UNIWERSYTECKI SZPITAL KLINICZNY — UNIWERSYTET INFORMACJI

Information Security's Rules

Wieńczysław Bielecki

„The greater our knowledge increases the more our ignorance unfolds!"

J.F. Kennedy

Whoever has the information has the power

This relation has been known since the dawn of time. Without knowledge about citizens, their needs and moods, and without information from the world, no power can be effectively exercised
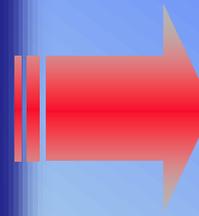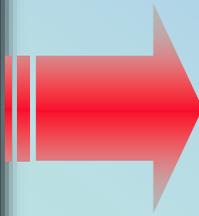
**Information, like any other important organization's assets, is essential to its operation and is of value to it -
so it should be properly protected!**

Classic …
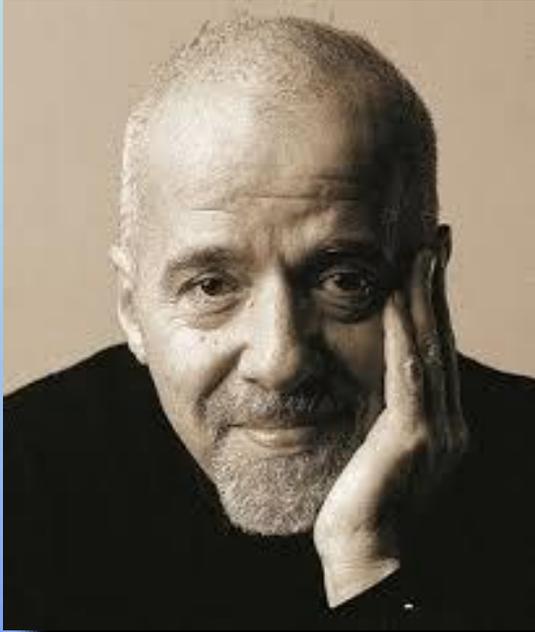
The simple things are also the most extraordinary things.
Paolo Coelho

1

The principle of individual accounts in the IT system

Each employee is obliged to work in IT systems on the accounts assigned to him. It is forbidden to make accounts available to other employees.
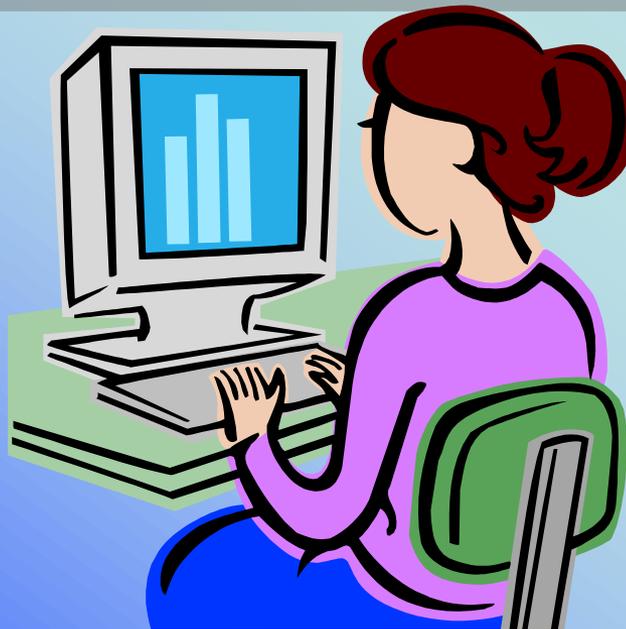
2

The principle of confidentiality of passwords and access codes

Each employee is obliged to maintain confidentiality and not to disclose to unauthorized persons the passwords made available to him. This rule applies in particular to the employee's personal access passwords to IT systems and protected zones.
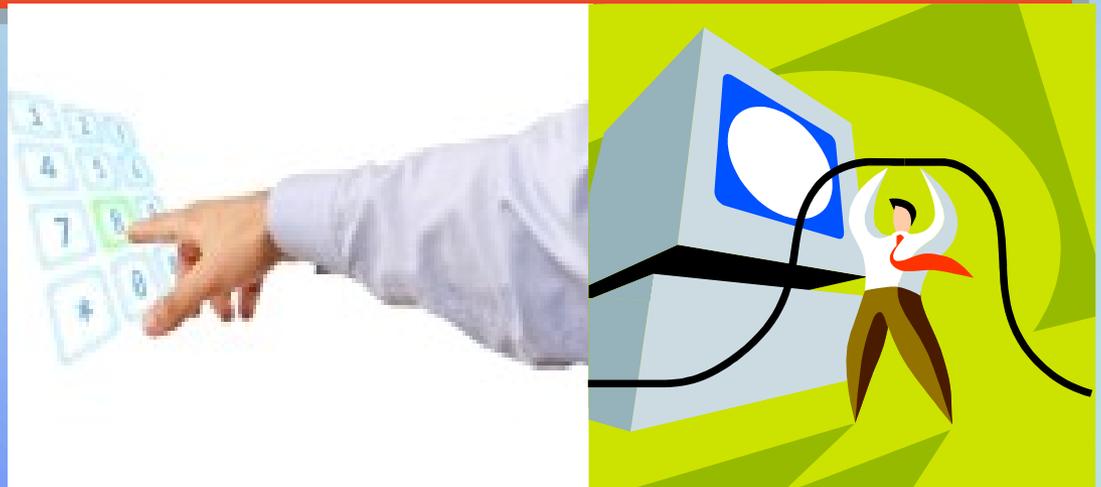
WORST PASSWORDS RANKING

	Password	Last year
1	123456	1 up
2	password	1 down
3	12345678	No change
4	qwerty	1 up
5	abc123	1 down
6	123456789	new
7	111111	2 up
8	1234567	5 up
9	iloveyou	2 up
10	adobe123	new
11	123123	5 up
12	admin	new

3

The principle of a closed room

It is unacceptable to leave an unsecured office room, both during working hours and after its completion, if the authorized person does not stay in it.
The rule does not apply to generally accessible rooms
After the end of the working day, the last person leaving the room is obliged to close all windows and doors and, in accordance with the applicable arrangements, secure the keys to the room.

4 Principle of supervision of documents

After working hours, all documents containing information relevant to the interests of the University's Hospital should be stored in closed cabinets or drawers, protected against access of unauthorized persons.

5 The principle of a clean desk

Avoid leaving documents on your desk unattended. After finishing work, clear the desk of paper documents and other electronic information carriers
(CDs, DVDs, pen-drives, etc.).

The principle of a clean board

After the end of classes, meetings, discussions, etc., you should clear all the materials and clean the boards, take the materials, ...

7 The principle of a clean screen

Each computer must have a screen saver set after entering a password or turning off automatically after a specified period of user inactivity.
Additionally, before leaving the computer switched on unattended, the user should lock it (including the screen saver) or log out of the system in case of a longer absence.

The principle of a clean desktop

Icons for a standard software and business applications as well as shortcuts of folders may appear on the computer desktop, provided that the names of the folders do not contain information about ongoing projects or clients.

Kosz   Panel sterowania   Sieć   Dokumenty   Komputer

The principle of clean printers

Printed information should be collected from printers immediately after printing.
In the event of an unsuccessful attempt to print, the user should contact the service technician responsible for the correct operation of the device.
The employee should delete information from the printer's memory by himself or according to the service technician's instructions.

The principle of a clean trash can

Paper documents, with the exception of promotional, marketing and informational materials, should be destroyed in a way that makes them unreadable (preferably in a shredder), placed in special containers, etc.

11

The principle of responsibility for resources

Each employee is responsible for the resources made available to him (computers, software, systems, accounts, etc.).
These resources are intended solely for business purposes. Using them for private purposes is possible only to a limited extent by internal regulations.
Unauthorized installation of illegal software is strictly prohibited.

12

The principle of necessary knowledge, justified "need-to-know"

"**Need-to-know**" means that information may be made available only to those persons who have a confirmed need to obtain knowledge about or have such information in order to perform their official or professional tasks.

The principle of informed conversation

Not always and everywhere you have to say what you know, but always and everywhere you need to know what, where and to whom ...

Taking data out of the company

We should remember that the employer must agree to take the data outside the workplace, regardless of whether it is data collected on electronic, optical, magnetic media, external drives, portable computers, etc. or in paper form.

Each data transfer will always involve additional risk, such as loss or theft.

15   e-mail

We only use company e-mail accounts for business contacts, e.g. *jan.kowalski@umw.edu.pl*

We do not use private email at work, …@gmail.com, …@onet.pl, …@wp.pl, itp..

Speeches, conferences, articles, publications, etc.

All public appearances (presentations, lectures) presented at various types of trainings, conferences, briefings should be agreed in advance with the appropriate supervisor (vertical director).

Using the resources of USK when writing research papers, publications, articles should be done with the consent of the Director of USK.

They apply to the above:
➤ Work regulations …
➤ Code of ethical conduct for employees…
➤ Information Security Policy …

…

LET'S PROTECT

INFORMATION

LET'S PROTECT

PRIVACY

THANK YOU FOR YOUR ATTENTION

GOOD PRACTICES - INFORMATION SECURITY - GOOD PRACTICES - INFORMATION SECURITY -

Wieńczysław BIELECKI