CYBERSEC
EDUCHECK

MANUAL FOR SECONDARY EDUCATION INSTITUTIONS

FACILITATING THE MAINTENANCE OF AN ADEQUATE LEVEL OF INFORMATION SECURITY WITHIN THE SCHOOL AND PROMOTING EDUCATION AND AWARENESS IN THE REALM OF CYBERSECURITY

Prepared by:
Mateusz Pękala

PROJECT NO. 2023-2-PL01-KA210-VET-000176822

Co-funded by the European Union

LEADER: Research Institute Europe | Coventry University

PARTNERS: KREA STOWARZYSZENIE KREATYWNI DLA BIZNESU; EUROPEAN CENTRE FOR CAREER EDUCATION

Contents

ATTACHMENTS

For whom is this intended?

This guide is intended for you if:

You serve as the principal or vice principal of a secondary school, overseeing information security within your institution.

You observe an increasing necessity to implement effective educational initiatives in the realm of cybersecurity for both students and employees.

You aim to formulate technology policies that effectively mitigate cyberbullying, disinformation, and various digital threats.

Are you seeking practical strategies to cultivate cyber awareness within the school environment, engaging both students and staff?

You aspire for your school to serve as a model of exemplary practice in the management of digital security and data protection.

This handbook has been crafted to function as a thorough guide for school principals in establishing a robust framework for cybersecurity education and information security management. It tackles the challenges associated with school administration and seeks to mitigate, among other issues, unethical, ambiguous, and risky behaviors among youth in their use of technology.

What information can you expect to find in the manual?

The handbook offers resources to assist you in effectively executing an information security program within your school.

- **Defining roles and responsibilities – You will acquire the skills to effectively assign information security responsibilities to all personnel, ranging from educators to management.**
- **Establishing Security Policies – You will acquire the skills to implement an Information Security Management System and an Information Security Policy that will guarantee data protection within your school.**
- **Awareness Enhancement Program – Enclosed is a proposal for educational initiatives designed to elevate awareness of cyber threats among students and staff.**

In the appendices of the handbook, you will find document templates. These resources will assist you in tailoring the security policies to the unique characteristics of your school, establishing a robust framework for digital security. Review the handbook and utilize the templates to efficiently oversee information security within your institution.

Defining roles and responsibilities.

In educational institutions where resources are constrained and the primary focus is on delivering the curriculum and attending to students' needs, it is essential to delineate roles and responsibilities regarding information security.
This represents a vital initial step in the development of an Information Security Management System.
Every member of the school community, including teachers, educators, counselors, psychologists, and principals, plays a vital role in cybersecurity. Assigning clear roles and responsibilities guarantees that information security measures are effectively executed at all levels of the institution and that established policies are adhered to.

To streamline this process, please find attached the “Roles and Responsibilities in the ISMS” template (document 02) along with the parent document “Information Security Policy” (document 01).
Both documents will assist you in effectively managing information security within your facility.

Establishing an Information Security Management Framework

The implementation of the Information Security Management System (ISMS) within the school is grounded in established methodologies frequently employed in the business sector, such as adherence to the ISO 27001 security standards.
Although schools encounter distinct challenges compared to businesses, certain solutions—such as information security policies, acceptable use policies for IT resources, and mobile device management—can be effectively tailored to meet the requirements of educational institutions.

The fundamental instrument in this process is the "Information Security Policy" (ISP) template, located in the appendix of the handbook (document 01). It serves as a declaration in which the school pledges to uphold information security.

PBI delineates the objectives that the school aims to accomplish. The document titled "Information Security Principles" (document 03) elaborates on the implementation of PBI in detail. It comprises several sections, including general guidelines, remote work protocols, access control measures, password management, Internet and email usage, and BYOD (Bring Your Own Device) policies. This document establishes the security principles that both teachers and students are required to adhere to, thereby ensuring data protection within the school environment and during remote work.

These policies must be conveyed to students and staff as a component of the Cybersecurity Awareness Program, which is a critical aspect of the school's ISMS.

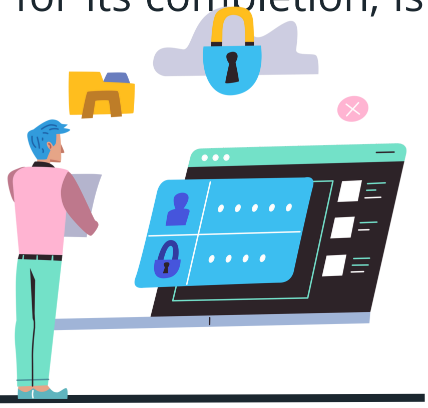
Cybersecurity Awareness Development Program at Educational Institutions

A fundamental component of the Information Security Management System (ISMS) within an educational institution is the establishment of a Training Program designed to cultivate and sustain awareness of cybersecurity. While the primary focus of education is the dissemination of new knowledge, it is equally crucial to consistently remind students of pertinent regulations, including security protocols and the importance of utilizing strong passwords. In this regard, the school should implement mechanisms to ensure ongoing reminders and reinforcement of these guidelines.

It is important to recognize that students do not bear the same responsibilities as adult employees; therefore, the awareness-building program must be tailored to the unique context of the school. This initiative encompasses the entire school community—both staff and students—united in the effort to combat cyber threats.

To accomplish this objective, we propose a template titled "Cybersecurity Awareness Building Program" (document 04). This document necessitates customization to align with the particularities of each institution— not every school has access to resources such as police lectures, external training, or support from parents employed in the IT sector. Nevertheless, if such opportunities are available, it is advisable to incorporate them into the plan.

The template for the “Cybersecurity Awareness Program” (document 04), along with the instructions for its completion, is located in the appendix of the manual.



List of Attachments

1. Information Security Policy (ISP)

A document outlining the fundamental principles and objectives of information security within the educational institution.

Roles and Responsibilities within the ISMS

Document template outlining the responsibilities and tasks of school personnel (teachers, administration, management) in the realm of information security.

3. Principles of Information Security

Regulations governing the utilization of IT resources, mobile devices, and adherence to security policies.

4. Cybersecurity Awareness Enhancement Program

A training program framework for students and employees that fosters education and enhances awareness of cyber threats.

1. Information Security Policy (ISP)

Document Attributes

Name	**Information Security Policy**
Approval and oversight	Headmaster
Review	School Information Security Officer
Inspection frequency	Annually or following any substantial alteration in the process
Storage site	Intranet / designated folder on network drive

Version History

Version	Data	Author	Description of modifications
0.1	01.10.2024	Coventry University	Preparing the design template

Contents

Introduction

The responsibility for information security is shared by all employees, temporary and external workers (contractors), as well as the management of the School.

Students are accountable for adhering to the information security guidelines issued by the School Management and Teachers.
The school implements educational activities designed to safeguard employees, contractors, students, and parents from adverse security incidents that may compromise the confidentiality, integrity, and/or availability of processed information.

The objective of this document is to implement an Information Security Management System (ISMS) at the School, which encompasses the delineation of responsibilities for its operation and the establishment of a framework for defining specific security objectives.
The School Management affirms that information security is a critical component of the School's operations and expresses its unwavering commitment to the implementation and management of the ISMS, including the provision of adequate organizational and financial resources.

Information Security Policy

• Goal

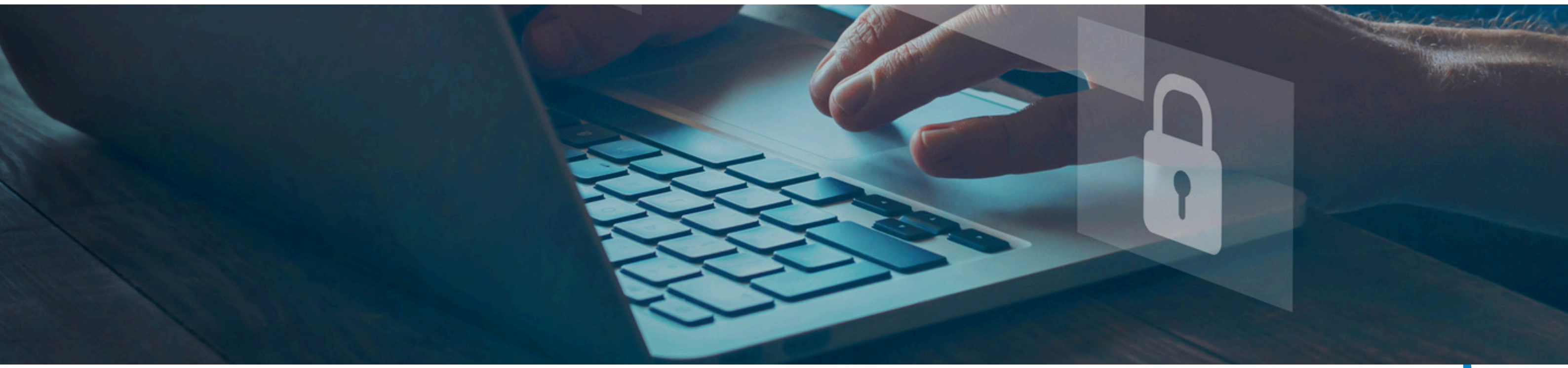
The objective of the ISMS is to guarantee information security in alignment with the recognized needs and expectations of the Management, Employees, Students, Parents, and other stakeholders of the School.

• Endorsed Objectives of the Institution

The ISMS facilitates the following objectives of the Organization:

- Exhibiting the dedication and backing of School Leadership for information security.
- Implementing suitable safeguards in accordance with identified risks.
- Adherence to internal and external obligations.
- Adherence to the stipulations set forth by the School Supervisory Bodies and contractual commitments pertaining to information security.
- Adherence to relevant data privacy regulations, including GDPR stipulations.

This Information Security Policy is reinforced and complemented by additional policies, procedures, and other documentation related to the ISMS and GDPR Policy.



• Scope of the Information Security Management System (ISMS)

This Policy encompasses all processes and information overseen by the School, including cloud services, software, devices, personnel, and facilities.

• Roles and Responsibilities within the ISMS

Considering the necessity to integrate information security processes with the School's ongoing operations, along with operational and reporting responsibilities, the School Management will establish a suitable framework of roles and responsibilities, ensuring the assignment of accountability for the overall functioning of the Information Security Management System.

The School Information Security Officer is tasked with upholding the Information Security Policy, facilitating its objectives, and providing guidance on its execution.

Staff (Teachers, Educators, Pedagogues) will be accountable for executing and enforcing the stipulations of the Information Security Policy and related documents within their respective domains.

Students must be made aware of their responsibilities concerning information security.

2. Roles and Responsibilities within the ISMS

Document Attributes

Name	**Roles and Responsibilities within the ISMS**
Approval and oversight	Headmaster
Review	School Information Security Officer
Inspection frequency	Annually or following any substantial alteration in the process
Storage site	Intranet / designated folder on network drive

Version History

Version	Data	Author	Description of modifications
0.1	01.10.2024	Coventry University	Preparing the design template

Contents

Goal

The document aims to delineate the roles and responsibilities crucial for the efficient functioning of the Information Security Management System (ISMS).

ISMS Roles and Responsibilities

The institution has delineated roles and responsibilities within the Information Security Management System (ISMS).
Roles within the ISMS may be consolidated and executed by the same individuals, depending on the competencies of the School.

- **Headmaster**

The School Principal articulates the vision, facilitates the implementation and functioning of the ISMS, and offers comprehensive guidance, direction, and support for the operation of the Information Security Management System within the School.

The responsibilities of the School Principal encompass:

- Acceptance of the objectives and scope of the Information Security Management System (ISMS), while considering the School's goals and legal obligations.
- Assigning responsibilities and endorsing organizational modifications pertaining to the ISMS,
- Approval of the Information Security Policy.
- Approval of ISMS documentation derived from the Information Security Policy,
- Approval of the acceptable risk threshold, risk analysis outcomes, and risk treatment strategies within the processes encompassed by the ISMS.
- Approval of the budget pertaining to the ISMS.
- Approval of the outcomes of ISMS audits and evaluations,
- Decision-making within the crisis management framework.

- **School Information Security Officer**

The School Information Security Officer oversees the operation of the Information Security Management System (ISMS) and is tasked with developing guidelines and supervising information security protocols.

The responsibilities of the Officer encompass:

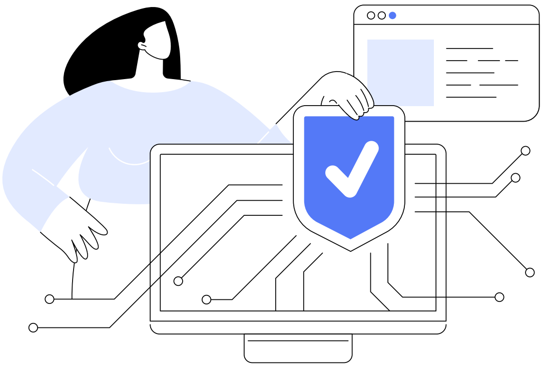
1. Introducing modifications and overseeing the coherence of the ISMS documentation while conducting regular reviews and updates.
2. Enhancing awareness among employees and students regarding information security matters, particularly overseeing the Cybersecurity Awareness Building Program at the School.
3. Implementation and oversight of adherence to information security regulations and mechanisms,
4. Evaluation of the efficacy of implementing requirements stemming from information security regulations.

- **Data Protection Officer (DPO)**

Schools that possess existing documentation regarding personal data protection (GDPR) may reference these provisions without the need to redefine the responsibilities of the Data Protection Officer (DPO). It is essential for the Information Security Management System (ISMS) documentation and the Personal Data Protection Policy to be harmonized. Indeed, adherence to GDPR constitutes one of the primary objectives of the ISMS.

The IOD supports the School staff in all aspects concerning the safeguarding of personal data. The responsibilities of the IOD encompass:

- Advising and informing the School Management and staff regarding their responsibilities under personal data protection legislation,
- Monitoring adherence to all data protection regulations, encompassing audits, awareness initiatives, and training for personnel engaged in processing operations,
- Offering guidance on conducting a DPIA and assessing its effectiveness,
- Serving as a liaison for inquiries from individuals concerning the handling of their personal data and the exercise of their rights,
- Collaboration with data protection authorities and serving as a liaison for these authorities regarding issues related to the processing of personal data.
- Support for activities associated with the maintenance and enhancement of the Information Security Management System (ISMS) in the realm of personal data protection.
- Assistance in identifying protective measures suitable for the volume and extent of personal data processing.
- Assistance for design initiatives related to systems that handle personal data,
- Classification of personal data processing activities based on quantity, type, and purpose of processing.
- Maintaining documentation of personal data processing activities.



- **Teacher/Employee**

All employees with access to the School's information resources, including staff, contractors, interns, and external service providers, are required to:

1. Adherence to the Information Security Policy and the information security principles outlined in other pertinent documents,
2. Adherence to the Personal Data Protection Policy and associated regulations,
3. Reporting information security breaches,
4. Participation in the information security training initiative.

- **Student**

All students who have access to the school's informational resources as pertinent to their courses.
Students are responsible for:

1. Adherence to the Information Security Policy and the information security principles outlined in other pertinent documents,
2. Adherence to the Personal Data Protection Policy and associated regulations,
3. Reporting information security breaches,
4. Participation in the information security training initiative.
5. Adhering to directives from educators and other instructional personnel concerning the utilization of electronic devices and the Internet within the School.

3. Information Security Policy

Document Attributes

Name	**Information Security Policy**
Approval and oversight	Headmaster
Review	School Information Security Officer
Inspection frequency	Annually or following any substantial alteration in the process
Storage site	Intranet / designated folder on network drive

Version History

Version	Data	Author	Description of modifications
0.1	01.10.2024	Coventry University	Preparing the design template

Contents

Please keep in mind that the document must be tailored to the context of the School. If you find any provisions impractical to implement, it is certainly worthwhile to consider the reasons behind this and subsequently remove, modify, or replace them with alternative measures that mitigate the risk.

General guidelines

1. User refers to any individual (School Employee or Student) utilizing the School’s IT resources, including the Internet.
2. The School supplies the Employee with IT equipment as a resource to facilitate the execution of work tasks for the School.
3. The user is accountable for the hardware and software assigned to them and the manner in which they function.
4. The User is responsible for the financial and legal ramifications of possessing illegal software on the IT equipment entrusted to him by the School.
5. Testing and/or compromising the security of the devices and IT systems provided by the Company is strictly prohibited.
6. Equipment entrusted to the School must not be made accessible to unauthorized individuals.
7. Modifications to the configuration of the supplied devices or software are strictly prohibited unless approved by the School's Information Security Officer. This restriction particularly pertains to alterations of security settings.
8. Each user is required to familiarize themselves with all regulations, instructions, and internal procedures established by the School Management.

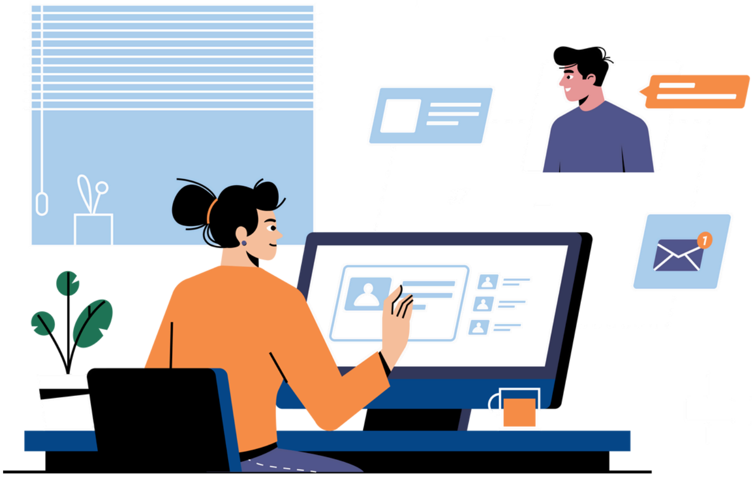
Telecommuting

Note: This pertains to equipment acquired by the School, rather than, for instance, a teacher's personal laptop utilized for work. This scenario will be addressed in the section regarding the use of personal devices or BYOD, which stands for Bring Your Own Device in English.

1. Removing entrusted mobile equipment from the School’s premises must be justified by the responsibilities undertaken by the user.
2. The user of mobile equipment has an obligation to safeguard it. Risky behaviors should be avoided, which may encompass:

- leaving equipment unsupervised (in a vehicle, hotel room, etc.),
- leaving a laptop case unattended,
- not logging the user out during periods of temporary absence or inactivity,
- configuring monitors to permit unauthorized individuals to access screen content.

3. In the event of the loss of entrusted mobile equipment utilized outside the Company, the user must promptly notify the School’s Information Security Officer and, in cases of theft, also report the incident to the Police.



Secure Authentication and Credential Management

Information regarding identifiers should be eliminated for schools that do not utilize them. The password policy must align with the current guidelines in this domain: Comprehensively about passwords | CERT Polska. The practice of requiring frequent password changes, such as every 30 days, and the common use of short, 8-character passwords, prevalent in numerous organizations, is inadvisable.

1. The user assumes responsibility for all activities conducted using his or her ID and password.
2. User passwords and other credentials are subject to enhanced protection.
3. Every user granted access to the School's IT system is required to:

- maintaining the confidentiality of all passwords and other authentication credentials utilized within the School's IT system,
- Change the password promptly if there is any suspicion or confirmed disclosure of the password.
- Utilize passwords with a minimum length of 12 characters; the password must include both uppercase and lowercase letters, as well as numbers and/or special characters.
- It is advisable to implement two-factor authentication whenever feasible.

4. Passwords must not be stored in any unambiguous format (e.g., text files, notebooks, etc.).
5. The use of an approved system specifically designed for secure password storage, such as a password manager, is permitted.
6. Logging into the system using another user's credentials is strictly prohibited.
7. The User is required to secure a computer that is not in use against unauthorized access by implementing a password-protected screen lock (clean screen policy).

Utilizing the Internet, email, and instant messaging within the educational environment.

1. **If you utilize the Internet at school, it is imperative to avoid engaging in risky behaviors, including:**
   - browsing websites that feature inappropriate content, particularly pornographic, racist, hate-promoting, sectarian, gambling-related, or any material that may offend the feelings of others or violate widely accepted principles of social coexistence,
   - browsing websites that host various forms of malicious software (e.g., malware, exploits, etc.),
   - browsing websites that host codes capable of circumventing or evading copyright protection,
   - downloading, installing, storing, or distributing software that is not authorized by the Company from the Internet.
2. Accessing websites utilized for the illegal distribution of content in violation of copyright protection regulations is strictly prohibited.
3. Mailboxes associated with an email address issued by the School are to be utilized exclusively for correspondence pertaining to the School's activities.
4. Forwarding mail to mailboxes not associated with the School, particularly private ones, is prohibited.

This provision stipulates that, for instance, a teacher is prohibited from sending materials to their personal email address; the school must evaluate whether it can realistically enforce this restriction.

5. When sending attachments that are classified as School secrets or protected by relevant legal regulations (e.g., containing personal data), such attachments must be encrypted with a password that adheres to the criteria outlined in point three of the rules. The password must not be transmitted through the same communication channel as the message.

Requirements for Utilizing Personal Devices (BYOD) for Work or Study at School

Only devices and systems endorsed by the manufacturer, for which security patches are available, may be utilized.
2. In the event of:

- loss of private equipment (e.g., due to loss or theft) utilized for processing confidential School data,
- suspicion of revealing confidential Company information,

The user must promptly notify the School's Information Security Officer upon the occurrence of such an event.

In the event of the loss of the user's personal device, its sale, or the termination of collaboration with the School, the user agrees to the School's deletion of selected or all data belonging to the School, depending on technical capabilities.

In the event of the termination of cooperation with the School, cessation of the device's use for BYOD purposes, or disposal of a personal device utilized for processing data on behalf of the School, the user agrees to contact the School's Information Security Officer to ensure the permanent deletion of data owned by the School from the device.

Information security

1.It is the user's responsibility to implement measures to safeguard the information they develop or create. The user has the following options for securing information (files):

- It is advisable to store the data in the directory specified by the School Information Security Officer.
- utilizing a school-sanctioned data storage solution.

2.Alternative solutions for storing school data are not permitted.

3. The processing of information on external data carriers (e.g., USB drives, portable disks) that are not owned by the School and have not been cryptographically secured is strictly prohibited.

4. The disclosure of information (data, files) belonging to the School to unauthorized individuals is strictly prohibited.

Secure work environment

1. To mitigate the risk of unauthorized access, loss, or damage to information during and outside of working hours, the user is required to:

- adhere to the principle of ensuring that all doors are closed and secured to prevent unauthorized access to the room.
- secure the access card; in the event of loss, promptly notify facility security and the School Information Security Officer.
- store paper documents and removable media in suitably secured office furniture,
- After completing your work, organize your workspace to prevent unauthorized access to documents containing sensitive information, adhering to the "clean desk" principle.

Incident and event reporting

1. **If you observe an incident that could indicate a security breach, software malfunction, error, or system failure, you should:**

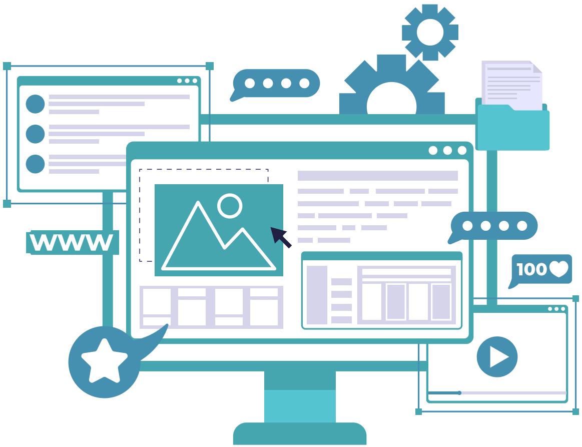
- cease using the computer,
- Promptly notify the School Information Security Officer, IT Specialist, and/or your immediate supervisor or management regarding the incident, who will assess the necessity of disconnecting the computer from the network.

The application may be submitted:

- By email to the address zgloszenia-it@szkola.pl
- In person to the School Information Security Officer, IT Specialist, and/or direct supervisor or management.

3. The application must encompass:

- indication of the user or region that observed/participated in the event,
- indication or identification of the system impacted by the incident,
- estimated time of incident,
- description of the conditions and locations where the event transpired, along with the symptom/characterization of the event.



Disciplinary measures

1. Noncompliance with the regulations established in this Policy may lead to suitable disciplinary measures.
2. Should a breach of specific regulations raise suspicions of legal infractions, the Directorate will submit all pertinent evidence to law enforcement agencies for further action.
3. Each user is obligated to remain informed about all regulations, instructions, and internal procedures established by the School Management. All regulations are archived on Google Drive, OneDrive, SharePoint, or the Network Drive.
4. When a new document (regulations, procedures, instructions, etc.) is introduced, the Information Security Officer and/or Line Manager is tasked with ensuring that the aforementioned regulations are effectively communicated to users.
5. Ignorance of current security regulations will not serve as a basis for any consideration of the user's innocence and may result in disciplinary action.

4. Cybersecurity Awareness Development Program in Educational Institutions

Document Attributes

Name	**Cybersecurity Awareness Development Program at Educational Institutions**
Approval and oversight	Headmaster
Review	School Information Security Officer
Inspection frequency	Annually or following any substantial alteration in the process
Storage site	Intranet / designated folder on network drive

Version History

Version	Data	Author	Description of modifications
0.1	01.10.2024	Coventry University	Preparing the design template

Contents

The report

The objective of this policy is to guarantee that all school personnel and students receive adequate training and consistent updates regarding organizational information security policies and procedures.

The School Management is dedicated to safeguarding the well-being of Students and Staff by implementing training and various initiatives that enhance awareness of cyber threats.

Awareness Enhancement Initiative

The awareness program encompasses the following topics:

- Information Security Policy
- Accountability for the conduct of students and school personnel, along with disciplinary measures.
- Incident Reporting Guidelines
- Education in the field of comprehensive digital security

Appendix 04.1 Cybersecurity Communication and Training Plan constitutes a vital component of the Program. This Appendix is revised annually prior to the commencement of the academic year.

Roles and Responsibilities

The School Information Security Officer is accountable for the comprehensive operation of the Programme as requested by the Management.

The instructional team endorses the execution of the program.

Students must engage in the Program as a component of their coursework at School.

4.1 Cybersecurity Communication and Training Strategy

Document Attributes

Name	**Cybersecurity Communication and Training Strategy**
Institution name	School

Version History

Version	Data	Author	Description of modifications
0.1	01.10.2024	Coventry University	Preparing the design template

Cybersecurity Communication and Training Strategy

What is the essence of our communication?	When do we engage in communication?	How do we convey information? (training method)	Who is re sponsible for t raining?	For whom is this intended?	Was it executed as intended?	Evidence of execution in accordance with the plan
School Information Security Policy and Information Security Policy	September	Educational Council	School Management/Information Security Officer	Educators and administrative personnel	NO	
Information Security Policy	September	Educational Hour - a presentation of the rules delivered in a lecture format	School Information Security Officer/Educator	Students	NO	
Lesson: Phishing Awareness	October	Educational Hour - training presentation and workshop session	School Information Security Officer/Educator	Students	NO	
Lesson: Passwords – How to Create and Manage Passwords?	November	Educational Hour - training presentation and workshop session	School Information Security Officer/Educator	Students	NO	
Incidents – how to address threats?	December	Educational Hour - training presentation and workshop session	School Information Security Officer/Educator	Students	NO	
Cyberbullying: Strategies for Prevention and Response.	January	Educational Hour - training presentation and workshop session	School Information Security Officer/Educator	Students	NO	
Disinformation – how to identify false information?	February/March (Holidays)	Educational Hour - training presentation and workshop session	School Information Security Officer/Educator	Students	NO	
Visit from a representative of the municipal guard or police	Throughout the year, for instance, April	Training for the entire school	Invited delegate	Educators and learners	NO	
Ad hoc – updates regarding contemporary cyber threats	The entire academic year	Newsletter and educational hours during meetings	School Information Security Officer/Educator	All stakeholders (students, educators, parents)	NO	
Reports on student engagement in digital security conferences and events.	subsequent to the event, e.g. May	Meeting, report presentation	School Information Security Officer	Administration, educators, guardians	NO	
Presentations by students engaged in digital security projects and competitions.	subsequent to the event, e.g. June	Gathering, a distinguished event focused on cybersecurity	Students with guardians	Educators and learners	NO	
Guest lecture by a representative of parents employed in the cybersecurity sector.	Once per semester	Lecture	Invited parent.	Educators and learners	NO	
					NO	
					NO	
					NO	
					NO	
					NO	
					NO	
					NO	
					NO	
					NO	
					NO	

About the Author

Mateusz Pękala is a specialist in enhancing information security awareness, ensuring security compliance, conducting information security audits, and managing risk. He possesses extensive experience as an auditor, trainer, and consultant in the field of information security. He is an active member of professional organizations, including ISSA Polska and ISACA. He holds several prestigious certifications: Certified in Risk and Information Systems Control™ (CRISC), Certified Information Systems Security Professional (CISSP), Certified Data Privacy Solutions Engineer™ (CDPSE®), and Certified Information Systems Auditor® (CISA), in addition to auditor certification in accordance with ISO 27001.

Additional details regarding the project

CYBERSEC

EDUCHECK

- https://www.coventry.ac.uk/wroclaw/
- https://kreatywnidlabiznesu.pl/cyber-sec-edu-check/
- https://eccedu.net/

Funded by the European Union, the views and opinions expressed herein are solely those of the author(s) and do not necessarily represent the views of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor the EACEA can be held accountable for these perspectives.

All outcomes generated within this project are accessible under open licenses (CC BY-NC 4.0). They may be utilized at no cost and without limitations. Reproduction or modification of these materials, in whole or in part, without the author's permission is strictly forbidden. When utilizing the results, it is essential to acknowledge the source of funding and the authors.

PROJECT NO. 2023-2-PL01-KA210-VET-000176822

Co-funded by the European Union

LEADER: Research Institute Europe | Coventry University

PARTNERS: STOWARZYSZENIE KREATYWNI DLA BIZNESU

EUROPEAN CENTRE FOR CAREER EDUCATION