United Nations
Educational, Scientific and
Cultural Organization

Knowledge Management and Information Systems

ICT Security

What is Information Security?

Information Security is the ongoing process of exercising due care and diligence to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It's main objective is maintaining the information under the principles of **Confidentiality**, **Integrity**, and **Availability**.

- **Confidentiality** is the term used to prevent the disclosure of information to unauthorized parties.
- I**ntegrity** means that the information is maintained without modifications.
- In order to serve its purpose, the information needs to be **available** whenever it is needed.

UNESCO's information systems and networks are an integral part of the Organization and are fundamental to its continued success. Substantial human resources and financial investments go into maintaining them and ensuring that they continue to evolve in order to meet the changing requirements of the Organization, both at HQ and in the field.

Inadequate information security and continuity is a substantial business risk that threatens not only important organizational assets, but also business processes critical to the continued operations of the Organization.

Information security is therefore vital. However, a good IT security system should aim to strike the right balance between the necessary security-related restrictions and users' comfort.

Information Security is intended to support the protection, control, and management of the Organization's information assets, which includes data and information that is stored in databases or on computers, stored in applications, transmitted across the internal and public networks, and stored on removable media.

Passwords

Passwords are the entry point to UNESCO's information systems and the front line of protection for user accounts. They ensure that the systems remain secure and the information within remains authentic and available.

Passwords of user accounts must meet the following minimum complexity requirements:

- At least 8 characters long;
- Do not contain the user's network Logon name, first name or last name
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Numerical characters (0 through 9)
  - Non-alphabetic characters (for example !, *, -,%,@)

System passwords shall be changed every 120 days.

Beside the minimum requirements, passwords shall not be based on personal information or single common words.

User names and passwords are for individual use. Sharing login name and password with other personnel, or accessing UNESCO systems using the login and password of another user is strictly forbidden and can lead to disciplinary action of the involved personnel.

UNESCO, your bank, or other service provider will never ask you for your password.

General Password Tips

1) Mix and Match

- Mixing upper case and lower case characters increase significantly the amount of time it takes to crack a password
- Use the space bar to separate words. Multi-word phrases are more secure passwords than a single 8-12 character password
- Use numbers and symbols where it makes sense. A password with many numbers and symbols replacing letters often doesn't make it more complex.

2) Use multiple passwords

Try to never use the same password in different places. You should at least have a different password for your banking, another for your email, and another for social networks. Diversify them for added security, especially the social network ones.

3) Avoid:

- Using sequential keyboard characters or numbers (1234, azerty, dfghj)
- Repeating characters (441122,ddffgg)
- Reusing recently used passwords

Viruses

A virus is a small program that causes serious damage to computers. Viruses can be found in files which are downloaded from websites or emails. They can also be transmitted through removable storage media (portable hard drives, usb flash drives, CDs). When an infected file is opened, the virus will be launched and can spread through the computer or network causing damage to data or other systems.

You can avoid virus infections by:

- Never opening attachments from unsolicited or suspicious email messages
- Only downloading files from sources you trust
- Running a virus scan on any removable storage media that has been connected in other computers outside of the Organization before opening any document
- Staying away from gamble, free games, and pirated software websites.

Social Engineering

Social Engineering is the act of manipulating people in order to obtain confidential information from them. It is done in such way that the user releases the information without realizing that it will be misused. This can be done either via telephone, email, written form, or in a face-to-face conversation.

Never give away your username, password, or any other sensitive information to anyone. No one is authorized to ask you for your password, and you are not authorized to give it away.

Phishing

"Phishing" is the act of attempting to obtain confidential or sensitive information by using email messages and websites that appear to be legitimate, encouraging the user to provide personal information, credit card numbers, banking details, passwords, access codes, among other information that the user would otherwise not release.

Phishing messages and websites can impersonate our own Organization or any other UN agency, financial institutions, and websites in such a way that the user does not realize that he or she is providing information to an illegitimate source.

Five tips to protect you against Phishing attacks:

1) **Know the places where you have a user account.** Ignore emails that come from websites where you are not an active user, including the ones from places where you have done business in the past but not currently.
2) **Be familiar with the typical communications sent by the websites where you have a user account.** This includes the typical content and visual style of the email, the sender address, and the procedures used to reset a password.
3) **Verify that the Link provided in the emails point to the website concerned.** Phishing links always point to an unknown website**.**
4) **Always ensure you are using a secure connection.** This can be verified by making sure the address starts with HTTPS instead of HTTP and that there are no messages from the web browser notifying that the website is not trusted or has an expired security certificate
5) **Contact Helpdesk.** If you ever consider that an email received is questionable, it probably is. Always report any suspicious emails, so other users can be informed about potential phising attacks.

Personal Computers

Personal computers must not be connected to the Local Network without previous authorization from KMI. The use of such equipment on UNESCO's network will be authorized only under special circumstances. However, they can be connected to the Wireless Network (Wifi).

Any equipment authorized to be connected to the network must follow UNESCO's software standards and security policies.

Email Security

E-mail is one of UNESCO's primary business communication means. The authentication and security model used by the corporate e-mail system can guarantee message authenticity and confidentiality within the UNESCO network. Employees must not use the UNESCO e-mail system for purposes that are illegal, unethical or harmful to the Organization.

Email is for individual use, and each user is responsible and accountable for the messages sent, received, and stored using his/her email account. Under special circumstances, email access can be delegated to other users; however, the delegated user must use their credentials in order to access the delegated account. Official and confidential information must be sent via the UNESCO email account and not using a personal email account.

You should always refrain from opening unsolicited email messages. "**Unsolicited**" means that it comes from an unknown sender or a colleague but its subject doesn't relate to the typical daily activities of the Organization.

Mobile Devices

Mobile devices, due to their nature, must be handled with special care and diligence. The same security policies that apply to desktop computers also apply to mobile devices. Additionally, mobile devices must be protected with a password to lock/unlock the device. The password must be at least four characters long, composed of either numeric and/or alphanumeric characters.

Official UNESCO Mobile devices will be automatically locked after 1 hour of inactivity. Should the user exceed ten failed password unlock attempts, the content on the device will be automatically deleted. Users must abide by the Policy on the Use of UNESCO Mobile Telephones. Also, users must immediately report any loss, theft, or damage of mobile devices to
KMI.

To find more about protecting your mobile device, please refer to the mobile devices guide located at https://teams.unesco.org/services/mobile/SitePages/Home.aspx

United Nations
Educational, Scientific and
Cultural Organization

Knowledge Management and Information Systems

Remember

- Always use strong passwords and never use common words. Passwords must be hard to guess but easy to remember.
- Never share your password. No one is authorized to ask you for your password, and you are not authorized to give it away.
- Do not open email attachments from unsolicited or suspicious emails
- Refrain from visiting questionable websites.
- Run a virus scan on any hard drives or USB flash drive that has been connected in a computer outside of UNESCO before opening any documents.
- Pay special attention to any email you receive concerning your personal information, passwords, and other sensitive information. Never provide such information to anyone.
- Report any suspicious email to the Helpdesk
- Refrain from using your personal email to send or receive official messages.
- Keep your inbox confidential and do not provide access to anyone.
- Always lock your computer whenever you leave your desk.
- Lock your mobile device using a password or access code.
- Report any lost or stolen mobile device to KMI.
- Do not connect any portable equipment (Laptops, tablets, and other devices) to the network without previous authorization from KMI.

The IT Security Policy can be found in the Administrative Manual, item 9.3.
Please refer to this policy for more information.

Better safe than sorry!