Incident management procedure
for Licensees processing data using the wwWareshop System

General terms

The Information Security Incident Management Procedure is designed to ensure the operational continuity of Licensee's business and to limit the impact of breaches of security of information assets (hereinafter also referred to as assets), including security of personal data processing, on the Licensee's business.

Definitions

Security of information (also: Security **information**) - is a set of regulations which should be followed while designing and using systems and applications used for information processing in order to ensure that under all circumstances access to the information is consistent with the objectives.

Information security incident[1] - is an event that results or may result in a breach of the security of information assets (resources) due to confidentiality, availability, and integrity of information.

Data integrity - means the property of ensuring that personal data is not modified or destroyed in an unauthorized manner;

[1] „An information security **incident** is defined as an event or sequence of events (comprising the realization of a risk) that causes, or may cause, an undesirable change in significant values of information quality criteria.
The sources of incidents are therefore realized risks".
„Incident means something dynamic, something that is happening right now (known as an ongoing incident) or has happened at some point in the past, resulting in some change (e.g., in the state of information resource protection)".
Krzysztof Liderman „Security information", Scientific Publishing PWN, Warsaw 2017, p. 50).

Licensee - business entity using the wwWareshop system license (hereinafter also referred to as **"System")** provided by Licensor, being the personal data administrator **("Personal Data Controller")** of Users.

Information security breach (including personal data breach) - means a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to information, including personal data transmitted, stored or otherwise processed.

Vulnerability - "Vulnerabilities are flaws or gaps in an organization's physical structure, hardware and software, management and administration, work organization, procedures, staffing, and personnel that can be exploited by risks to cause damage to an organization's[2] information system or operations" .

Processor - Licensor of the wwWareShop system, i.e. NAVIGAL Limited Liability Company with its registered office in Kraków, ul. Podole 60, postal code 30-394, entered in the Register of Entrepreneurs of the National Court Register under the number KRS 0000324788, whose registration documentation is kept by the District Court for Kraków-Śródmieście in Kraków, 11th Commercial Division of the National Court Register, NIP: 676-240-62-06, REGON: 121009007, with share capital of 100.000,00 PLN.

Data confidentiality - means the property of ensuring that data is not made available to unauthorized persons or entities.

Data accountability - means the property of ensuring that the actions of a person or entity can be uniquely attributed only to that person or entity.

Website Service - an online system, e.g. Amazon, integrated with the System and transferring registered Users' data to it.

Erasure od data - means the destruction of personal data or its modification in such a way that the identity of the data subject cannot be established.

[2] Krzysztof Liderman „Security information", Scientific Publishing PWN, Warsaw 2017, p. 29.

User - a user of Online Services, such as Amazon, that is individuals and legal entities represented by individuals, whose data is submitted to the Online Service.

Security[3] in the System - means the implementation and operation of technical and organizational measures to protect data against unauthorized processing.

Risk (to information security) - is a tangible and/or intangible factor that may cause an undesirable change in the required values of relevant information quality criteria[4], that is, the potential for an Incident to occur.

Resources (assets[5]) - "Under this term should be understood:

- information assets (databases and data files, contacts and contracts, system documents, research information, user manuals, training materials, operational and support procedures, business continuity plans, recovery plans, audit trails, and archived information)

- software assets (applications, system software, development tools, etc.)

- physical assets (computer hardware, communication devices, removable media and other equipment, and office furniture)

- infrastructure resources (heating, lighting, power, air conditioning)[6]" .

---

[3] „**Security devices** are:
- - physical (e.g., safe, remote control, building partition),
- - technical (e.g. alarm system, fire protection system),
- - Personal (e.g. security guards),
- - Software (e.g. anti-virus software)

and the organizational actions (e.g., training) used to prevent risks from exploiting the vulnerability". (Krzysztof Liderman „Security information", Scientific Publishing PWN, Warsaw 2017, p. 41)

[4] Krzysztof Liderman „Security information", Scientific Publishing PWN, Warsaw 2017, p. 23.

[5] „In contrast, ISO/TEC 270xx uses the term asset, defined as follows:
1) **Assets** - anything that has value to the organization; there are many types of assets, including:
a) information assets;
b) software, such as a computer program;
c) physical, such as a computer;
d) services;
e) personnel and their qualifications, skills and experience;
f) intangible assets such as reputation and image;
2) ***Information assets - knowledge or data that has value to the organization***".
(Krzysztof Liderman „Security information", Scientific Publishing PWN, Warsaw 2017, p. 31).

[6] Op. cit., p. 31.

Incident Management - "is the systematic application of policy, procedures and practice to the tasks of: detecting and recording incidents, analysing and classifying incidents, minimising the negative effects of incidents, determining and performing preventive actions. Incident management also means that the quality of performance of tasks listed in the definition is subject to evaluation, and activities performed within the framework of these tasks should constitute the so-called Deming cycle"[7] - i.e. be subject to the principle of continuous improvement.

General and specific scope of the information security incident management procedure

The Information Security Incident Management Procedure applies to the Licensee's headquarters, branches and offices. The procedure also applies to external entities (including the Processor) that have been permitted to process data that are Licensee's information resources.

Reporting of information security incidents

1. Breaches of security of Licensee's information resources, including security of personal data processing may be reported by Users, Licensee's employees and collaborators, and external entities. The reporter is responsible for describing the Incident in a comprehensive manner appropriate to his or her knowledge and skill. Incident reports must be submitted to Licensee by telephone at _____ and confirmed electronically at: _____
2. The application must include the following information:

    - name and surname of the submitter,
    - optionally, the name of an outside entity,
    - the location and date of the Incident,
    - a description of the Incident in a comprehensive manner appropriate to the reporter's knowledge and skill.

3. Failure by a reporter to correctly identify an Incident shall not be a reason for not reporting. A person who has knowledge of the possibility of an Incident or an existing

[7] Op. cit., p. 51.

Incident cannot decide for himself or herself whether an incident is or may be a Breach and should, regardless of his or her judgment, report the incident to Licensee.

4. Any person who has knowledge of an Incident that has occurred or may occur shall report it to Licensee as soon as possible, and if it appears that a Breach may have occurred or may occur, report it without undue delay.

Taking action on reported information security incidents

1. A report of an incident is registered by Licensee in the Information Security Incident Log. The person reporting an Incident should secure evidence (e.g., screenshots, photographs of unsecured material containing personal information) and, if possible, secure or remove access to unsecured material containing personal information, etc.
2. Actions related to the handling of a report of a suspected Incident shall first address the identification and classification of the report as an Incident. If a report is classified as an Information Security Incident, an assessment of its significance is made. The above actions are performed by _____ in consultation with designated _____ employees.
3. The following factors shall be considered in assessing the materiality of an incident:
    a. the damage incurred as a result of the Incident;
    b. the effect of the Incident on System operations;
    c. the effect of the Incident on Licensee's business continuity;
    d. the cost of remedying the effects of the Incident;
    e. the estimated time to remedy the effects of the Incident;
    f. an estimate of the resources necessary to restore continued operation of the System
4. The classification of a report of an incident as a "false alarm" terminates the proceedings, of which Licensee will inform the reporter.
5. If an incident is classified as an Information Security Incident, Licensee shall take protective and corrective action to remedy the damage caused by the incident.
6. If intentional acts are found, and the perpetrator of an Information Security Incident is identified, Licensee, if the perpetrator is a subordinate of Licensee, shall decide whether to impose disciplinary consequences, if any, on the perpetrator of the Incident. At the

same time, depending on the severity of the Incident or whether it qualifies as a Breach, law enforcement authorities may be notified.

7. The above actions are reported in the Information Security Incident Log.

Taking action on reported security incidents of personal data processing

1. In the case of a personal data breach, the provisions of Articles 33-34 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - RODO, Official Journal of the EU L 119 of 5 April 2016).
2. A report of an Incident shall be recorded by Licensee in the Incident Log and marked as data protection related..
3. The person reporting the Incident shall, to the extent possible, secure evidence (e.g., screenshot, take photographs of unsecured materials containing personal information) and, to the extent possible, secure or remove access to unsecured materials containing personal information, etc. Report handling activities first relate to the recognition and qualification of the report. In case when the notification is qualified as a Security Incident of personal data processing, an assessment of its relevance is carried out. .
4. The following factors shall be considered in assessing the materiality of an Incident:
    1) the character of the personal data breach;
    2) the categories and approximate number of data subjects;
    3) the categories and approximate number of personal information entries/records affected by the Incident;
    4) the possible consequences if a Data Breach has occurred;
    5) the impact of the Incident on Licensee's business continuity;
    6) the costs of removing the consequences of the Incident;
    7) the estimated time to remedy the effects of the Incident;
5. Classification of an incident report as a "false alarm" ends the investigation and the DPO informs the reporter.

6. Classification of an Information Security Incident as an Information Security Breach involving personal information initiates the procedure to make a notification:

    - supervisory authority, within the statutory period, i.e. up to 72 hours after Licensee becomes aware of the Breach;
    - and, if it is a Personal Data Breach that results in a risk of violation of the rights or freedoms of natural persons, the Licensee shall notify the data subjects without undue delay;

    and preparing the appropriate documentation.

7. Licensee shall also take precautionary and corrective action to remedy any effects resulting from an Incident as well as remedial action to prevent future occurrences of similar Incidents.
8. If notice to data subjects would require disproportionate effort, the Licensor shall prepare a public communication or select another appropriate means by which notice will be provided to such data subjects.
9. If an intentional act is detected and the perpetrator of a Personal Data Security Incident is identified, Licensee, if the perpetrator is a subordinate of Licensee, shall decide whether to impose disciplinary consequences, if any, on the perpetrator of the Incident. At the same time, depending on the severity of the Incident or whether it qualifies as a Breach, law enforcement authorities may be notified.
10. The above actions shall be reported in the Information Security Incident Log and marked as involving the processing of personal data.