DATA SECURITY POLICY OF THE INFORMATIC SYSTEM

A. General info

Need for "data security policy" *
With the extensions of the computer system, most of the operations carried out by the hired personnel are carried out by computer (orders, electronic auctions, internal and external communication, management, accounting, etc.). At the same time, the risks are increased due to the high volume of data, Internet access possibilities, computer viruses, software problems and, last but not least, the inappropriate use of software or hardware.
Therefore, the staff has an essential role in preventing such incidents.
Examples of problems that may arise if the computer system loses its integrity:

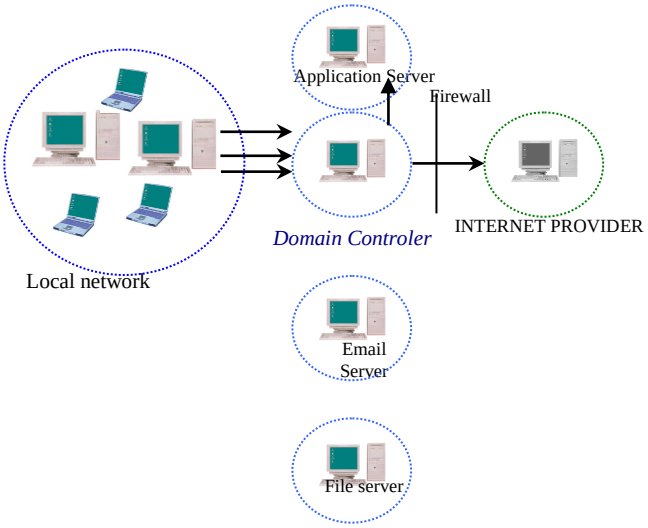
- partial / total blocking of the activity (for a person or group of people)
- data loss (time spent on restoring databases)
- Increase processing time (delays)
- calculation errors (wrong decisions)
- loss of confidentiality

This policy applies to all members of SofMedica Group of Companies, taking into account similar regulations used in other national and international companies.

It is very important for all staff to know and understand this document. (If you do not understand please contact your IT manager for details).

The update for this document will be made at any system's (significant) change.

About the Information System
For system maintenance, the system administrator performs periodic configuration, modification, update and testing with special software to check the security level of the local computer network. Also analyzed are a series of reports generated by specialized software: traffic (customer <> internet), antivirus reports, server logs, etc.
How to connect to the Internet (informative) is shown in the following figure:
:



B. Software

Antivirus
Program (software) designed to protect against computer viruses *
Bitdefender Antivirus is used for network security.

Update antivirus = automatic
- Antivirus application update is automatically done. Report the system administrator if you notice problems with this software (antivirus not running - alert message, virus detected, etc.)

Antivirus scanning
Antivirus scanning should be done whenever an external data medium is used.

Alerts = IT responsible
- When there are some risk factors in the network or the Internet, staff will be informed as quickly as possible by email or directly

---

*** Types of unwanted software (malware)**

VIRUS
A program that can "infect" different types of files
TROJAN
It spies on the user's activity, transferring information to the desired destination by the sender.
Keylogger
Write down everything typed so you can capture the user's USERNAME and PASSWORD
This type of software is usually installed with a program that initially looks useful.
WORM
Virus contacted by email. Once installed, he will send copies of his (viruses) to all the contacts he finds
Adware / Spyware
A program that displays unwanted ads or redirects your Internet browser (Internet Explorer) to unwanted pages
SPAM
Advertisements that over time collide the mailbox
Examples: x% discount for ..., free ...., software for ...,
HOAX
Rumors or letters in the chain (like "send away")

ROOTKIT
It's a software tool used by attackers to hide their processes, system files or malicious programs.
DIALER
These are Internet connection programs that do not make a connection to the tariff
Local calls are being made with surcharge.
PSISHING
It is a way of trying to get access to bank accounts or a whole series of other information, usually pretending to restore the lost database or updating the existing one.
SOCIAL ENGINEERING
This technique is based on the fact that employees provide information on the phone if asked or if they are under pressure.

Local network
Connecting to a computer's local computer network is only done by the IT support

Connecting a guest to the local network or telephone is only done with the consent of the Managing Director or another department manager, by the IT manager.

Email - Actions

Message from an unknown source (possibly VIRUS) = deletion
Never open an email coming from an unknown source. By breaking an email, your computer can be corrupted.
Deletion is recommended.

Unannounced attachment (possibly VIRUS) = not open
Never open an attachment unless you wait for it (worms have the ability to attach themselves to email).
Examples of maximum risk files: exe, bat, com, scr, vbs, pif ...

Unsolicited email (SPAM) = ignore / not respond
It never answers unsolicited offers (SPAMs) no matter how tempting they are (discounts, new products, etc.).
This type of offer is banned by law, but it is still widespread.

Chain Email (HOAX or CHAIN LETTER) = stop
We often receive messages that we announce (we can help someone, we can win a prize, we are notified of an event) by forwarding a message. These messages are always phrases (HOAX) and should not be forwarded.
Danger: loss of credibility

Transmission of confidential data = forbidden
It is forbidden to send by email the data of very high importance or ISO documents.
They will be stored on the server in locations where access rights are granted only to users who are authorized by the company policy.
In the computer, important files will only be encrypted (passwords) on a disk partition that does not share.
Important files can only be sent by email if they are password-protected or secured with a digital certificate.

Large Files> 10mb = Contact the IT Support
For larger files to be sent / received contact the IT support.

Access to a colleague's email can only be done with the consent of the account holder and the Managing Director.

Email server
Currently, mail server is managed by Rolink with an encrypted connection between locations.

In most cases, the mail server identifies and marks unwanted or dangerous emails by showing in Subject:

{Disarmed} – potentially dangerous links
{Spam} – unwanted messages, ads
{Filename?} Potentially dangerous files

Borowser

Download= forbidden
It is not allowed to download files (programs, music * .mp3, video * .avi, pictures, etc.) from the Internet unless they are for the benefit of SofMedica. There is a risk that they may be infected or large files (to block the connection or reduce the connection speed across the network> "flood").

Chat, Messenger = forbidden
The use of integrated chat systems on some sites is dangerous (these applications can lead to computer malware).
The same can happen with messenger (yahoo messenger, icq, MSN, etc.).

Unknown websites = not recommended (with care)
It is not recommended to visit unknown sites (visit only recommended sites).
These can cause computer viruses due to the existence of certain Internet Explorer security issues ("Exploits").

Personal email addresses (WebMAIL) = not recommended
Reading or opening personal email addresses can lead to computer malware (these messages are not checked by the server antivirus).
Examples: yahoo, hotmail, gmail, aol.

Transmission of personal data = not recommended
It is not recommended to transmit personal data to sites.

Passwords

Important: All employees are required to memorize their own passwords (computer access, email, network resources, files, etc) and are not allowed to communicate them to other persons.

PC
The passwords are to be changed by IT responsible or at request.
At leaving the workplace the PC access must be blocked by pressing the key combination CTRL+Alt+Del and then the key K or combination Window key and L.

The level of complexity of passwords must be high to reduce their detection risk.

Documents
The important MS Office files or archived files *.zip, *.rar must be password protected.

Cards – Internet payments

Before making an online transaction after your card, it is advisable to consult the IT manager for this operation.

Software and files

Install / uninstall programs = forbidden
Installing / uninstalling software, software upgrades, changing properties, settings and system parameters (examples: registry editing, device manager, drivers).

Windows Update = recommended
It is recommended that you update your operating system (Windows) when Microsoft resolves (patches).
Do not turn off your computer while updating because it can damage the Windows operating system!

Sharing = on demand
A directory may be (as needed)
- non shared
- Read Only - (All Users can read)
- Shared Read / Write (Full Access) - Read, Write (for access group members)

It is recommended to share as restrictive as possible with well defined rights!
The shared storage area (Share or Public) is considered unsafe and is temporary storage.

Note: It is recommended to involve staff in ranking resources by importance (databases, documents, email, etc.) whenever changes occur and finding solutions to increase data security for that department through appropriate SHARING policies required for document sharing.

The client program for access to the ERP application is only installed with the department manager's approval on the systems where it is deemed necessary.

C. Hardware

Important:
It is necessary to know the "**Regulations for the use of equipment**"

PC

a. Use
It is forbidden for others to use received goods (PC, phone, printer, etc.)
It is forbidden to leave the work place with equipment without the agreement of the department manager.

After work hours
> it is necessary to close the equipment (printers, monitors, faxes)
> Notebook PCs must be stored in cabinets
> Only devices that have a continuous active role (servers) are left open

b. Troubleshooting
The only person who has the right to open equipment for servicing or upgrading is the IT support
For warranties, call the equipment supplier

Data storage devices CDs/ /Memory Cards/External hard-drives

Data entry = with antivirus scan
Any USB, CD, memory card, or other external data storage device must be pre-checked by the IT officer (antivirus scanner).

Data exit = with the agreement of the department manager
Any information to be broadcast externally on one of the listed media should be done with the agreement or information of the department manager.

Printer
The person who has printed must go to recover their sheets as soon as possible.
Do not print documents with many pages to avoid creating waiting queues when lifting them.

Copier
After multiplying a document, it should not be forgotten in the copier.
If you find a document, it should be handed over to the Administrative Assistant or at reception desk.
Copier access is only allowed to employees.
In special cases the guest is helped by the contact person in the company.

Projector
Reservation (for presentations outside the company) is made by email to the IT Support.

Telephone
Place the correctly the receiver of the landline phone correctly so that it does not remove the machine from work.
If you temporarily move to another office, redirect your personal extension to the new location.

Fax
Never responds to commercial offers arriving without prior request (SPAM)

Entry and exit of documents by fax is registered at the secretariat.
The fax log is done in the Excel table "register fax entries outputs yyyy.xls "

D. IT Support

IT support is outsourced. their obligations are:

- Identifying vulnerabilities and finding ways to prevent incidents
- Call staff intervention in case of unusual manifestations of the equipment used.
- Regularly changing passwords, setting programs where they are used, and communicating them to staff
- Installing and configuring new software versions
- Checking the status of servers
- Windows update check
- Check for antivirus, firewall update
- Surveillance of server services
- Security tester
- Emergency disconnection from the network for compromised systems (quarantine)
- Monitoring of the information system
- Connecting equipment to the network
- Equipment verification (integrity)
- Checking fixed / mobile hard drives
- Checking software used
- Checking email accounts
- Securing / overseeing transactions in an electronic environment

Access in the server room is allowed only to IT specialist