Mapping of maritime protocols for CyberSEA Report

Project Acronym:	CyberSEA
Full Title:	CyberSEA - Increasing Cyber Security at SEA through digital training
Project no.:	2023-1-ES01-KA220-VET-000159793
File Ref:	WP2-Review of Best Practices
Version:	0.1
Status:	Final
Start date of the project:	01.09.2023 ***Duration:*** 36 months

Funding body: Co-funded by the European Union

Partners' logo:

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

List of Output Contributors

No.	Participant Organisation Name	Participant Short Name	Country
1	UNIVERSITAT POLITECNICA DE CATALUNYA	UPC	ES
2	AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSI ANONYMI ETAIREIA	IDEC	GR
3	SPINAKER, navticno izobrazevanje in trgovina, d.o.o.	SPINAKER	SI
4	Academia Navala "Mircea cel Batran"	RNA	RO
5	Berlin School of Business and Innovation GmbH	BSBI	DE
6	Centre for Factories of the Future	C4FF	SE
7	POLITECHNIKA MORSKA W SZCZECINIE PM	MUS	PL
8	ELLINIKO MESOGEIAKO PANEPISTIMIO	HMU	EL
9	SATAKUNNAN AMMATTIKORKEAKOULU OY	SMK	FL

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Contents

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

1. Introduction

1.1. Document Purpose

The purpose of this document is to report on the findings and achievements of Work Package 2 (WP2) of the CyberSEA project. WP2 is focused on developing practical training resources for cadets and seafarers, enhancing their understanding of cyber threats and improving their ability to respond effectively. This report outlines the objectives, methodologies, and outcomes of WP2, The report aims to provide stakeholders with a comprehensive understanding of the steps taken to identify maritime cyber vulnerabilities transfer best practices from other industries.

1.2. Approach Applied

To achieve the objectives of WP2, a systematic and multi-pronged approach was applied:

Cross-Industry Best Practices: Comprehensive desk research was conducted to identify and analyze cybersecurity best practices from other industries. These best practices were then adapted to the unique context of maritime operations to prevent cyber threats.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

2. Review of Current Practices

2.1. Introduction

The maritime industry is increasingly dependent on digital technology and internet-based communication for its operations, making it vulnerable to cyber threats that can disrupt the safe transport of goods and jeopardize human safety at sea. In recent years, there has been a growing recognition of the need to strengthen cybersecurity measures across the sector, particularly following high-profile incidents that have highlighted vulnerabilities in shipping networks and onboard systems.

To address these challenges, the CyberSEA project was launched with the objective of enhancing cybersecurity awareness and training among cadets and seafarers, thereby improving the overall resilience of the maritime industry. Work Package 2 (WP2) plays a critical role in achieving this goal by developing practical and realistic training resources tailored to the unique requirements of the maritime context.

2.2. Desk Research

2.2.1. Cybersecurity Best Practices Data Collection Germany

Organization Information	**Industry Type/sector**	*Education sector*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Medium, 250 people*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Managed by IT department*
	Governance Structure	• *IT department supervised by Chief Information Officer from the group.*
	Compliance with Standards	• *in accordance with ISO 27001*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Access Control and Authentication	**Access Management**	• Access policy development • User access management • Monitoring • Training and awareness
	Authentication Methods	• *Username and password authentication* • *VPN* • *MS Authenticator*
Data Protection and Privacy	**Data Encryption**	• *Encrypted sensitive data. No information about the method. .*
	Data Backup	• *Daily backups stored in IT department*
	Data Retention Policies	*Data classified based on its sensitivity, value and regulatory requirements. Retention periods determined on legal regulatory.*
Incident Response and Security Monitoring	**Incident Response Plan**	*No data*
	Security Monitoring	*Cameras, network monitoring*
Employee Training and Awareness	**Training Programs**	*Regular trainings for the employees, once a three months*
	Phishing Awareness	*Regular information distributed among the employees*
Network Security	**Firewall and Intrusion Detection Systems**	*Constantly monitored by IT department*
	Vulnerability Management	• *No data*
Third-Party Security	**Vendor Risk Management**	*Not applicable*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Mobile Device Management	**Mobile Security Policies**	*Separate WiFi for students. Using authentication software for mobile devices.*
	BYOD (Bring Your Own Device) Policies	*Not applicable*

Organization Information	**Industry Type/sector**	*Local internet provider*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Small / 15 people*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	*Based on constant monitoring of the network. LMS software used.*
	Governance Structure	*No structure. We are too small.*
	Compliance with Standards	n/a
Access Control and Authentication	**Access Management**	*Managed by LMS software.*
	Authentication Methods	*Username and passwords, VPN*
Data Protection and Privacy	**Data Encryption**	*Only for sensitive data.*
	Data Backup	*Weekly backups*
	Data Retention Policies	*Based on the regulatory framework.*
	Incident Response Plan	*No plan*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Incident Response and Security Monitoring	**Security Monitoring**	*We use open-source software. Administrator responsible for the security.*
Employee Training and Awareness	**Training Programs**	*Irregular trainings for the employees. Mandatory trainings for the new employees.*
	Phishing Awareness	*Awaraness increased during the trainings.*
Network Security	**Firewall and Intrusion Detection Systems**	*Windows Firewall*
	Vulnerability Management	*LMS software*
Third-Party Security	**Vendor Risk Management**	*We use only the equipment authorized by our administrator.*
Mobile Device Management	**Mobile Security Policies**	*None*
	BYOD (Bring Your Own Device) Policies	*It is allowed.*

2.2.2. Cybersecurity Best Practices Data Collection Sweden

Organization Information	**Industry Type/sector**	*Construction sector*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Small, 35 people*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Policy in accordance with ISO 27001* • *Policy reviewed once yearly*
	Governance Structure	• *The management team together with the external IT Partner have the responsibility to update and monitor.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Compliance with Standards	• *in accordance with ISO 27001 and NIS2*
Access Control and Authentication	**Access Management**	• *All access is controlled by who is logged in, Zero Trust is applied as often as possible. You therefore only see what you should have access to.*
	Authentication Methods	• *Authentication usually takes place against a Windows Active Directory, which then controls what you should have access to, system/files/mail etc.* *Multifactor is used 100% where it can be activated. Often together with an app in your mobile. But also additional security with a physical security key (YubiKey's)* *All data stored locally on each workstation is encrypted by default.* *If a computer were to be stolen, there is no need to worry about the data located locally on the hard drive.* *Individual files are normally not encrypted, unless it may be sent via email and contains sensitive data.* *All data sent between a server and online service is encrypted in one way or another.*
Data Protection and Privacy	**Data Encryption**	• *Daily backups stored in Sweden. All data is encrypted during transit and storage.*
	Data Backup	• *Daily backups stored in Sweden. All data is encrypted during transit and storage.*
	Data Retention Policies	• *In some cases, unless exceptions are made, everything that falls under the GDPR is purged after 365 days.* *Otherwise, all data remains until someone actively clears it manually.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Incident Response and Security Monitoring	**Incident Response Plan**	*There is no such plan due to savings.*
	Security Monitoring	*No such monitoring due to savings.*
Employee Training and Awareness	**Training Programs**	*No training programs*
	Phishing Awareness	*Phishing tests are done occasionally, where controlled emails are sent out.* *Users must report suspicious emails to the IT Manager / IT Partner*
Network Security	**Firewall and Intrusion Detection Systems**	*The firewall monitors all traffic according to specific rules that you set up.* *All deviations are reported directly to the IT Partner.*
	Vulnerability Management	• *Unfortunately this is done very rarely, every three years. Done by the IT partner.*
Third-Party Security	**Vendor Risk Management**	*It is rarely relevant in our case.*
Mobile Device Management	**Mobile Security Policies**	*For mobile phones, the password function or unlock function via fingerprint must be activated.* *Email programs or other company-specific applications should not be left open when the phone is not in use.* *Mail or attachments from unknown senders should not be opened.* *Open wireless networks should not be used in any context, not even in the home. Only*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		trusted networks with passwords should be used. *Surfing should not take place to websites that may pose a risk. If there is uncertainty as to whether a place or page can be considered safe, surfing there should not take place.* *Pin codes and passwords must not be spread or written down near the phone.* *The mobile phone must not be left unattended, for example in a car, in a wardrobe or the like.* *Apps may not be installed without express consent.* *Backup of mail, calendar and contacts is handled by the company.* *A lost telephone must be reported to the person in charge of telephony.*
	BYOD (Bring Your Own Device) Policies	*Not allowed*

Organization Information	**Organization Name**	University Centre
	Industry Type	*Education*
	Contact Person	*Data Protection & Freedom of Information Officer*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *THE CENTRE has a comprehensive cybersecurity policy in place that outlines guidelines for securing sensitive information, data access, and incident reporting. The policy is reviewed and updated annually.*
	Governance Structure	• *The IT department oversees cybersecurity initiatives at THE CENTRE. The Chief Information Officer (CIO) is responsible for the governance of cybersecurity practices.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Compliance with Standards	• *THE CENTRE adheres to cybersecurity standards such as ISO 27001 and follows guidelines from the Family Educational Rights and Privacy Act (FERPA) to ensure compliance.* • *They are certified "Cyber Essentials Plus" organisation*
Access Control and Authentication	**Access Management**	• *Access to student records, financial data, and other sensitive information is managed through role-based access controls. Access rights are regularly reviewed and updated.*
	Authentication Methods	• *THE CENTRE employs a combination of username/password authentication and multi-factor authentication (MFA) for secure access to systems and applications.* • *THE CENTRE uses Duo Security to verify user identity with login tools like biometrics, security keys, and the Duo Push mobile app.*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data, including student and staff information, is encrypted both in transit and at rest using industry-standard encryption algorithms.*
	Data Backup	• *Regular backups of critical data are performed nightly, and backups are stored in an offsite location to ensure data recovery in the event of a cyber incident.*
	Data Retention Policies	• *THE CENTRE follows a strict data retention policy to manage the lifecycle of data. Obsolete data is securely disposed of in accordance with best practices.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Incident Response and Security Monitoring	**Incident Response Plan**	• *THE CENTRE has a detailed incident response plan in place, regularly tested through simulations and updated based on lessons learned from each exercise.*
	Security Monitoring	• *The university employs advanced security monitoring tools to detect and respond to security incidents.* • *Logs are regularly reviewed for anomalies, and automated alerts are in place.*
Employee Training and Awareness	**Training Programs**	• *Annual cybersecurity training is mandatory for all faculty and staff, covering topics such as data security, phishing awareness, and best practices for securing personal devices.*
	Phishing Awareness	• *THE CENTRE conducts regular phishing awareness campaigns, simulating phishing attacks to educate employees on identifying and reporting potential threats.* • *The victims of phishing campaigns then undergo cybersecurity awareness training.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Firewalls and intrusion detection systems are implemented to monitor and control network traffic. Regular vulnerability assessments are conducted to identify and address potential weaknesses.*
	Vulnerability Management	• *Vulnerability assessments are performed quarterly to identify and remediate vulnerabilities in systems and applications.*
Third-Party Security	**Vendor Risk Management**	• *Third-party vendors are assessed for cybersecurity risks before engagement. Contracts include cybersecurity clauses, and vendors are required to adhere to university cybersecurity standards.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Mobile Device Management	**Mobile Security Policies**	• *Policies are in place to secure mobile devices used by faculty and staff, including encryption, remote wipe capabilities, and the use of passcodes.*
	BYOD (Bring Your Own Device) Policies	• *THE CENTRE has a Bring Your Own Device (BYOD) policy outlining security requirements for personal devices used for work purposes.*

Organization Information	**Industry Type/sector**	*Technology*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Medium-sized Enterprise*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *The company has a robust cybersecurity policy that outlines security standards, roles, and responsibilities. The policy focuses on protecting sensitive information and ensuring compliance with international cybersecurity standards. It is reviewed and updated annually to reflect new threats and regulatory changes.*
	Governance Structure	• *The Chief Information Security Officer (CISO) oversees cybersecurity efforts and reports directly to the CEO. The IT Security Committee, comprising representatives from each department, ensures the implementation of cybersecurity measures.*
	Compliance with Standards	• *The company adheres to ISO/IEC 27001 standards for information security management. Compliance is ensured through regular audits by internal teams and external consultants.*
Access Control and Authentication	**Access Management**	• *Access to sensitive systems is managed through role-based access control (RBAC). Employees are granted access based on their role and responsibilities, ensuring minimum access to critical data.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Authentication Methods	• *Multi-factor authentication (MFA) is mandatory for all employees. It includes the use of passwords combined with biometric verification or one-time codes sent to secure devices.*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data is encrypted using AES-256 standards both in transit and at rest to safeguard against unauthorized access.*
	Data Backup	• *Data backups are performed daily, with copies stored in secure cloud environments and physical locations in Sweden.*
	Data Retention Policies	• *The company retains data for seven years, after which unnecessary or obsolete data is securely deleted using certified methods, such as data wiping and shredding.*
Incident Response and Security Monitoring	**Incident Response Plan**	*The incident response plan includes predefined steps for identifying, assessing, and responding to security breaches. It is tested biannually through simulated cyberattack scenarios.*
	Security Monitoring	*The company uses SIEM (Security Information and Event Management) tools to monitor network traffic and detect any anomalies. Advanced tools like Splunk are used to automate threat detection.*
Employee Training and Awareness	**Training Programs**	*Employees undergo mandatory cybersecurity training every quarter, which includes lessons on secure data handling, phishing prevention, and social engineering attacks. Performance is assessed through quizzes and simulated attack tests.*
	Phishing Awareness	*A phishing awareness program includes regular simulated phishing emails. Employees who identify phishing attempts are rewarded, while those who fail are given additional training.*
Network Security	**Firewall and Intrusion Detection Systems**	*Next-generation firewalls (NGFW) are employed to inspect incoming and outgoing traffic. Additionally, intrusion detection systems (IDS) monitor for any suspicious activity within the network.*
	Vulnerability Management	*Vulnerabilities are identified through monthly vulnerability assessments using tools like Nessus.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		High-risk vulnerabilities are patched within 48 hours of detection.
Third-Party Security	**Vendor Risk Management**	*Third-party vendors are assessed for their cybersecurity postures, with only those compliant with ISO/IEC 27001 being approved. Vendors undergo an annual review to ensure continued adherence to security standards.*
Mobile Device Management	**Mobile Security Policies**	*Mobile devices are secured through mobile device management (MDM) software, which enforces encryption, remote wipe, and secure access policies.*
	BYOD (Bring Your Own Device) Policies	*Employees using personal devices must install company-approved security software, which includes anti-malware protection and VPN access. Security audits on personal devices are conducted quarterly.*

2.2.3. Cybersecurity Best Practices Data Collection Greece

Organization Information	**Organization Name**	*Company 1*
	Industry Type	*Packaging*
	Contact Person	*John Doe*
	Email	
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Company has a comprehensive cybersecurity policy in place that outlines guidelines for securing sensitive information, data access, and incident reporting.*
	Governance Structure	• *The IT department oversees cybersecurity initiatives at Company 1. The head of IT department is responsible for the governance of cybersecurity practices.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Compliance with Standards	• *Company does not adhere to any cybersecurity standards.*
Access Control and Authentication	**Access Management**	• *Access to records, financial data, and other sensitive information is managed through role-based access controls. Access rights are regularly reviewed and updated.*
	Authentication Methods	• *Company employs a combination of username/password authentication for secure access to systems and applications.*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data, are not encrypted.*
	Data Backup	• *Regular backups of critical data are performed nightly, and backups are stored in the cloud to ensure data recovery in the event of a cyber incident.*
	Data Retention Policies	• *Company follows a data retention policy to manage the lifecycle of data. Obsolete data is dispose.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *Company has a not an incident response plan in place.*
	Security Monitoring	• *The company employs advanced security monitoring tools to detect and respond to security incidents.* • *Logs are not reviewed for anomalies, automated alerts are in place.*
Employee Training and Awareness	**Training Programs**	• *No training programs.*
	Phishing Awareness	• *Company conducted phishing awareness simulations to educate employees on identifying and reporting potential threats.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		• *The victims of phishing campaigns then undergo phishing awareness training.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Firewalls and intrusion detection systems are implemented to monitor and control network traffic. Vulnerability assessments are conducted to identify and address potential weaknesses.*
	Vulnerability Management	• *Vulnerability assessments are performed annually to identify and remediate vulnerabilities in systems and applications.*
Third-Party Security	**Vendor Risk Management**	• *Third-party vendors are not assessed for cybersecurity risks before engagement.*
Mobile Device Management	**Mobile Security Policies**	• *Policies are in place to secure mobile devices used by faculty and staff, remote wipe capabilities, and the use of passcodes.*
	BYOD (Bring Your Own Device) Policies	• *Company has a Bring Your Own Device (BYOD) policy outlining security requirements for personal devices used for work purposes.*

Organization Information	**Organization Name**	*Company 2*
	Industry Type	*Education*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Company has a comprehensive cybersecurity policy in place that outlines guidelines for securing sensitive information, data access, and incident reporting. The policy is reviewed and updated frequently.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Governance Structure	• *The IT department oversees cybersecurity initiatives at Company. The head of IT department is responsible for the governance of cybersecurity practices.*
	Compliance with Standards	• *Company adhere to cybersecurity standards with* ISO 27001 and 27701.
Access Control and Authentication	**Access Management**	• *Access to records, financial data, and other sensitive information is managed through role-based access controls. Access rights are regularly reviewed and updated.*
	Authentication Methods	• *Company employs a combination of username/password authentication for secure access to systems and applications.*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data, are encrypted.*
	Data Backup	• *Regular backups of critical data are performed nightly, and backups are stored in the cloud to ensure data recovery in the event of a cyber incident.*
	Data Retention Policies	• *Company follows a data retention policy to manage the lifecycle of data.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *Company has a not an incident response plan in place.*
	Security Monitoring	• *The company employs advanced security monitoring tools to detect and respond to security incidents.* • *Logs are rarely reviewed for anomalies, and automated alerts are in place.*
Employee Training and Awareness	**Training Programs**	• *Company 2 has training programs for their employees.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Phishing Awareness	• *Company conducted phishing awareness in their training programs.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Firewalls and intrusion detection systems are implemented to monitor and control network traffic. Regular vulnerability assessments are conducted to identify and address potential weaknesses.*
	Vulnerability Management	• *Vulnerability assessments are not performed to identify and remediate vulnerabilities in systems and applications.*
Third-Party Security	**Vendor Risk Management**	• *Third-party vendors are assessed for cybersecurity risks before engagement. Contracts include cybersecurity clauses, and vendors are required to adhere to university cybersecurity standards.*
Mobile Device Management	**Mobile Security Policies**	• *Policies are in place to secure mobile devices used by faculty and staff, remote wipe capabilities, and the use of passcodes.*
	BYOD (Bring Your Own Device) Policies	• *Company has a Bring Your Own Device (BYOD) policy outlining security requirements for personal devices used for work purposes.*

Organization Information	**Industry Type/SIZE**	*Food factory / 60 employees*
	Contact Person	
	Email	

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *There is an installed firewall, which is updated daily with blacklists.* • *In servers the access is allowed in specific mac address*
	Governance Structure	• *For the overseeing cybersecurity responsible is the system admin*
	Compliance with Standards	• *Firewall and internet gateways* • *User access control* • *Antivirus* • *Secure configuration*
Access Control and Authentication	**Access Management**	• *In servers the access is allowed in specific mac address* • *VPN for remote access* • *Username and password for shared folders* • *VLANs isolation*
	Authentication Methods	• *Username and password* • *Openvpn, wireguard*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data are compressed and locked with password*
	Data Backup	• *Daily Local backup* • *Daily Cloud Backup*
	Data Retention Policies	• *At the end of each tourist season, outdated data are backed up and deleted at the start of the next season. Data concerning customer reservations as well as accounting data are not deleted.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *Servers are backed-up using a virtual machine backup system.* • *There is a second backup server.* • *The response plan is tested once a year.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Security Monitoring	• *Firewall holds blocked IPs for 14 days and emails the list to admin.*
Employee Training and Awareness	**Training Programs**	• *There is no training program.*
	Phishing Awareness	• *Employees are told to delete an email immediately with a strange subject and do not open it.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Firewall holds blocked IPs for 14 days and emails the list to admin.*
	Vulnerability Management	• *Antivirus systems alerts* • *Firewall alerts*
Third-Party Security	**Vendor Risk Management**	• *n/a*
Mobile Device Management	**Mobile Security Policies**	• *If the lost or stolen devices have an account that has access to the network, all codes related to this account are immediately changed.*
	BYOD (Bring Your Own Device) Policies	• *There is no BYOD policy*

Organization Information	**Industry Type/SIZE**	*Hotel/20 employees*
	Contact Person	
	Email	
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *There is an installed firewall, which is updated daily with blacklists.* • *The access to servers is allowed only to specific MAC addresses.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Governance Structure	• *The system administrator is responsible for cybersecurity incidents.*
	Compliance with Standards	• *Firewall and internet gateways.* • *User access control* • *Antivirus* • *Secure configuration*
Access Control and Authentication	**Access Management**	• *The access to servers is allowed only to specific MAC addresses.* • *VPN for remote access.* • *Username and password for shared folders.* • *VLANs isolation.*
	Authentication Methods	• *Username and password* • *Openvpn, wireguard*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data are compressed and locked with password.*
	Data Backup	• *Daily Local backup* • *Daily Cloud Backup*
	Data Retention Policies	• *At the end of each tourist season, outdated data is backed up and deleted at the start of the next season. Data concerning customer reservations as well as accounting data are not deleted.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *Servers are backed-up using a virtual machine backup system. The response plan is tested once a year.*
	Security Monitoring	• *Firewall holds blocked IPs for 14 days and emails the list to the admin.*
Employee Training and Awareness	**Training Programs**	• *There is no training program.*
	Phishing Awareness	• *Employees are told to delete an email immediately with a strange subject and do not open it.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Network Security	**Firewall and Intrusion Detection Systems**	• *Firewall holds blocked IPs for 14 days and emails the list to the admin.*
	Vulnerability Management	• *Antivirus systems alerts* • *Firewall alerts.*
Third-Party Security	**Vendor Risk Management**	• *n/a*
Mobile Device Management	**Mobile Security Policies**	• *If the lost or stolen devices have an account that has access to the network, all codes related to this account are immediately changed.*
	BYOD (Bring Your Own Device) Policies	• *There is no BYOD policy*

Organization Information	**Industry Type/SIZE**	*Frozen food factory/20 employees*
	Contact Person	
	Email	
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *There is an installed firewall, which is updated daily with blacklists.* • *The access to servers is allowed only to specific MAC addresses*
	Governance Structure	• *The system administrator is responsible for cybersecurity incidents.*
	Compliance with Standards	• *Firewall and internet gateways.* • *User access control.* • *Antivirus.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Access Control and Authentication	**Access Management**	• *The access to servers is allowed only to specific MAC addresses.* • *VPN for remote access.* • *Username and password for shared folders.* • *VLANs isolation.*
	Authentication Methods	• *Username and password* • *Openvpn, wireguard*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data are compressed and locked with password.*
	Data Backup	• *Daily Local backup* • *Daily Cloud Backup*
	Data Retention Policies	• *Outdated data are backed up and deleted every six months. Accounting data are not deleted.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *Servers are backed-up using a virtual machine backup system. The response plan is tested once a year.*
	Security Monitoring	• *Firewall holds blocked IPs for 14 days and emails the list to the admin.*
Employee Training and Awareness	**Training Programs**	• *There is no training program.*
	Phishing Awareness	• *Employees are told to delete an email immediately with a strange subject and do not open it.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Firewall holds blocked IPs for 14 days and emails the list to the admin.*
	Vulnerability Management	• *Antivirus systems alerts* • *Firewall alerts*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Third-Party Security	**Vendor Risk Management**	• *n/a*
Mobile Device Management	**Mobile Security Policies**	• *There is no Mobile Security policy*
	BYOD (Bring Your Own Device) Policies	• *There is no BYOD policy*

Organization Information	**Organization Name**	*Winery Company*
	Industry Type/SIZE	*Winery /Medium*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *The company has a comprehensive cybersecurity policy in place that outlines guidelines for securing sensitive information, data and general access, and incident reporting during the production line. The policy is reviewed and updated annually.*
	Governance Structure	• *The IT department oversees cybersecurity initiatives with the supervisor of external IT. The Chief Information Officer (CIO) is responsible for the governance of cybersecurity practices along with Production & Quality Manager.*
	Compliance with Standards	• *The company adheres to cybersecurity standards such as ISO 27001 and follows guidelines from IFS/BRC standard for Data Security for Food Production.* • *They are also certified with Authorised Economic Operation (AEO) Certification. Traders who voluntarily meet a range of criteria work in close cooperation with customs authorities to assure the common objective of supply chain security are entitled to enjoy benefits throughout the EU. In order to be certified by Greek Custom Authorities, The company successfully audited by General Secretariat of Information Systems and Digital Governance.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Access Control and Authentication	**Access Management**	• *Only the central system administrator is responsible for users, access rights (both to shared resources and internal subsystems) and for changing passwords.* • *The company employs a username/password authentication with great complexity that change every 90 days* • *In office applications (which also have online access) the user has full access to change the password.* • *Due to the mandatory security policies set by Microsoft strict two factor authentication policies are enforced.*
	Authentication Methods	• *Due to the mandatory security policies set by Microsoft strict two factor authentication policies are enforced..* • *In order to get access to specific areas of the company, the Quality & Production Manager shall give you card with permitted access.*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data, including wine production, alcohol use in production and clients, is encrypted both in transit and at rest using industry-standard encryption algorithms.*
	Data Backup	• *The VEEAM suite is mainly used by the company for backup and disaster recovery.* • *Full copies of the central servers are created daily and kept for seven days. Recovery can be done either piecemeal at the file level or at the virtual server level.* • *Recovery can be done on a daily basis.* • *Individual batches in parallel with VEEAM during the day create copies of important files (Databases, office application files) on the storage server (storage server) in folders with limited access rights.* • *On certain days of the month, they create intermediate copies.* • *This acts as an additional layer of security and an instant process to recover selected data or create a test development environment.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		• *At irregular intervals, for reasons of randomness, critical parts of the systems and mainly databases are created and stored on removable media.* • *The backup copies are stored on the storage server (synology) of the headquarters and, as the case may be, on the corresponding one in Athens.*
	Data Retention Policies	• *The company follows a strict data retention policy to manage the lifecycle of data. Obsolete data is securely disposed of in accordance with best practices.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *The company has an updated and recorded Security Plan and Business Continuity Plan, which specifies the measures taken to protect the information system from unauthorized intrusion and from intentional destruction or loss of information and the response plans in case of incidents.* • *Parts or scenarios of the plans are simulated annually due to ISO 27001 audits.*
	Security Monitoring	• *Users of the company's information system are prohibited from installing and using software that has not been approved and legally purchased by the company. In addition, each computer/tablet runs software that protects against viruses and malicious code (antivirus, anti-spyware, etc.), which is even updated frequently and automatically.* • *This software controls all incoming and outgoing files from the computer, whether they are moving over a network, the Internet, web pages, e-mail or portable storage media. In addition, a central management console of the anti-virus software has been installed, through which the frequent updating of the versions on the individual computers is controlled and a record of the detected viruses is kept.* • *If the above are central applications with clients per device or are installed on each device autonomously, Policies that impose on the systems.* • *A central management console of the anti-virus software is installed, through which the frequent*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		updating of the versions on the individual computers is controlled and a record of the detected viruses is kept. • *For the installation of updates on each workstation there is a policy from AD. It is updated frequently and automatically.*
Employee Training and Awareness	**Training Programs**	• *All employees are informed and trained about the Information System Security Plan and the Emergency Plan, Privacy and Data Protection Policies and shared on all terminals by the Server.* • *The company's Quality Manager in the context of in-house trainings keeps a record of trainers and a program that includes the correct use of company's IT system.* • *Also, the IT manager informs the staff and management via email about malicious software, emails, etc. when they arise.*
	Phishing Awareness	• *The IT manager informs the staff and management via email about malicious software, emails, etc. when they arise.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Firewalls and intrusion detection systems are implemented to monitor and control network traffic. Regular vulnerability assessments are conducted to identify and address potential weaknesses.*
	Vulnerability Management	• *Vulnerability assessments are performed a*nnually, both with penetration tests *to identify and remediate vulnerabilities in systems and applications*
Third-Party Security	**Vendor Risk Management**	• *Third-party vendors are assessed for cybersecurity risks before engagement. Contracts include cybersecurity clauses, and vendors are required to adhere to the company's cybersecurity standards.*
Mobile Device Management	**Mobile Security Policies**	• *Policies are in place to secure mobile devices used by staff, including encryption, remote wipe capabilities, and the use of passcodes.*
	BYOD (Bring Your Own Device) Policies	• *The company permit personal devices only in the office areas and prohibit them in the production area.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Organization Information	**Organization Name**	*Batteries production and recycling company*
	Industry Type/SIZE	*Batteries production and recycling industry / Large*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *The company has a comprehensive cybersecurity policy in place that outlines guidelines for securing sensitive information, data and general access, and incident reporting during the production line. The policy is reviewed and updated annually.*
	Governance Structure	• *The IT department oversees cybersecurity initiatives. The Information Manager is responsible for the governance of cybersecurity practices.*
	Compliance with Standards	• *The company adheres to cybersecurity standards such as ISO 27001 and* ISO 22301 (business continuity). • *They are also certified with Authorised Economic Operation (AEO) Certification. Traders who voluntarily meet a range of criteria work in close cooperation with customs authorities to assure the common objective of supply chain security are entitled to enjoy benefits throughout the EU. In order to be certified by Greek Custom Authorities, the company successfully audited all its facilities by General Secretariat of Information Systems and Digital Governance.*
Access Control and Authentication	**Access Management**	• *Information systems and applications have mechanisms that prohibit access to resources/subsystems/files by unauthorized users. Essentially, they have appropriate measures to ensure the guaranteed correct identification and authentication of users, while at the same time specific rights/authorizations are assigned to each user on a technical level.* • *Access to the Group's information systems is provided only to users, for whom it is necessary to carry out their professional activities. In addition, the minimum acceptable level of rights is provided, based on need-to-know / need-to-use.* • *The Information Security Committee at the information level determines the general categories*

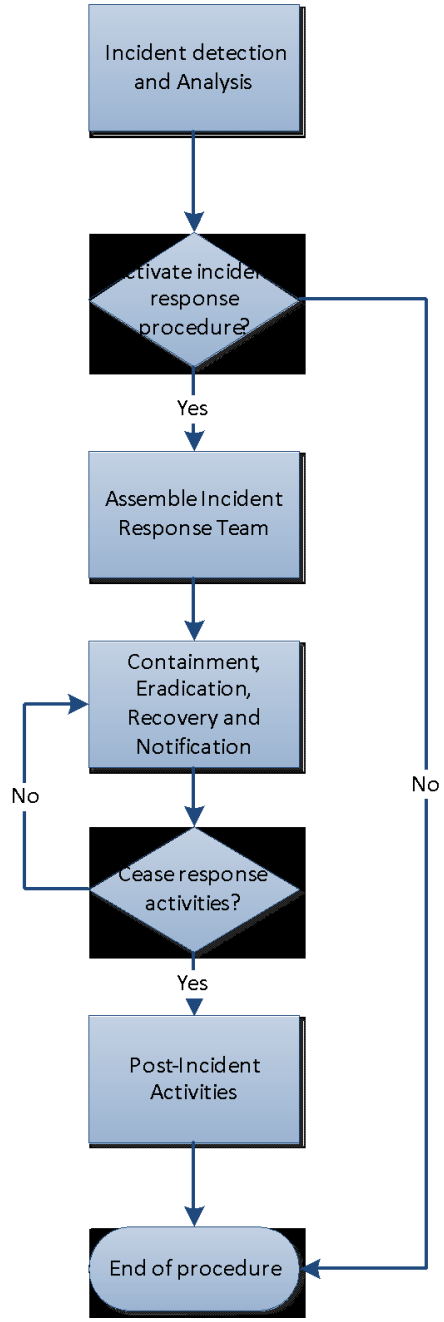
The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		of users and their access rights. Accordingly, the Head of each Department of the Company can determine which users of the Department have access to the information, as well as what type of access. The Information Technology Directorate at the application level and at the operating system level of the information systems determines the categories of users as well as their access rights.
	Authentication Methods	• *The used logical access control mechanisms, in the Company's information systems, should belong to one of the two basic categories:* • *Mechanisms that confirm that the user knows a secret (password, passphrase, code (2FA) etc.)* • *Mechanisms that confirm that the user is in possession of a credential (magnetic card, "smart" card, etc.).* • *If required by security requirements (e.g. remote access or not to critical information systems), mechanisms may be chosen that combine both of the aforementioned mechanisms (two factor authentication).*
Data Protection and Privacy	**Data Encryption**	• *Sensitive data, including wine production, alcohol use in production and clients, is encrypted both in transit and at rest using industry-standard encryption algorithms.*
	Data Backup	• *Policy for taking and managing backup copies is applied to all central critical resources ie information systems, applications, databases, systems, files, user file data, log files.* • *Selected backup copies are kept in a different space/physical location from the original data location, i.e. they are kept in another secure place within the organization and measures are taken to transport them safely. The storage of backup copies outside the central building facilities of the organization is facilitated by the creation and operation of a Data Center in an alternative location (Disaster Recovery Site), which additionally ensures business continuity in cases of catastrophic events in (e.g. fire, flood, etc. .).* • *In distributed registers of the information and network infrastructures, the software systems as well as the categories of files and data used and maintained, all the central information resources of*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		the organization related to information security are recorded. In particular, each official organizational unit that has and operates an IT and network infrastructure under the responsibility of the unit's administrative manager and in collaboration with the IS manager ensures that the following are recorded: *• Computing equipment (servers, workstations, disk systems)* *• Network equipment* *• Network security devices* *• Mobile Devices* *• Operating systems, middleware, databases* *• Software applications and information systems* *• Data / information (databases, printed or electronic documents, data on optical or magnetic media, etc..)* *• Auxiliary networks / supporting systems (electricity, telecommunications, air conditioning)* ● *The Data Backup of the systems, servers, mail servers and databases are described in the "Backup Policy and Procedures" form which is attached and describes the procedures for each company installation.*
	Data Retention Policies	● *The company follows a strict data retention policy to manage the lifecycle of data. Obsolete data is securely disposed of in accordance with best practices.*
Incident Response and Security Monitoring	**Incident Response Plan**	● *The company has an updated and recorded Security Plan and Business Continuity Plan, which specifies the measures taken to protect the information system from unauthorized intrusion and from intentional destruction or loss of information and the response plans in case of incidents.* ● *Parts or scenarios of the plans are simulated annually due to ISO 27001 and ISO 22301 audits.*
	Security Monitoring	● The security logs of the Server/Firewall are checked daily as well as there is a 24x7 SOC that informs us of security incidents for their immediate treatment. ● The company has an Information Security Incident Handling Procedure, which describes the steps to control, record and deal with incidents.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		• The flow of the incident response process is shown in the diagram below: 
Employee Training and Awareness	**Training Programs**	• *All employees are informed and trained about the Information System Security Plan and the Emergency Plan, Privacy and Data Protection Policies and shared on all terminals by the Server.* • *The company's Quality Manager in the context of in-house trainings keeps a record of trainers and a*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		program that includes the correct use of company's IT system. ● *External partner CISCO organizes security webinars.*
	Phishing Awareness	● *The IT manager informs the staff and management via email about malicious software, emails, etc. when they arise.* ● *Whenever a company employee receives an email from a domain that does not bear the company name, the receiver is automatically signalled to check the domain before owning the message.*
Network Security	**Firewall and Intrusion Detection Systems**	● *Firewalls and intrusion detection systems are implemented to monitor and control network traffic. Regular vulnerability assessments are conducted to identify and address potential weaknesses.*
	Vulnerability Management	● *Vulnerability assessments are performed a*nnually, both with penetration tests *to identify and remediate vulnerabilities in systems and applications*
Third-Party Security	**Vendor Risk Management**	● *Third-party vendors are assessed for cybersecurity risks before engagement. Contracts include cybersecurity clauses, and vendors are required to adhere to the company's cybersecurity standards.*
Mobile Device Management	**Mobile Security Policies**	● *Policies are in place to secure mobile devices used by staff, including encryption, remote wipe capabilities, and the use of passcodes.*
	BYOD (Bring Your Own Device) Policies	● *The company permit personal devices only in the office areas and prohibit them in the production area.*

	Organization Name	IT Company
	Industry Type	*Software development / SME*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	● *The company has a comprehensive cybersecurity policy. The protection of information and its processing systems is of high importance for the Company in order to achieve its short and long-term objectives and to ensure the confidentiality of the data it manages. The applied cybersecurity*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		Policy also aims at ensuring the integrity and availability of managed information along with the integrity and confidentiality of the information contained in the information system.
	Governance Structure	• *The IT department oversees cybersecurity initiatives at the company. The Chief Information Officer (CIO) is responsible for the governance of cybersecurity practices. He is also responsible to keep track of the asset inventory list of the company*
	Compliance with Standards	• *The management of the company is committed to the effort of continuous improvement and implementation of the Information Security Management System according to the international standard ISO 27001*
Access Control and Authentication	**Access Management**	• *Access control policy: User access rights to OneDrive folders are recorded in a document (Cloud Environment, Active directory with 365). Access rights of employees are defined by IT Manager who creates local user account in specific work station and gives access to cloud Fileserver. IT Manager is the only one with Administrator rights*
	Authentication Methods	• *The company's employees receive their passwords via email or phone call from the IT Manager.* • *Secure log-on procedures: password at least 8 characters with password complexity. Reuse of the same password is allowed after 10 times of changing*
Data Protection and Privacy	**Data Encryption**	• *Encryption of all data transferred by the company either on USB. Encryption is implemented on all Company Laptops* • *Key management: IT Manager*
	Data Backup	• *Backup services are supported by the hosting platforms of external partner*
	Data Retention Policies	• *The company follows a strict data retention policy to manage the lifecycle of data.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Incident Response and Security Monitoring	**Incident Response Plan**	• *The company has a detailed incident response plan. This plan is well described in specific procedure of ISMS*
	Security Monitoring	• *Information security requirements analysis and specification: contracts with suppliers* • *Securing application services on public networks: use of certificates* • *Protecting application services transactions: bank transactions via SSL and high encryption*
Employee Training and Awareness	**Training Programs**	• *Annual cybersecurity training concerning ISO 27001 and information security policies*
	Phishing Awareness	• *The company informs the employees concerning cyber attacks, how to report and treat incidents and about important rules of business continuity*
Network Security	**Firewall and Intrusion Detection Systems**	• *The company uses Firewall in order to prevent intrusions and other cyber attacks.*
	Vulnerability Management	• *Vulnerability assessments are performed every 6 months to identify and remediate vulnerabilities in systems and applications.*
Third-Party Security	**Vendor Risk Management**	• *Contracts with suppliers include cybersecurity clauses. All of the company's suppliers are required to adhere to company's cybersecurity standards.*
Mobile Device Management	**Mobile Security Policies**	• *In accordance with teleworking policy, included in the ISMS*
	BYOD (Bring Your Own Device) Policies	• *Not implemented*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

2.2.4. Cybersecurity Best Practices Data Collection Poland

Organization Information	**Organization Name**	*Financial Company*
	Industry Type/SIZE	*Financial / 500+ employees*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Provide an overview of your organization's cybersecurity policy.* Cybersecurity policy is part of Information Security Policy, which is based on ISO 27k standards and partially on NIST standards. • *How frequently is the policy reviewed and updated?* At least once a year and after every significant change in organisations plans or business strategy as well as after change in law regulations.
	Governance Structure	• *Describe the governance structure for cybersecurity within your organization.* Independent team, head of cybersecurity team reports directly to management board • *Who is responsible for overseeing cybersecurity initiatives?* Head of cybersecurity team is responsible and accountable for cybersecurity strategy. Each and every initiative must be accepted by management board and be included in budget plan. In general management board is responsible for security of organization (as they decide about costs).
	Compliance with Standards	• *List the cybersecurity standards or frameworks your organization adheres to.* ISO 27k, NIST (partially),recommendations for polish financial institutions • *How is compliance with these standards ensured?* We are obliged to pass internal and external audits.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Access Control and Authentication	**Access Management**	• *Explain how access to systems and data is managed.* We have process on granting and revoking user access rights with special attention to privileged accounts (admin, root). • *Are there role-based access controls in place?* We follow the rule of minimal necessary access rights.
	Authentication Methods	• *Describe the methods of user authentication employed in your organization.* Depending on the system / application, we implemented „something you know' and / or „something you have" and / or „something you are" methods. • *Any use of multi-factor authentication?* Yes
Data Protection and Privacy	**Data Encryption**	• *Specify how sensitive data is encrypted.* With trusted algorithms, both in-transit and at-rest. • *Is encryption employed both in transit and at rest?*
	Data Backup	• *Outline your organization's data backup procedures.* They based on business continuity plans and level of criticality of the system for business. • *How frequently are backups performed, and where are they stored?* Frequency depends on RTO (Recovery Time Objective) and RPO (Recovery Point Objective) parameters. We use dedicated backup systems that are placed both in primary and secondary data centers.
	Data Retention Policies	• *Describe your organization's policies on data retention.* Those policies depends on business needs and law regulations. • *How is obsolete or unnecessary data disposed of?* Data that are erased cannot be restored

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Incident Response and Security Monitoring	**Incident Response Plan**	• *Provide an overview of your incident response plan.* It is based on NIST standard (Incident handling) • *How often is the plan tested and updated?* As often as it is needed.
	Security Monitoring	• *Explain how your organization monitors for security incidents.* We use a number of systems, including SIEM (Security Incident & Event Management) and DLP (Data Loss Prevention) • *What tools or technologies are used for security monitoring?* Please take a look above
Employee Training and Awareness	**Training Programs**	• *Detail your organization's cybersecurity training programs for employees.* On-line trainings, 3-10 min length, on monthly basis • *How is the effectiveness of training assessed?* For example short tests and phishing tests
	Phishing Awareness	• *Describe any initiatives to raise awareness about phishing attacks.* Test phishing campaigns • *How are employees educated on identifying and reporting phishing attempts?* Through trainings, one-page materials, newsletters, test phishing campaigns

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Network Security	**Firewall and Intrusion Detection Systems**	• *Detail the use of firewalls and intrusion detection systems.* We follow the principle „defense-in-depth" • *How is network traffic monitored for anomalies?* We use few different technologies for that.
	Vulnerability Management	• *Explain how vulnerabilities in systems and applications are identified and addressed.* We conduct vulnerability scans; findings are addressed according to internal procedure. • *How frequently are vulnerability assessments conducted?* It depends on criticality of the vulnerability and server.
Third-Party Security	**Vendor Risk Management**	• *How does your organization assess and manage cybersecurity risks associated with third-party vendors?* We conduct audit before we start cooperation with external company and then after every year and/or incident • *What criteria are used to evaluate the cybersecurity posture of vendors?* Depends on cooperation model
Mobile Device Management	**Mobile Security Policies**	• *Outline the policies in place for securing mobile devices.* We use MDM (Mobile Device Management) system in order to force security policies on mobile devices • *How are lost or stolen devices handled?* There is a possibility to erase all data from mobile device remotely.
	BYOD (Bring Your Own Device) Policies	• *If applicable, describe policies related to employees using personal devices for work.* • *How is security ensured in a BYOD environment?* Private devices are not allowed in our organization

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Organization Information	**Organization Name**	*Kindergarten*
	Industry Type/SIZE	*Education/Kindergarten – up to 50 employees*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Organisation doesn't have policy regarding cybersecurity*
	Governance Structure	• *All IT services are outsourced - external company is responsible for the whole IT infrastructure including security*
	Compliance with Standards	• *We do not follow any standards*
Access Control and Authentication	**Access Management**	• *Separate computer designed for administration of kindergarten, without admin access rights; teachers use notebooks*
	Authentication Methods	• *Login plus password and Windows Hello service*
Data Protection and Privacy	**Data Encryption**	• *Hard drives are encrypted with BitLocker*
	Data Backup	• *Data backup is stored on dedicated hard drive which is connected to computers via USB*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Data Retention Policies	• *We do not have such policy*
Incident Response and Security Monitoring	**Incident Response Plan**	• *We do not have such plan*
	Security Monitoring	• *We use ESET to monitor security events*
Employee Training and Awareness	**Training Programs**	• *We do not have any training program regarding security issues*
	Phishing Awareness	• *We do not take any actions regarding phishing awareness*
Network Security	**Firewall and Intrusion Detection Systems**	• *We use ESET Internet Security as a firewall*
	Vulnerability Management	• *We do not have such process*
Third-Party Security	**Vendor Risk Management**	• *We do not have policy on Vendor Management*
Mobile Device Management	**Mobile Security Policies**	• *Employees do not have company mobile devices*
	BYOD (Bring Your Own Device) Policies	• *We do not have any policy on BYOD*

Organization Information	**Organization Name**	Logistics Company
	Industry Type/SIZE	Transport, Logistics & Shipping */ 500+ employees*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Provide an overview of your organization's cybersecurity policy.* Cybersecurity policy is part of Information Security Policy, which is based on ISO 27k standards and partially on NIST standards. • *How frequently is the policy reviewed and updated?* At least once a year and after every significant change in organisations plans or business strategy as well as after change in law regulations.
	Governance Structure	• *Describe the governance structure for cybersecurity within your organization.* Cybersecurity team reports to CIO • *Who is responsible for overseeing cybersecurity initiatives?* Head of cybersecurity team is responsible and CIO is accountable for cybersecurity initiatives.
	Compliance with Standards	• *List the cybersecurity standards or frameworks your organization adheres to.* ISO 27001, TAPA standard (in part related to information security) • *How is compliance with these standards ensured?* We are obliged to pass internal and external audits on a yearly basis.
Access Control and Authentication	**Access Management**	• *Explain how access to systems and data is managed.* We have process on granting and revoking user access rights with special attention to privileged accounts (admin, root). • *Are there role-based access controls in place?* Yes

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Authentication Methods	• *Describe the methods of user authentication employed in your organization.* Depending on the system / application: login plus password, biometry, hardware / software tokens • *Any use of multi-factor authentication?* Yes
Data Protection and Privacy	**Data Encryption**	• *Specify how sensitive data is encrypted.* With trusted algorithms. • *Is encryption employed both in transit and at rest?* Yes
	Data Backup	• *Outline your organization's data backup procedures.* Backup scope and frequency are dependent from business needs (continuity plans) • *How frequently are backups performed, and where are they stored?* We use dedicated backup systems that are placed both in primary and secondary data centers.
	Data Retention Policies	• *Describe your organization's policies on data retention.* Those policies depends on business needs and law regulations. Each system (database) has different policy. • *How is obsolete or unnecessary data disposed of?* Data that are erased cannot be restored
Incident Response and Security Monitoring	**Incident Response Plan**	• *Provide an overview of your incident response plan.* Administrators on duty are responsible for handling incident, CIO communicates / reports to management board.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Security Monitoring	• *Explain how your organization monitors for security incidents.* We use SIEM (Security Incident & Event Management) and few network monitoring tools, mostly freeware. • *What tools or technologies are used for security monitoring?* SIEM
Employee Training and Awareness	**Training Programs**	• *Detail your organization's cybersecurity training programs for employees.* At least once a year there is a dedicated training • *How is the effectiveness of training assessed?* -
	Phishing Awareness	• *Describe any initiatives to raise awareness about phishing attacks.* • *How are employees educated on identifying and reporting phishing attempts?* Trainings for employees
Network Security	**Firewall and Intrusion Detection Systems**	• *Detail the use of firewalls and intrusion detection systems.* Edge firewall (separate internal network from Internet) and internal firewall that secure databases. • *How is network traffic monitored for anomalies?* We use few freeware tools for that
	Vulnerability Management	• *Explain how vulnerabilities in systems and applications are identified and addressed.* We conduct vulnerability scans; findings are addressed according to internal procedure. • *How frequently are vulnerability assessments conducted?* Once a month

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Third-Party Security	**Vendor Risk Management**	• *How does your organization assess and manage cybersecurity risks associated with third-party vendors?* • *What criteria are used to evaluate the cybersecurity posture of vendors?* We cooperate with vendors who have high reputation
Mobile Device Management	**Mobile Security Policies**	• *Outline the policies in place for securing mobile devices.* We use MDM (Mobile Device Management) system in order to force security policies on mobile devices • *How are lost or stolen devices handled?* There is a possibility to erase all data from mobile device remotely.
	BYOD (Bring Your Own Device) Policies	• *If applicable, describe policies related to employees using personal devices for work.* • *How is security ensured in a BYOD environment?* Private devices are not allowed in our organization

Organization Information	**Organization Name**	*Cable TV*
	Industry Type/SIZE	*Local Internet & Cable TV provider – up to 200 employees*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *We have Information Security Policy where best practices regarding network security are placed. These practices base on CIS Benchmark. Policy is updated at least once a year.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Governance Structure	• *IT department is responsible for maintaining good practices. We do not have CISO, this role is to some point covered by head of IT department.*
	Compliance with Standards	• *We do not follow any standards although we use CIS Benchmark as a baseline for configuration of servers and network devices*
Access Control and Authentication	**Access Management**	• *We use Active Directory groups to control access to different subnetworks*
	Authentication Methods	• *We use login plus password method with use of Active Directory. Admins have MFA for access to some online services (like email box)*
Data Protection and Privacy	**Data Encryption**	• *We use BitLocker to encrypt hard drives. Virtual machines are encrypted with the use of native VMWare mechanisms.*
	Data Backup	• *We make regular backups using NAS devices. Critical databases are copied once a day, user data once a week.*
	Data Retention Policies	• *We do not have such policy. Different data are stored for different periods - it depends on business needs.*
	Incident Response Plan	• *We do not have such plan*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Incident Response and Security Monitoring	**Security Monitoring**	• *We use open source tools for security monitoring. Administrators works in two shifts*
Employee Training and Awareness	**Training Programs**	• *Employees have access to e-learning platforms like Pularsight.*
	Phishing Awareness	• *We do not have such program*
Network Security	**Firewall and Intrusion Detection Systems**	• *We use Next Generation Firewall which has also IDS/IPS function. New malware definitions are updated on everyday basis*
	Vulnerability Management	• *We use open source vulnerability scanner to discover vulnerabilities in our network. Reports are presented on management board meetings. It is responsible for patching*
Third-Party Security	**Vendor Risk Management**	• *We have access to feeds from producers of devices / systems and we monitor websites like exploit-db.*
Mobile Device Management	**Mobile Security Policies**	• *We do not have such policy*
	BYOD (Bring Your Own Device) Policies	• *Private devices are not allowed in our company*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

2.2.5. Cybersecurity Best Practices Data Collection Romania

Organization Information	**Industry Type/sector**	*Financial/accounting*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Very small (8 persons)*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Provide an overview of your organization's cybersecurity policy.* Our organization prioritizes cybersecurity to safeguard sensitive financial data and client information. We rely on a specialized IT company for cybersecurity measures due to the absence of own IT department. • *How frequently is the policy reviewed and updated?* *The policy is updated annually or as needed in response to changes in the regulatory requirements. The contracted IT company ensures that the policy is applied properly.*
	Governance Structure	• *Describe the governance structure for cybersecurity within your organization.* Cybersecurity governance is managed by the IT counsultant company. • *Who is responsible for overseeing cybersecurity initiatives?* *The manager is responsible for overseeing cybersecurity initiatives, but she follows advice from the IT experts company.*
	Compliance with Standards	• *List the cybersecurity standards or frameworks your organization adheres to.* We follow the requirements of Romanian legislation (related to GDPR and baseline security for companies – law 362/2018). • *How is compliance with these standards ensured?* The contracted IT company is required by contract to maintain complience with national legislation.
Access Control and Authentication	**Access Management**	• *Explain how access to systems and data is managed.* Access to systems and data is managed through access controls and permissions

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		(managed by the IT contractor, with the approval of our manager) ● *Are there role-based access controls in place?* Yes
	Authentication Methods	● *Describe the methods of user authentication employed in your organization.* Username and passwords. Some sistems also use other tools, like MFA or client digital certificates. ● *Any use of multi-factor authentication?* Yes (for example, mobile app for banking systems, and one-time code via email and digital certificates for national reporting systems).
Data Protection and Privacy	**Data Encryption**	● *Specify how sensitive data is encrypted.* Our computer have encripted drives and passwords. Data is saved also encripted in OneDrive (Microsoft cloud). ● *Is encryption employed both in transit and at rest?* *Yes*
	Data Backup	● *Outline your organization's data backup procedures.* We have regular automated backups to offsite, managed by IT company. ● *How frequently are backups performed, and where are they stored?* *Daily.*
	Data Retention Policies	● *Describe your organization's policies on data retention.* We have a data retention policy according to legal requirements (some documents up to 10 years). We do yearly reviews for disposal of unnecessary data. ● *How is obsolete or unnecessary data disposed of?* *Unnecessary data is deleted.*
Incident Response and Security Monitoring	**Incident Response Plan**	● *Provide an overview of your incident response plan.* We call the specialized IT company. By contract, they have 1 working day to stop the issue and 3 working days to restore data/functionality or provide alternative working solution.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		• *How often is the plan tested and updated?* Backups restore exercised are performed twice per year by the IT company and reports sent to our manager.
	Security Monitoring	• *Explain how your organization monitors for security incidents.* The IT company installed antivirus and other dedicated software for monitoring such problems. • *What tools or technologies are used for security monitoring?* *Antivirus, firewall*
Employee Training and Awareness	**Training Programs**	• *Detail your organization's cybersecurity training programs for employees.* We do some IT trainings on new software features, but not necessarily focused on cybersecurity. • *How is the effectiveness of training assessed?* -
	Phishing Awareness	• *Describe any initiatives to raise awareness about phishing attacks.* Sometimes, we share among our employees information on such problems. • *How are employees educated on identifying and reporting phishing attempts?* *We sent awareness and/or warning emails.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Detail the use of firewalls and intrusion detection systems.* The IT company manages the network software, including firewall and such. They restrict incoming and outgoing data transfers (including downloads, email attachments, access to sites, etc) based on risk. • *How is network traffic monitored for anomalies?* Using dedicated software installed and managed by our IT contractor.
	Vulnerability Management	• *Explain how vulnerabilities in systems and applications are identified and addressed.* We don't do this directly, but the IT contractor installs updates regularly to keep the applications safe.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		• *How frequently are vulnerability assessments conducted?* -
Third-Party Security	**Vendor Risk Management**	• *How does your organization assess and manage cybersecurity risks associated with third-party vendors?* We don't do this. • *What criteria are used to evaluate the cybersecurity posture of vendors?* -
Mobile Device Management	**Mobile Security Policies**	• *Outline the policies in place for securing mobile devices.* We only use desktop computers. They are secured with username and password for each account. • *How are lost or stolen devices handled?* -
	BYOD (Bring Your Own Device) Policies	• *If applicable, describe policies related to employees using personal devices for work.* Our employees can bring devices at work, but they do not use them for work (just for personal use). • *How is security ensured in a BYOD environment?* -

Organization Information	**Industry Type/sector**	*Retail commerce*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Small (approx. 20 employments)*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Provide an overview of your organization's cybersecurity policy.* Our cybersecurity policy focuses on safeguarding sensitive data and maintaining up-to-date software. We also emphasize the use of strong passwords, encryption, and firewalls to protect our network and customer information. Regular updates and patches are applied to all systems to address vulnerabilities promptly. • *How frequently is the policy reviewed and updated?*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		The policy is reviewed and updated when there are significant changes in our infrastructure or legal environment.
	Governance Structure	• *Describe the governance structure for cybersecurity within your organization.* Cybersecurity governance is overseen by a designated IT manager, responsible for implementing and enforcing policies. • *Who is responsible for overseeing cybersecurity initiatives?* *The IT manager oversees cybersecurity independently without additional dedicated staff. Responsibilities may be shared among existing personnel as needed.*
	Compliance with Standards	• *List the cybersecurity standards or frameworks your organization adheres to.* We implemented various cybersecurity recommented best practices rather than specific standards, tailored to our specific business needs and constraints. • *How is compliance with these standards ensured?* *N/A*
Access Control and Authentication	**Access Management**	• *Explain how access to systems and data is managed.* Access to systems and data is managed through role-based access control. Each employee is granted specific access privileges based on their role. We enforce strong password policies. • *Are there role-based access controls in place?* Yes
	Authentication Methods	• *Describe the methods of user authentication employed in your organization.* User authentication is done with strong password policies. Employees are required to create complex passwords. We also use MFA for some critical systems • *Any use of multi-factor authentication?* Yes, via mobile app and one time codes.
Data Protection and Privacy	**Data Encryption**	• *Specify how sensitive data is encrypted.* We use LUKS and BitLocker for encripting stored data. Network data is encrypted using HTTPS and SCP.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		• *Is encryption employed both in transit and at rest?* *Yes*
	Data Backup	• *Outline your organization's data backup procedures.* Data backups procedures involve automated scheduled backups of critical data to an offsite locatiom. Ocasional manual tasks ensure the integrity of backups and cleanup of old backups. • *How frequently are backups performed, and where are they stored?* *Daily, first on a onsite NAS and then copied over off-site (in an OneDrive space).*
	Data Retention Policies	• *Describe your organization's policies on data retention.* Our data retention policy ensures data is kept for the required duration, aligning with legal and business requirements. • *How is obsolete or unnecessary data disposed of?* *Deletion of unnecessary data are conducted regularly to minimize storage costs and security risks.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *Provide an overview of your incident response plan.* We don't have suche plan. In the past, we addresed incidents (mostly phishing and spam) as they arise through ad-hoc measures. • *How often is the plan tested and updated?* N/A
	Security Monitoring	• *Explain how your organization monitors for security incidents.* Security monitoring in our organization involves up to date antivirus and periodic manual log reviews to identify and respond to potential security incidents. • *What tools or technologies are used for security monitoring?* *Antivirus (BitDefender)*
Employee Training and Awareness	**Training Programs**	• *Detail your organization's cybersecurity training programs for employees.* None. However, we provide basic security guidelines during onboarding. • *How is the effectiveness of training assessed?* *N/A*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Phishing Awareness	• *Describe any initiatives to raise awareness about phishing attacks.* Occasionally, the IT manager shares relevant information to enhance awareness. • *How are employees educated on identifying and reporting phishing attempts?* *The IT manger shares information (annotated screenshots) of recent attempts.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Detail the use of firewalls and intrusion detection systems.* In our organization, firewalls is used to block outgoing traffic to some dangerouse sites and block incomming traffic on various ports. Also, automated log monitoring (fail2ban) blocks IPs from attackers. • *How is network traffic monitored for anomalies?* Using logs and fail2ban
	Vulnerability Management	• *Explain how vulnerabilities in systems and applications are identified and addressed.* We perform regular software updates for the OS and applications in use. • *How frequently are vulnerability assessments conducted?* *Never.*
Third-Party Security	**Vendor Risk Management**	• *How does your organization assess and manage cybersecurity risks associated with third-party vendors?* We try to use software from well established vendors, which we aquire using trusted channels. • *What criteria are used to evaluate the cybersecurity posture of vendors?* *N/A*
Mobile Device Management	**Mobile Security Policies**	• *Outline the policies in place for securing mobile devices.* We require employees to have PIN, model or fingerprint activated. • *How are lost or stolen devices handled?* We don't have any policy for this. We didn't have such incident (yet).
	BYOD (Bring Your Own Device) Policies	• *If applicable, describe policies related to employees using personal devices for work.* Employees are allowed to use own mobile phones for work (phone calls, email access, etc). However, they can not install and run our applications on their devices.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		● *How is security ensured in a BYOD environment?* We provide a wifi network separated from office network.

2.2.6. Cybersecurity Best Practices Data Collection Finland

Organization Information	**Industry Type/sector**	*Education*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Large*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	● *Policy is published and available on the website, but it does not refer to any standard.* ● *Policy reviewed annually.* *Main headers in the policy are:* ● *Lawfulness, reasonableness and transparency* ● *Purpose binding* ● *Data minimization* ● *Accuracy of information* ● *Limiting data storage* ● *Data integrity and creativity* ● *The registrar's duty of proof*
	Governance Structure	● *The management team together with the university IT team have the responsibility to update and monitor. Ultimately top management is responsible for the cyber security.* ● *Each user register has its own responsible person.*
	Compliance with Standards	● *in accordance with data protection regulation of the European Union* ● *no published standard for the IT or cyber security related matters*
Access Control and Authentication	**Access Management**	● *Password protocols and Multi-Factor Authentication.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Authentication Methods	• *Multi-Factor Authentication*
Data Protection and Privacy	**Data Encryption**	• *Everyone's personal responsibility*
	Data Backup	• *Everyone's personal responsibility*
	Data Retention Policies	*GDPR related documents are dealt as per the data protection regulation of the European Union*
Incident Response and Security Monitoring	**Incident Response Plan**	*There is no such plan due to savings.*
	Security Monitoring	*No such monitoring due to savings.*
Employee Training and Awareness	**Training Programs**	*No training programs*
	Phishing Awareness	*No controls are available. Personnel send info for the IT department upon receiving phishing email and IT forwards the information for the staff.*
Network Security	**Firewall and Intrusion Detection Systems**	*Firewall is quite effectively guiding junk to trash. No details are available of the function of the firewall.*
	Vulnerability Management	*Not known.*
Third-Party Security	**Vendor Risk Management**	*Not applicable. No vendors are used normally.*
Mobile Device Management	**Mobile Security Policies**	*Same password and authentication protocols apply.* *Entering websites that may pose a risk is not allowed.* *Installation of apps is not restricted on the phone but is restricted on the personal computers.* *A lost telephone must be reported to the IT department.*
	BYOD (Bring Your Own Device) Policies	*Students use this option. Staff uses other network where personal computers are not allowed.*

	Industry Type/sector	*Offshore shipping company*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Organization Information		
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*large*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	*Strict policy exists.*
	Governance Structure	*Flow chart available.*
	Compliance with Standards	*Approaches to cyber risk management will be company and ship specific but should be guided by the requirements of relevant national, international and flag state regulations and guidelines.* *In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). This is as per the BIMCO guidelines for maritime actors.*
Access Control and Authentication	**Access Management**	*Password protocol. MFA.*
	Authentication Methods	*Multi-Factor Authentication.*
Data Protection and Privacy	**Data Encryption**	*No sensitive data is shared via emails unless absolutely necessary. If such data is shared, it is done using encrypted link that is opened using multifactor authentication.*
	Data Backup	*Not known. There is a cloud service to which the data is stored.*
	Data Retention Policies	*Not known. There is a cloud service to which the data is stored.*
Incident Response and Security Monitoring	**Incident Response Plan**	*Detailed response and reporting regimes are available.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Security Monitoring	*Constant monitoring is done on a global level.*
Employee Training and Awareness	**Training Programs**	*Mandatory generic cyber security training programme is available. This is accompanied by the unit-specific training that emphasizes subject applicable for the particular business unit.*
	Phishing Awareness	*Training and awareness news flashes.*
Network Security	**Firewall and Intrusion Detection Systems**	*Effective firewalls.*
	Vulnerability Management	*Risk management is done all the time.*
Third-Party Security	**Vendor Risk Management**	*Risk management is done and all computers used by vendors are contractor owned, not vendors computers.*
Mobile Device Management	**Mobile Security Policies**	*Same password and authentication protocols apply.* *Entering websites that may pose a risk is not allowed.* *Installation of apps is allowed.*
	BYOD (Bring Your Own Device) Policies	*Not applicable. Connecting private computers to any network is prohibited.*

Organization Information	**Industry Type/sector**	*Towing company*
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	*Medium*
Cybersecurity Policies and Governance	**Cybersecurity Policy**	*Policy exists but is not updated very effectively or regularly. The policy mostly exists to satisfy the need for the ISM auditing.*
	Governance Structure	*Not available.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Compliance with Standards	*Approaches to cyber risk management will be company and ship specific but should be guided by the requirements of relevant national, international and flag state regulations and guidelines.* *In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). This is as per the BIMCO guidelines for maritime actors.*
Access Control and Authentication	**Access Management**	*Password protocol. Some softwares used are accessible through Multi-Factor Authentication only.*
	Authentication Methods	*Multi-Factor Authentication, when applicable.*
Data Protection and Privacy	**Data Encryption**	*Not known.*
	Data Backup	*Not known. There is a cloud service to which the data is stored, but this service is available for the management team only.*
	Data Retention Policies	*Not known. There is a cloud service to which the data is stored.*
Incident Response and Security Monitoring	**Incident Response Plan**	*Only on the level of ISM code requirements.*
	Security Monitoring	*Reactive monitoring. As in, action is taken only when the incident is imminent. No preventive actions apart from very basic every household protocols.*
Employee Training and Awareness	**Training Programs**	*None used or existing.*
	Phishing Awareness	*None used or existing.*
Network Security	**Firewall and Intrusion Detection Systems**	*MS365 package provided.*
	Vulnerability Management	*Risk management for cyber security is not practiced.*
Third-Party Security	**Vendor Risk Management**	*All computers used by vendors are contractor owned, not vendors computers.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Mobile Device Management	**Mobile Security Policies**	*Same password and authentication protocols apply.* *Installation of apps is allowed.*
	BYOD (Bring Your Own Device) Policies	*Not applicable.*

2.2.7. Cybersecurity Best Practices Data Collection Spain

Organization Information	**Organization Name**	Company A
	Industry Type/SIZE	*Education / Large*
	Contact Person	
	Email	
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Security Policy following requirements of the Spanish National Security Framework (ENS)* • *Every 2 years minimum*
	Governance Structure	• *The organisation's Information Security Committee is responsible for overseeing cybersecurity initiatives*
	Compliance with Standards	• *National Security Framework (ENS)* • *Currently on the path to Certification (using an approved certifier)*
Access Control and Authentication	**Access Management**	• *Assign role access for users* • *Management and users*
	Authentication Methods	• *Access by credentials or two-factor authentication*
Data Protection and Privacy	**Data Encryption**	• *Use Google encryption and Owncloud encryption (AES)* • *Encryptioni n transit: TLS*
	Data Backup	• *Full and incremental backup* • *Full backup: annual; Incremental backup: diary. Stored on local computer and cloud.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

	Data Retention Policies	• *Annual, last 12 months, last four week, and last seven days.* • *Overwriting*
Incident Response and Security Monitoring	**Incident Response Plan**	• *There is a corporate IRP updated as major changes are detected.*
	Security Monitoring	• *Spanish and Catalonia CERT report security incidents and vulnerabilities* • *Several local systems are dedicated to monitor and report anomalies*
Employee Training and Awareness	**Training Programs**	• *Currently, we have a basic security training available for all users. Usage reported monthly to the CISO.*
	Phishing Awareness	• *Annual phishing test*
Network Security	**Firewall and Intrusion Detection Systems**	• *Global perimeter firewall and currently implementing inside perimeter*
	Vulnerability Management	• *Spanish and Catalonia CERT report us security incidents and vulnerabilities* • *Internal procedure resolves them (with required SLA)*
Third-Party Security	**Vendor Risk Management**	• *Vendor Risk Management performed as required by the ENS*
Mobile Device Management	**Mobile Security Policies**	• *Updating OS and Apps* • *How are lost or stolen devices handled?*
	BYOD (Bring Your Own Device) Policies	• *If applicable, describe policies related to employees using personal devices for work.* • *How is security ensured in a BYOD environment?*

Organization Information	**Organization Name**	*Company B*
	Industry Type/SIZE	*Financial Technology / Large Enterprise*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Company B has a comprehensive cybersecurity policy focusing on data protection, risk management, and regulatory compliance. The policy covers internal protocols, third-party vendor management, and customer data protection. It is reviewed quarterly to address emerging threats and regulatory requirements like the GDPR and PCI-DSS.*
	Governance Structure	• *The cybersecurity team is led by the Chief Information Officer (CIO) and supported by an internal audit team and an external consultancy firm. The board of directors receives quarterly cybersecurity updates.*
	Compliance with Standards	• *Company B adheres to PCI-DSS for payment processing and ISO 27001 for information security management. Annual compliance audits are conducted, and employees undergo cybersecurity certifications.*
Access Control and Authentication	**Access Management**	• *Access to systems is managed via identity and access management (IAM) software, ensuring permissions are aligned with employee roles. Access is restricted through the principle of least privilege, and regular access reviews are conducted.*
	Authentication Methods	• *Multi-factor authentication (MFA) is enforced for all system access, requiring a combination of password, fingerprint scanning, and token-based authentication.*
Data Protection and Privacy	**Data Encryption**	• *All sensitive customer and financial data is encrypted using 256-bit encryption protocols. Data in transit is protected with TLS, while data at rest is stored in encrypted databases.*
	Data Backup	• *Company B performs daily data backups, stored both on-premises and in encrypted cloud storage. Backup recovery tests are conducted monthly to ensure data integrity.*
	Data Retention Policies	• *Customer data is retained for a period of 10 years in compliance with legal requirements. After this period, data is securely deleted using certified methods.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *The incident response plan involves a dedicated team to detect, analyze, and respond to security breaches. It includes predefined roles for communication, containment, and recovery.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		Biannual drills simulate different types of cyberattacks.
	Security Monitoring	• *Company B uses a combination of Security Information and Event Management (SIEM) systems and artificial intelligence to monitor network traffic, detect anomalies, and provide real-time alerts.*
Employee Training and Awareness	**Training Programs**	• *Employees are required to attend monthly training sessions on cybersecurity best practices, including phishing and ransomware prevention. Assessments are conducted through quizzes and simulated cyberattacks.*
	Phishing Awareness	• *Company B runs quarterly phishing simulations to assess employee readiness. Employees who fall victim are required to undergo additional cybersecurity training.*
Network Security	**Firewall and Intrusion Detection Systems**	• *Next-generation firewalls (NGFW) and intrusion detection systems (IDS) are deployed to safeguard the network. Company B also utilizes AI-driven systems to detect and respond to potential threats in real-time.*
	Vulnerability Management	• *The IT security team performs bi-weekly vulnerability assessments using automated scanning tools. Critical patches are deployed within 24 hours of discovery.*
Third-Party Security	**Vendor Risk Management**	• *Company B rigorously evaluates third-party vendors using a risk-based approach. Vendors must meet specific cybersecurity criteria and are audited yearly for compliance.*
Mobile Device Management	**Mobile Security Policies**	• *All mobile devices accessing company data are secured using mobile device management (MDM) software. This includes encryption, remote lock, and wipe capabilities.*
	BYOD (Bring Your Own Device) Policies	• *Company B has strict policies in place to manage employee-owned devices. Personal devices used for work must adhere to security guidelines, including the installation of anti-malware and VPN software.*

Organization Information	**Organization Name**	*Company C*
	Industry Type/SIZE	*Healthcare Technology / Medium-sized Enterprise*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Company C enforces a data-centric cybersecurity policy with a focus on patient data protection, aligned with GDPR and healthcare-specific regulations (e.g., ISO 27799). The policy is updated twice a year and after major security incidents.*
	Governance Structure	• *The cybersecurity governance structure is led by the Data Protection Officer (DPO), who collaborates with the IT Security team. The executive board is responsible for cybersecurity oversight and risk management.*
	Compliance with Standards	• *Company C adheres to GDPR for data privacy and ISO 27001 for security management. Compliance is ensured through quarterly audits and employee training on data protection policies.*
Access Control and Authentication	**Access Management**	• *Company C uses a role-based access control (RBAC) model to limit access to sensitive healthcare data. Access is granted only to authorized personnel, with periodic access reviews to ensure compliance.*
	Authentication Methods	• *Multi-factor authentication (MFA) is mandatory for all employees accessing patient records or critical systems. It combines password authentication with biometric verification or one-time tokens.*
Data Protection and Privacy	**Data Encryption**	• *Patient data is encrypted both at rest and in transit using AES-256 encryption standards. Company C also employs encryption tools to ensure secure communication with healthcare providers.*
	Data Backup	• *Data is backed up daily and stored on secure servers within Spain. Regular tests are conducted to ensure the reliability of backup systems, and offsite backups are encrypted.*
	Data Retention Policies	• *Patient data is retained for 15 years as per Spanish healthcare regulations. Once this period expires, data is securely destroyed using digital shredding techniques.*
Incident Response and Security Monitoring	**Incident Response Plan**	• *The incident response plan covers detection, containment, and recovery from cybersecurity incidents. It includes specific protocols for handling breaches of patient data. Annual tabletop exercises are conducted to test the plan.*
	Security Monitoring	• *Company C uses a 24/7 security operations center (SOC) and advanced SIEM systems to*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		monitor for potential security threats. Anomaly detection is performed using AI-based tools.
Employee Training and Awareness	**Training Programs**	• *Employees receive cybersecurity training tailored to healthcare-specific threats, including ransomware and data breaches. The training is conducted biannually, and its effectiveness is measured through follow-up assessments.*
	Phishing Awareness	• *Regular phishing tests are conducted, with employees encouraged to report suspicious emails. Additional awareness workshops are provided for staff in high-risk positions (e.g., those handling patient data).*
Network Security	**Firewall and Intrusion Detection Systems**	• *Firewalls and intrusion detection systems are used to secure the network perimeter. Continuous monitoring of incoming and outgoing traffic ensures protection against cyber threats.*
	Vulnerability Management	• *Company C performs monthly vulnerability scans and ensures that critical security patches are applied immediately after discovery. Security updates are monitored through automated systems.*
Third-Party Security	**Vendor Risk Management**	• *Third-party vendors are required to comply with Company C's cybersecurity policies. Vendors undergo a thorough risk assessment before onboarding, and regular reviews ensure adherence to cybersecurity standards.*
Mobile Device Management	**Mobile Security Policies**	• *Mobile devices used to access patient data are protected using encryption and secured through MDM software. Remote wipe capabilities are enabled to ensure data security in case of loss or theft.*
	BYOD (Bring Your Own Device) Policies	• *Employees using personal devices must install the company's security software, which includes anti-malware, encryption, and remote monitoring tools. Access to patient data is restricted on personal devices unless approved by IT security.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

2.3. Proposal for Cybersecurity Best Practices in the Maritime Sector

The maritime sector, like many others, is increasingly reliant on digital systems to enhance operational efficiency, safety, and navigation. However, this growing dependence on technology also presents heightened risks related to cybersecurity threats. By analyzing the cybersecurity best practices from companies in sectors like fintech and healthcare in Spain, we can extract key lessons and adapt them to fit the specific needs of the maritime industry.

Analysis of Best Practices

1. **Cybersecurity Policies and Governance**
    - The maritime industry should adopt similar policy structures, including compliance with international regulations such as **IMO's (International Maritime Organization) Guidelines on Maritime Cyber Risk Management**, **ISO 27001**, and **NIST** standards. Policies should be frequently updated to account for evolving cyber risks in maritime environments, such as those targeting **Shipboard Operational Technology (OT)** and **Navigation Systems**.
2. **Governance Structure**
    - Maritime organizations should establish clear cybersecurity governance by appointing a **Chief Information Security Officer (CISO)** or a cybersecurity officer within the IT or safety department. The governance team should work closely with vessel operators and technicians to ensure operational and cybersecurity alignment.
3. **Access Control and Authentication**
    - The maritime sector must adopt similar access control mechanisms to protect shipboard systems and shore-based control centers. Only authorized personnel should have access to critical systems like navigation, propulsion, and cargo management systems. **MFA** should be mandatory, combining passwords, security tokens, or biometric verification.
4. **Data Protection and Privacy**
    - Encryption should be used for all data, including vessel-to-shore communication and internal ship systems, to prevent unauthorized interception or tampering of sensitive data (e.g., cargo data, passenger records, and ship navigation details). Encryption is essential for protecting data stored in **Electronic Chart Display and Information Systems (ECDIS)**, **Automatic Identification Systems (AIS)**, and satellite communication systems.
5. **Incident Response and Security Monitoring**
    - Vessels and maritime facilities should have an incident response plan that includes predefined steps for identifying, mitigating, and reporting cyberattacks. Frequent

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

drills and exercises must simulate cyberattacks, such as ransomware, phishing, or OT sabotage. **SIEM systems** and continuous monitoring tools should be employed to detect anomalies in real time on vessels and shore-based systems.

6. **Employee Training and Awareness**
    - The maritime sector should train seafarers and shore-based staff on recognizing cyber threats, including phishing, ransomware, and social engineering. Awareness initiatives like simulated phishing attacks should be conducted regularly, especially for employees responsible for onboard critical systems and communication with shore facilities.
7. **Network Security**
    - The maritime industry should deploy similar security tools for vessels' operational and administrative networks. Firewalls, IDS, and **AI-based anomaly detection** should be used to monitor communication between onboard systems, shore-based centers, and third-party vendors. Continuous monitoring of traffic ensures real-time detection of unauthorized access attempts.
8. **Vulnerability Management**
    - The maritime sector should conduct regular vulnerability assessments on both OT and IT systems aboard ships, port infrastructure, and communication systems. Patching known vulnerabilities in **navigation systems**, **cargo management software**, and **satellite systems** must be a top priority, especially for critical components that could be exploited for operational disruption or hijacking.
9. **Third-Party Security**
    - Maritime organizations should assess and manage cybersecurity risks related to third-party vendors, such as software providers, satellite communication services, and maintenance contractors. Vendors handling critical ship systems should be required to comply with **IMO** cyber risk guidelines, and regular security audits should be performed.
10. **Mobile Device Management and BYOD Policies**
    - The maritime sector should enforce policies that secure mobile devices used on ships, including tablets and smartphones for navigation or communication. **MDM software** should enforce encryption and remote wipe capabilities. BYOD policies should be implemented cautiously, requiring strict security measures like encrypted connections and restricted access to sensitive systems.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

2.4. Proposal for Tailored Cybersecurity Framework for the Maritime Sector

Based on the practices mentioned above, the following cybersecurity framework is proposed for the maritime industry:

1. **Cybersecurity Policy & Governance:**
    - Develop a maritime-specific cybersecurity policy aligned with **IMO**, **NIST**, and **ISO 27001** standards.
    - Create a governance structure with a dedicated **CISO**, responsible for monitoring both IT and OT environments on vessels and shore facilities.
2. **Access Control & Authentication:**
    - Implement **Role-Based Access Control (RBAC)** and **Multi-Factor Authentication (MFA)** for critical onboard systems, like **ECDIS**, **AIS**, and propulsion systems.
    - Regular audits should be performed to review and adjust access permissions.
3. **Data Protection & Encryption:**
    - Enforce **AES-256 encryption** for all maritime communication, including **ship-to-shore** and internal network communication.
    - Ensure encryption for both **in-transit** and **at-rest** data, particularly for navigation and cargo management systems.
4. **Incident Response & Security Monitoring:**
    - Develop a robust **Incident Response Plan (IRP)** specific to maritime environments. Test the IRP through regular cyberattack simulations.
    - Use **SIEM tools** for continuous monitoring and detection of anomalies on both onboard and shore-based systems.
5. **Employee Cybersecurity Training:**
    - Conduct regular cybersecurity training for seafarers, emphasizing phishing, ransomware, and network breaches.
    - Run quarterly phishing simulations and assessments to reinforce cybersecurity awareness among all employees.
6. **Network Security:**
    - Deploy **Next-Generation Firewalls (NGFW)** and **Intrusion Detection Systems (IDS)** for all vessels and port infrastructures.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

- Use **AI-powered anomaly detection** to monitor traffic patterns and detect potential intrusions in real time.

7. **Vulnerability Management:**
   - Perform regular vulnerability assessments of OT systems, including **SCADA**, **cargo management**, and **navigation systems**.
   - Patch high-risk vulnerabilities within 24-48 hours to prevent cyberattacks on critical maritime infrastructure.
8. **Third-Party Vendor Security:**
   - Conduct annual cybersecurity audits of all third-party vendors and contractors handling critical maritime systems.
   - Ensure that vendors comply with the maritime industry's cybersecurity policies, including **IMO** guidelines and **ISO standards**.
9. **Mobile Device Management (MDM) & BYOD Policies:**
   - Implement **MDM software** on all mobile devices used for shipboard operations and communication.
   - Strictly enforce encryption, VPN access, and remote wipe capabilities for any personal devices used on board.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

3. Conclusion

By implementing these cybersecurity best practices adapted from leading industries like fintech, education, construction, finance, technology, security and healthcare, the maritime sector can strengthen its defences against ever-evolving cyber threats. This proposal ensures the protection of operational systems, sensitive data, and personnel through comprehensive policies, robust monitoring, regular employee training, and secure vendor management.

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Appendix

A.1. Data Collection Template

Organization Information	**Industry Type/sector**	
	Organization Size (very small <10 persons, small <50 persons, medium <250 persons, large >250 persons)	
Cybersecurity Policies and Governance	**Cybersecurity Policy**	• *Provide an overview of your organization's cybersecurity policy.* • *How frequently is the policy reviewed and updated?*
	Governance Structure	• *Describe the governance structure for cybersecurity within your organization.* • *Who is responsible for overseeing cybersecurity initiatives?*
	Compliance with Standards	• *List the cybersecurity standards or frameworks your organization adheres to.* • *How is compliance with these standards ensured?*
Access Control and Authentication	**Access Management**	• *Explain how access to systems and data is managed.* • *Are there role-based access controls in place?*
	Authentication Methods	• *Describe the methods of user authentication employed in your organization.* • *Any use of multi-factor authentication?*
Data Protection and Privacy	**Data Encryption**	• *Specify how sensitive data is encrypted.* • *Is encryption employed both in transit and at rest?*
	Data Backup	• *Outline your organization's data backup procedures.*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

		• *How frequently are backups performed, and where are they stored?*
	Data Retention Policies	• *Describe your organization's policies on data retention.* • *How is obsolete or unnecessary data disposed of?*
Incident Response and Security Monitoring	**Incident Response Plan**	• *Provide an overview of your incident response plan.* • *How often is the plan tested and updated?*
	Security Monitoring	• *Explain how your organization monitors for security incidents.* • *What tools or technologies are used for security monitoring?*
Employee Training and Awareness	**Training Programs**	• *Detail your organization's cybersecurity training programs for employees.* • *How is the effectiveness of training assessed?*
	Phishing Awareness	• *Describe any initiatives to raise awareness about phishing attacks.* • *How are employees educated on identifying and reporting phishing attempts?*
Network Security	**Firewall and Intrusion Detection Systems**	• *Detail the use of firewalls and intrusion detection systems.* • *How is network traffic monitored for anomalies?*
	Vulnerability Management	• *Explain how vulnerabilities in systems and applications are identified and addressed.* • *How frequently are vulnerability assessments conducted?*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793

Third-Party Security	**Vendor Risk Management**	• *How does your organization assess and manage cybersecurity risks associated with third-party vendors?* • *What criteria are used to evaluate the cybersecurity posture of vendors?*
Mobile Device Management	**Mobile Security Policies**	• *Outline the policies in place for securing mobile devices.* • *How are lost or stolen devices handled?*
	BYOD (Bring Your Own Device) Policies	• *If applicable, describe policies related to employees using personal devices for work.* • *How is security ensured in a BYOD environment?*

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
Project Number: 2023-1-ES01-KA220-VET-000159793