School Security Plan

INTRODUCTION

The School Security Plan is a document that defines and describes the security standards and procedures for ensuring the confidentiality, integrity and availability (CIA triad) of all information systems and resources in school being them cyber or physical.

It contains a list of rules and advices for a better ensurance of the CIA triad.

This plan is divided in 3 crucial parts:

- Security for teachers.
- Security for auxiliaries.
- Security for students.

All parts together count as one and some of the standards and procedures may repeat in some of them.

PURPOSE

Its purpose is to correct deficiencies, enhance and maintain the IT Security in all possible ways, from incorporating current security programs and developing new ones if necessary, to formalizing responses and reporting procedures for security incidents.

Co-funded by the Erasmus+ Programme of the European Union

Security for Teachers

This first part below is related to every teacher working on the school, regardless of his/her subject area.

RULES

- Use apps and platforms authorized by the Department of Education, if you want to use one which wasn't reviewed by it, ask for a review and if authorized then use it.
- School panel account's password must be changed at least once every month.
- The usage of personal hardware is forbidden during the classes, unless those which were authorized by the school directory.
- The school hardware must be used exclusively for professional purposes, do not use them for personal purposes.
- Warn the tech responsible if anything is wrong with the system or if you notice any irregularities.
- Any changes in software or hardware must be done with the knowledge of the tech responsible.
- The sharing of work accounts is forbidden.
- Every hardware like pen drives or similar must be scanned by the antivirus before the usage.
- Every file received from emails or similar must be scanned by the antivirus before the download.
- Keep the hardware and software clean after the usage.
- The printing of personal documents in the school area is forbidden, unless authorized by the school directory.
- Every information and data used in the workspace must be protected from abuse, improper handling, destruction or loss.
- Any software that is not related to work will be removed without any warning.
- Only connect to the school Wi-Fi when working.

Co-funded by the Erasmus+ Programme of the European Union

ADVICES

- Always be aware of the state of your school panel account and secure it well.
- Secure your own computer if you bring one to the workspace.
- Use the appropriate user when signing in to the computer.
- Always sign out of your session when leaving the computer.
- Don't login to bank accounts in the workspace.
- Don't login to social network accounts in the workspace.
- Avoid opening links/files from unknown sources.
- Avoid using your personal email for school purposes, use an alternative one if the school didn’t give you one of their email host.
- Always clear the browser history when leaving the computer.
- Use strong passwords for educational apps and platforms.
- Avoid saving your login credentials unless using your own computer.
- Avoid writing passwords in front of anyone.
- Teach students about privacy and security.
- Be aware of what your students are doing on their computers, both hardware and software could be damaged without you knowing.
- Avoid using pen drives or similar hardware, use google drive or similar platforms instead.
- Verify the security of the websites, apps or extensions before using them.

Co-funded by the Erasmus+ Programme of the European Union

Security for Auxiliaries

This second part below is related to every auxiliary working on the school, regardless their working area.

RULES

- School panel account's password must be changed at least once every month.
- The usage of personal hardware is forbidden during the work, unless in special occasions.
- The school hardware must be used exclusively for professional purposes, do not use them for personal purposes.
- Warn the tech responsible if anything is wrong with the system or if you notice any irregularities.
- Any changes in software or hardware must be done with the knowledge of the tech responsible.
- The sharing of work accounts is forbidden.
- Every hardware like pen drives or similar must be scanned by the antivirus before the usage.
- Every file received from emails or similar must be scanned by the antivirus before the download.
- Keep the hardware and software clean after the usage.
- The printing of personal documents in the school area is forbidden, unless authorized by the school directory.
- Only connect to the school Wi-Fi when working.

Co-funded by the Erasmus+ Programme of the European Union

ADVICES

- Always be aware of the state of your school panel account and secure it well.
- Always sign out of your session when leaving the computer.
- Don't login to bank accounts in the workspace.
- Don't login to social network accounts in the workspace.
- Avoid opening links/files from unknown sources.
- Always clear the browser history when leaving the computer.
- Use strong passwords for accounts related to your work.
- Avoid saving your login credentials.
- Avoid writing passwords in front of anyone.
- Avoid using pen drives or similar hardware.

Co-funded by the Erasmus+ Programme of the European Union

Security for Students

This third part below is related to every student that belongs to the school, regardless what classes is he/she having or what is he/she doing.

RULES

- Only use apps and platforms authorized by your teacher.
- The usage of personal hardware is forbidden during the classes, unless if authorized by your teacher.
- The school computers must be used exclusively for class purposes.
- Warn the responsible teacher if anything is wrong with the system or if you notice any irregularities.
- Any changes in software or hardware must be done with the authorisation of the responsible teacher.
- The sharing of school accounts is forbidden.
- Every hardware like pen drives or similar must be scanned by the antivirus before the usage.
- Every file received from emails or similar must be scanned by the antivirus before the download.
- Keep the hardware and software clean after the usage.
- The sharing of work or project files is forbidden.
- Every information and data used in the workspace must be protected from abuse, improper handling, destruction or loss.
- Students must have their own session on the computer they are using.

Co-funded by the Erasmus+ Programme of the European Union

ADVICES

- Always be aware of the state of your school panel account and secure it well.
- Secure your own computer if you bring one to the class.
- Use the appropriate user when signing in to the computer.
- Always sign out of your session when leaving the computer.
- Don't login to social network accounts in the workspace.
- Avoid opening links/files from unknown sources.
- Always clear the browser history when leaving the computer.
- Use strong passwords for educational apps and platforms.
- Avoid saving your login credentials unless using your own computer.
- Avoid writing passwords in front of anyone.
- Avoid using pen drives or similar hardware, use google drive or similar platforms instead.
- Install security tools before connecting to the school network.
- Write your laptop's serial number in case it ever gets stolen.
- Enable two factor security authentication (2FA), it's always better than one factor.

Co-funded by the Erasmus+ Programme of the European Union