# 1 OBJECTIVE

The objective of the document is to define the obligations and responsibilities of the Budimex’s Supplier (and its employees) in the protection of Budimex information assets, to which the Supplier will have access and which it will process in the course of providing its services.

# 2 SCOPE

This document constitutes the Information Systems Security Policy for Budimex SA’s Suppliers, hereinafter referred to as the "Policy".

The provisions contained below regulate two basic areas of information security:

* Provision of services by the Supplier using IT systems entrusted by Budimex and/or IT systems connected to Budimex's infrastructure
* Provision of services by the Supplier using its own IT systems, but processing information owned or for which Budimex is responsible (e.g. personal data of Budimex employees).

# 3 RESPONSIBILITY

Budimex S.A. makes every effort to ensure the effective and safe functioning of the company in order to best meet the needs of the Company's customers, shareholders and employees. A manifestation of special diligence on the part of the management of Budimex S.A. is the minimisation of operational risk, among others, by ensuring an appropriate level of security of the processed information assets. To this end, the management of Budimex S.A. decided to implement the rules on information security.

This document is an expression of Budimex's intention to ensure the security of information assets, resulting from the adopted Information Security Policy, of assets made available and processed by Budimex's Suppliers.

# 4 DEFINITIONS

**Information assets** – information and systems, infrastructure, devices and software used to process information.

**Information security** – ensuring the confidentiality, integrity and availability of IT assets.

**Personal data** – any information relating to an identified or identifiable natural person, directly or indirectly.

**Security incident** – an undesirable event or series of events that creates a significant probability of disrupting business operations and may have a negative impact on the security of information assets.

**Information** - any information, regardless of its form, i.e. in electronic form, on paper, transmitted verbally.

**Classified information** – a term defined in the Act of 5 August 2010 on the protection of classified information. It means information that requires protection against unauthorized disclosure as constituting a state or professional secret, regardless of the form and manner of its expression.

**Information processing** - any action performed on information, such as creating, collecting, recording, storing, reading, changing, sharing, deleting, etc.

User – anyone who has access to Budimex's information assets – users are employees, temporary employees, consultants, apprentices, customers, etc.

# 5 PROCEDURE DESCRIPTION - GENERAL PRINCIPLES

## 5.1 Compliance with the Policy

5.1.1 The Policy is part of the rules and procedures governing the relationship between the Parties. The policy is subject to periodic review. Compliance with the Policy is a condition for the provision of services to Budimex.

## 5.2 Compliance with the law

5.2.1 The Parties must comply with the law and regulations relating to Information Technology.

5.2.2 The use of Information Systems resources resulting in the infringement of intellectual property rights is prohibited.

5.2.3 Installing software or saving any other materials in the IT System entrusted by Budimex, which have not been obtained in a way that authorizes Budimex to use them, is contrary to the Policy.

**5.3 Proprietary Rights and Protection of Information Stored in digital form.**

5.3.1 Data and information stored, processed and/or transferred through the IT Systems belonging to Budimex are under constant control. The control includes methods such as: interception, monitoring, entry in the event log and inspection. The purpose of the constant control is to protect the interests of Budimex and the Supplier.

5.3.2 Data and information are the property of Budimex or the Supplier and must be treated like any other company property.

5.3.3 Data and information concerning Budimex, stored on any media or in IT Systems, must not be deleted without authorisation and should be deleted/destroyed only with the consent and in a manner agreed with the data owner.

5.3.4 The data and information entrusted to the Supplier or generated by the Supplier in the course of providing services to Budimex and those under the control of the Supplier must be adequately protected by the Supplier against destruction, damage and unauthorised access using available means.

5.3.5 The Supplier must at all times apply appropriate protection mechanisms appropriate for the systems under its control and for the data/information contained therein. The supplier is fully responsible for creating regular backup copies of Budimex data placed on mobile computer equipment. Data and information should be stored on portable computers only in the minimum amount and only for the time necessary to perform the scope of services provided. Whenever possible, data should be stored on network drives.

5.3.6 Portable computer equipment containing material and/or confidential data and information concerning Budimex must at all times be equipped with technologies approved by the Parties to block unauthorised access.

5.3.7 Without the written consent of Budimex, data belonging to Budimex may not be processed or stored on equipment not owned by Budimex (e.g. on home computers).

5.3.8 The period and method of storing electronic data in the IT System must be in accordance with the assumptions adopted for a given system (document retention).

5.3.9 Equipment which has not been approved by Budimex cannot be connected to the Budimex IT System. Connecting business or private mobile phones to Budimex IT Systems is prohibited.

5.3.10 You may not transmit secret or confidential information via Internet. Relevant information (not secret and not confidential) received or sent over the Internet must be encrypted in accordance with the recommendations of the applicable Security Policy.

# 6 DESCRIPTION OF THE PROCEDURE - RULES CONCERNING THE SYSTEMS MADE AVAILABLE TO THE SUPPLIER BY BUDIMEX

## 6.1 Use of information technology for business purposes

6.1.1 The Supplier's employees, who are users of IT systems provided by Budimex, may occasionally use the said resources for private purposes. This type of use must not interfere with the performance of official duties and be contrary to Budimex's interest.

6.1.2 The Supplier may not use the resources of the IT Systems provided by Budimex for remunerated work for an entity other than Budimex.

**6.2 Control of access to information from electronic sources.**

6.2.1 Control of access to information stored in Budimex IT Systems is mandatory. For each System, Users are granted access authorization to the extent necessary to perform their work.

6.2.2 Access is controlled by means of individual identifiers and passwords, which clearly identify the User in the IT System and protect against unauthorized access.

6.2.3 Passwords are created in accordance with specific rules regarding their length, construction and frequency of changes.

6.2.4 Passwords must be kept confidential and must not be disclosed to any other person. In the event that the User performing the Supplier's obligations hands over the password to another person, the Supplier will remain fully responsible for the integrity and confidentiality of the information entrusted to it. Password protection is in the interest of both Budimex and the Supplier.

6.2.5. The User whose ID and password have been used to gain unauthorized access to the Information System will be considered as the person who has used the resources of this System in an unauthorized manner.

6.2.6. If you leave your work place for a while, lock the computer (e.g. in Windows use the CTRL-ALT-DEL + ENTER keys) to prevent unauthorized use of the computer.

6.2.7 In the case of adding new Users to the IT System, Budimex's consent is required.

6.2.8 Budimex will change the User's password only on the basis of the request of an authorised person, without disclosing the previous password.

6.2.9 It is forbidden to use IT Systems owned by Budimex or third parties without the consent of the person who is authorised to issue such permits.

## 6.3 Protection of shared resources of IT Systems

6.3.1 The Supplier may not modify devices belonging to Budimex, e.g. by installing computer components, software or in any other way without the written authorisation of the Budimex employee responsible for it.

6.3.2 The Supplier should constantly take care of the Budimex equipment entrusted to him, and in particular take care of protection against theft, prevent damage during transport or handling, properly store at the right temperature and not expose it to magnetic fields or bad weather conditions.

6.3.3 Particular care should be taken when handling materials on exchangeable media (e.g. CD-ROMs, etc.) which have been created or used outside the Budimex IT System. Media from a dubious or unknown source cannot be used on equipment owned by Budimex. All such materials should be scanned with an antivirus program and/or tested by the Budimex IT Office before use.

6.3.4 Any software installations on Budimex computers are carried out by Budimex. Only with the written consent of Budimex can the installation of legal software for business use by persons who are not Budimex employees be carried out.

6.3.5 Installation and/or use of private software/files on IT equipment entrusted by Budimex is prohibited.

6.3.6 The latest version of the antivirus software provided by Budimex must always be present and active on the computer equipment entrusted by Budimex. The instructions provided by Budimex regarding virus prevention and possible elimination of viruses that have penetrated the Budimex IT System must be followed. If an incorrect operation of the antivirus program is noticed, the User must immediately report this fact to the Budimex IT Office.

6.3.7 Any identified cases of threat, breach and weakening of the security of IT Systems or the operation of software unauthorised by Budimex (security incidents) must be immediately reported to the Budimex IT Office.

## 6.4 Sending Messages by electronic means

6.4.1 Budimex's corporate electronic mail, which may be made available to users for whom the Supplier is responsible, is an official mean of communication in Budimex and is treated as business mail.

6.4.2 The User, for whom the Supplier is responsible, may not present private opinions and judgments as the position of Budimex when sending messages by electronic means.

6.4.3 Only electronic message exchange systems approved by Budimex may be used on computers entrusted by Budimex.

6.4.4 On computers entrusted by Budimex, external services provided via Internet (e.g. Hotmail, Yahoo, WP, ONET, chat and instant messengers, etc.) may not be used to send or receive messages.

6.4.5 In order to prevent the operation of malicious software (e.g. viruses) that may get into the Budimex IT System, it is necessary to immediately delete any unexpected mail with attachments from an unknown sender. Attachments in such a message cannot be opened.

6.4.6 The distribution of e-mails in Budimex's corporate e-mail system must be limited only to persons who should know their content or to persons directly related to the content of the message. Distribution lists should not be used except when all recipients meet the above criteria.

6.4.7 In the Budimex corporate e-mail system, it is necessary to avoid sending messages with large attachments to a large group of people via distribution lists. You should use the compression software provided by Budimex to limit the size of large attachments and/or send several messages.

6.4.8 The size of the entrusted Budimex corporate mailbox is limited. The User, for whom the Provider is responsible, is obliged to regularly delete outdated messages.

## 6.5 Internet

6.5.1 In order to provide the services covered by the agreement, it may be necessary for Budimex to provide the Supplier with access to the Internet. Such access will be subject to the restrictions of the Information Security Policy of Budimex SA.

Access to the Internet from the devices and/or infrastructure made available by Budimex is permitted only through solutions provided and approved by Budimex.

6.5.2 Under no circumstances may the User, for whom the Supplier is responsible, connect the equipment entrusted to him to the Internet or other networks via cables, dialup modems or wirelessly without the safeguards required by the applicable Information Security Policy of Budimex SA. Each connection of computer equipment entrusted by Budimex to a computer network not belonging to the Budimex Group must be individually approved by Budimex.

6.5.3 Budimex reserves the right to monitor all types of Internet connections involving devices connected to Budimex IT Systems and to block access to services and websites that are considered to be inconsistent with the Information Security Policy of Budimex SA.

6.5.4 The User, for whom the Supplier is responsible, may not:

* attempt to bypass security, access control or content filtering mechanisms located at the gateway to the Internet;
* deliberately disrupt the functioning of the network, e.g. by sending computer viruses, using hacking practices and sending large amounts of data blocking the network and hindering the work of other users;
* disclose or publish secret or proprietary company information via internet, such as: financial information, new ideas or concepts related to the company, marketing strategies and plans, databases and the information contained therein, customer lists, software source codes, computer/network access codes and business relationships, etc;
* use internet, e-mail or other tools in order to create legal or contractual obligations without the required authorisation of the Management Board of Budimex;
* use resources in another improper manner specified by Budimex.

## 6.6 Inappropriate materials

6.6.1 The Supplier may not use the computer equipment, devices and rooms provided by Budimex to view, process, create and/or distribute materials among employees or anyone outside Budimex that include content:

* related to discrimination (racial or any other),
* harassment (sexual or any other),
* threatening,
* obscene,
* pornographic,
* defamatory,
* illegal

6.6.2 The Provider shall immediately destroy/remove the materials referred to in clause 6.6.1 received from anyone and shall send a request to the sender to cease such practices in the future. The IT Systems Security Manager of Budimex SA should also be immediately informed of the details of the incident, along with the sender's email address, subject and actions taken.

# 7 DESCRIPTION OF THE PROCEDURE - RULES CONCERNING IT SYSTEMS OF THE SERVICE SUPPLIER FOR BUDIMEX

If the Supplier uses its IT system not owned by Budimex and not connected to Budimex's infrastructure to provide services, the following requirements are the minimum for such a system to be allowed to provide services:

7.1 All software (Operating System and applications) installed and used in accordance with the law and license terms

7.2 Each operating system and application must be verified on an ongoing basis for security patch updates (frequency minimum 1x per month)

7.3 A system that has any possibility of interaction with the outside world (computer network, CD-ROM/DVD-ROM drive, USB, disk drive) must necessarily have up-to-date (with a frequency of updates of at least 24 hours) and working antivirus software. For Windows-based systems, the list of available providers - http://windows.microsoft.com/enUS/windows/antivirus-partners#AVtabs=win7

7.4 The system must have a properly updated and regularly synchronized time (in the case of systems with network access, the use of a time server; in the case of off-line systems, documented time synchronization at least 1 x month).

7.5 The system must have working and periodically verified (restoration tests at least once a year) software that makes data backups.

7.6 The entire environment used to provide services to Budimex must have appropriate logical and environmental protection – emergency power supply and protection against unauthorised physical and unauthorised logical access.

7.7 Operating personnel trained in the use of the system.

7.8 Where possible, multi-factor authentication (MFA) must be used when accessing information systems.

7.9 Particular care should be taken when using an external medium (e.g. a USB disk/pendrive) for data processing of Budimex SA, the data on the medium must be protected against loss and access by third parties (e.g. encrypted by a method generally accepted as safe).

1. **DOCUMENTED INFORMATION**

8.1 Report on the review of organizational and technical security measures of the Supplier

# 9. APPENDIXES AND TEMPLATES

NONE

Last updated: 2017-02-07