marking information in documentation as sensitive.

Dividing of arguments into three categories and several groups is mentioned in Annex No 4. From Annex No 4 follows that in category:

a) Technology, there were identified 12 groups of sensitive information in total;
b) Processes, there were identified 9 groups of sensitive information in total;
c) Human factor, there was identified 1 group of sensitive information.

The mentioned structure is quite unclear. Due to this reason, it was necessary to find further elements for conformity or proximity in order to reduce their number. The reduction is highlighted by different colour in Annex No. 5. After the reduction, there were reduced argumentation lines created included in Annex No. 6

We can state that division in Annex No.6 can be used for argumentation why a particular piece of information is considered a sensitive one.

Article 4
Processes, Activities, Responsibilities

1. Receipt and recording of request for providing or making available pieces of information or documentation.
   Responsible: Secretariat of the Authority

2. Assignment of the request for providing or making available pieces of information or documentation to a responsible department in line with the Registry Order and Registry Plan of the Authority /7/ in co-operation with the Office of the Authority.
   Responsible: Head of departments

3. Assessment whether it concerns request for making available documentation consisting of sensitive information.
   Responsible: Head of respective responsible department

4. Appointment of the employee responsible for removal of sensitive information or providing further instructions for processing of the filing.
   Responsible: Head of respective responsible department

5. In the case the documentation assessment requires co-operation of several experts within the department, or several departments of the Authority or and external organisation, the head of the respective responsible department shall assess the need and scope of such co-operation.
   Responsible: Head of respective responsible department

6. Co-operation of experts within the Authority is always required by an internal letter to which a respective part of documentation is being annexed.
   Responsible: Head of respective responsible department

7. Assessment of documentation by an external organisation shall be performed based on a commercial contract with the authorised entity and its professional assessment.
   Responsible: Head of respective responsible department

8. Creation of the copy of the document identifying and removing sensitive information in line with clause 3.2. hereof.
   Responsible: Appointed employee

9. Review of removed sensitive information/documentation.
   Responsible: Head of respective responsible department

10. Sending of document with removed sensitive information to the Office of the Authority by the means of internal letter.
    Responsible: Appointed employee

11. Elaboration of answer to request for provisioning/making available information/documentation and sending information/documentation to an applicant.
    Responsible: Office of the Authority

12. Sending of one counterpart of the sent answer to the appointed employee by the means of the internal letter.
    Responsible: Office of the Authority

13. Filing one counterpart of the sent documentation/information into a file.
    Responsible: Appointed employee

Article 5
Quality Targets

Not defined.

Article 6
Organisational Arrangement

1. The head of department to the power of whom the documentation belongs to shall be responsible for organisational arrangement of removal of sensitive information in documentation to be made available to the public.

2. Affected employees of the Authority follow in identification and removal or sensitive information the directive in question.

3. The head of department to the power of whom the documentation belongs to shall be responsible for compliance with this directive.

Article 7
Related Documents

1. Art. 4 (4) of Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (Notification No. 46/2006 Coll.).

2. Art. No. 11 (1) (j) of Act No. 211/2000 Coll. on Free Access to Information and on Amendments and Supplements to Certain Acts (Freedom of Information Act) as amended.

3. Act No. 541/2004 Coll. on Peaceful Use of Nuclear Energy (Atomic Act) and on Amendments and Supplements to Certain Acts as amended.

4. "Analysis of possible source of leakage of sensitive information about nuclear facilities with regard to physical protection of nuclear facilities", Doc. Ing. Jaroslav Sivák, CSc., MBA, Ing. Dušan Pivko, Stanislav Kabát, Daniel Ďurfina, Slavomír Jasan, 2013 elaborated in line with the Contract for Work No. 48/2013 concluded on 5 November 2013.

5. FINAL REPORT from project No. 19 (004)/2015 Content adjustment and specification of the document "Directive about Identification and Removal of Sensitive Information in Documents to be Made Available to Public". Elaboration of documentation of the pre-operation safety report MO34 with regard to identification of sensitive information, Doc. Ing. Jaroslav Sivák, CSc., MBA, Ing. Dušan Pivko, Ing. Radoslav Kaplan, elaborated in line with the Contract for Work No. 19/2015 concluded on 1 June 2015.

6. Act No. 215/2004 on Protection of Classified Information and on Change and Amendment to Certain Acts as amended.

7. The Registry Order and Registry Plan of the Nuclear Regulatory Authority of SR.

Article 8
Cancellation Provision

Directive about Identification and Removal of Sensitive Information in Documentation to be Made Available to Public S 330 006:14, No. 2290/2014 dated 7 April 2014 is being cancelled.

Article 9
Used Abbreviations

SeSy	–	Safety security system
ES	–	Elementary system
PP	–	Physical protection
HW	–	Hardware
PSA	–	Probabilistic Analysis
I&C	–	Instrumentation and control systems
SW	–	Software

Article 10
Annexes

Annex No.1: Flow Chart
Annex No. 2: Analysis of Indicators and Arguments
Annex No. 3: Analysis of Risks and Sensitive Information Catalogue
Annex No. 4: Division of arguments into three groups and several categories
Annex No. 5: Reduction of Categories and Groups
Annex No. 6: Reduced Argumentation Lines