SILVERSEA

Above and Beyond All Expectations℠

Vessel Management System

Maritime Cyber Security

Table of Contents

1 Overview

1.1 Background

The term “maritime cyber risk” refers to a measure of the extent to which a technological asset could be threatened by a potential circumstance or event, which can lead to operational, safety or security failures related to the shipment as a result of damage, corruption or loss of information or systems.
The Cyber risk management includes the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.
The final goal is to support safe and secure shipping, which is operationally resilient to cyber risks.

1.2 IMO Guidance

IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management.
The guidelines drafted provide high-level recommendations on maritime cyber risk management to safeguard shipping from existing and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations given can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.
The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Vessel Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing Vessel Management Systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

1.3 Other Guidance, Standards and Framework

Guidelines on Cyber Security on-board Ships issued by BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI and WORLD SHIPPING COUNCIL.

ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).

2 Introduction

2.1 Purpose and Applicability

The policy manual provides direction for consistent operations and continual improvement, fleet wide and ashore. This document provides High-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The policy manual is applicable to all the vessels in the fleet.

2.2 Definition

For the purpose of this document:

- ***Access Control*** is the process that limits and controls access to resources of a computer system.
- ***Cyber Risk Management*** refers to identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken
- ***Firewall*** is a logical or physical break designed to prevent unauthorised access to IT infrastructure and information.
- ***Information Technology*** (IT) covers the spectrum of technologies for data storing and processing, including software, hardware, and communication technologies.
- ***Malware*** refers to a malicious software, which is designed to access or damage a computer without the knowledge of the owner.
- ***Maritime Cyber Risk*** measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised
- ***Operational technology*** (OT) includes hardware and software that directly monitors/controls physical devices and processes, typically on-board.
- ***Patches*** are software designed to update software or supporting data to improve the software or address security vulnerabilities and other bugs in operating systems or applications.
- ***Removable media*** is a collective term for all methods of storing and transferring data between computers. This includes laptops, USB memory sticks, CDs, DVDs, and diskettes.
- ***Risk assessment*** is the process which collects information and assigns values to risks as a base on which to make decision on priorities and developing or comparing courses of action.
- ***Shipboard Computer System*** describes any computer hardware and/or software program used as part of the on-board standard equipment, or supplied third party to facilitate the ship's management, or any other task.
- ***Third party*** refers to suppliers, consultants and business partners doing business with Company, and other partners that have a need to exchange information with Company.
- ***Threats*** refer to malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions).

In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology

- ***Virtual Private Network*** (VPN) enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, thereby benefiting from the functionality, security and management policies of the private network.
- ***Virus*** is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer programme or system.
- ***Vulnerabilities*** is the result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber-discipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised
- ***Wi-Fi*** is all short-range communications that use some type of electromagnetic spectrum to send and/or receive information without wires.

2.3 Responsibilities

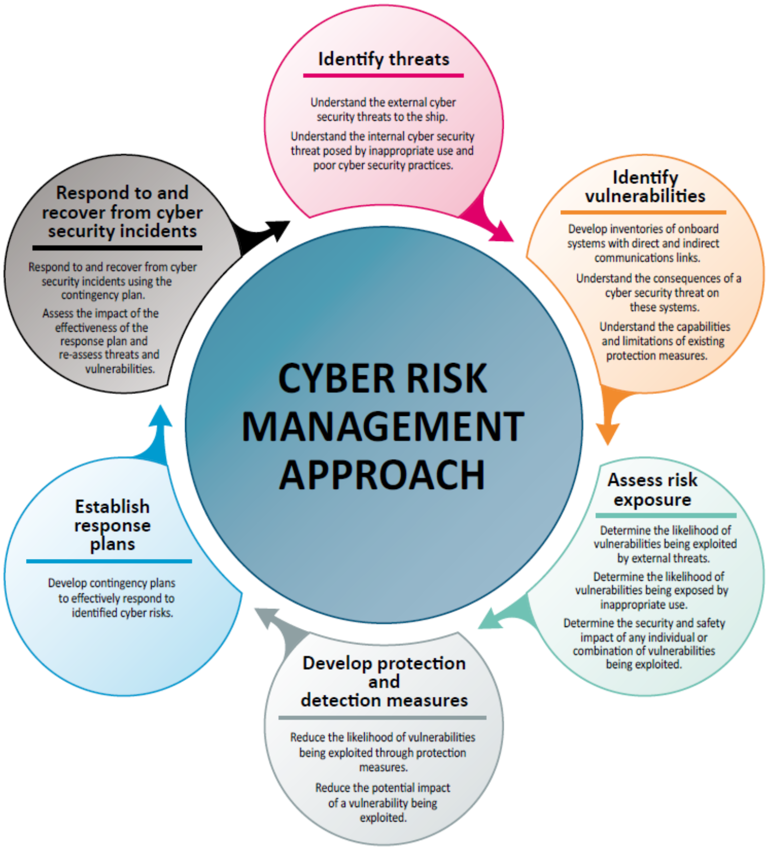
It is every employee's responsibility to follow company policies and procedures. Officers and above should be knowledgeable regarding VMS Policy and Guidance as it applies to their position, duties, and work/supervisory responsibilities. They should also ensure their employees receive orientation and are properly trained and instructed on the contents of VMS manual applicable to their work area of responsibilities. Specifically:

- The Master is responsible for cyber safety on-board:
  - Ensuring that all cyber security policies and procedures are adhered
  - Any cyber related incidents are reported (see chapter ***"4.4 Information Security Incident Management"***)
  - Ensuring all crew operate and following cyber safety training and instruction (see chapter ***"3.7 Training & Awareness"***)
  - Complete the Cyber Security Checklist periodically (see chapter ***"3.6 Risk Evaluation"***)
  - Maintain the Vessel IT Risk Assessment (see chapter ***"3.6 Risk Evaluation"***)
  - Conduct Vessel IT Audit periodically (see chapter ***"3.6 Risk Evaluation"***)
- The Master (through IT Officer/ ETO) is responsible for ensuring all computer users:
  - Fully understand these instructions
  - Are fully conversant with the instruction manuals
  - Where appropriate, are fully conversant with Company instructions relating to specific programs

3 Implementing Safety and Risk Management

3.1 Cyber-Risk Based Management Process

This procedure presents the functional elements that support effective cyber risk management. These functional elements are not sequential – but concurrent and continuous in practice and incorporated appropriately in a risk management framework.



CYBER RISK MANAGEMENT APPROACH

Identify threats

Understand the external cyber security threats to the ship.

Understand the internal cyber security threat posed by inappropriate use and poor cyber security practices.

Identify vulnerabilities

Develop inventories of onboard systems with direct and indirect communications links.

Understand the consequences of a cyber security threat on these systems.

Understand the capabilities and limitations of existing protection measures.

Assess risk exposure

Determine the likelihood of vulnerabilities being exploited by external threats.

Determine the likelihood of vulnerabilities being exposed by inappropriate use.

Determine the security and safety impact of any individual or combination of vulnerabilities being exploited.

Develop protection and detection measures

Reduce the likelihood of vulnerabilities being exploited through protection measures.

Reduce the potential impact of a vulnerability being exploited.

Establish response plans

Develop contingency plans to effectively respond to identified cyber risks.

Respond to and recover from cyber security incidents

Respond to and recover from cyber security incidents using the contingency plan.

Assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.

Figure 1. *Cyber risk management approach as set out in the guidelines* – Guidelines on Cyber Security On-board Ship v4

The following procedure must be followed:

Identify

a) Personnel roles and responsibilities of users, key personnel and management for cyber risk management

b) Vulnerable/critical systems, assets, data and capabilities that when disrupted, pose risk to ship operations and safety

- See section **"Asset Inventory"** of chapter ***"3.3 Identify Vulnerabilities"***

c) Threats and vulnerabilities that could pose a cyber-risk / event

- See chapter ***"3.3 Identify Vulnerabilities"***
- See example of **potential threats actors**:

Group	Motivation
Accidental actors	▪ No malicious motive but still end up causing unintended harm through bad luck, lack of knowledge or lack of care, e.g. by inserting infected USB in on-board IT or OT systems.
Activists (including disgruntled employees)	▪ Revenge ▪ Disruption of operations ▪ Media attention ▪ Reputational damage
Criminals	▪ Financial gain ▪ Commercial espionage ▪ Industrial espionage
Opportunists	▪ The challenge ▪ Reputational gain ▪ Financial gain
States **State sponsored organizations** **Terrorists**	▪ Political/ideological gain e.g. (un)controlled disruption to economies and critical ▪ National infrastructure ▪ Espionage ▪ Financial gain ▪ Commercial espionage ▪ Industrial espionage ▪ Commercial gain

Table 1. *Threat actors' motivation and objectives* - Guidelines on Cyber Security On-board Ship v.4

- See example of **potential threats** (the list provide examples, bit is not exhaustive):

Name	Description
Malware	▪ Malicious software, which is designed to access or damage a computer without the knowledge of the owner.
Water holing	▪ Establishing a fake website or compromising a genuine website to exploit ▪ unsuspecting visitors.

Scanning	▪ Searching large portions of the internet at random for vulnerabilities that could be exploited.
Typosquatting	▪ Also called URL hijacking or fake URL. Relies on mistakes such as typos made by internet users when inputting a website address into a web browser.
Targeted attacks	May be more sophisticated and use tools and techniques specifically created for targeting a certain company or ship. Examples of tools and techniques, which may be used in these circumstances, include: ▪ Social engineering ▪ Brute force ▪ Credential stuffing ▪ Denial of service (DoS) ▪ Phishing ▪ Spear-phishing ▪ Subverting the supply chain.

Table 2. *Potential Threat* - Guidelines on Cyber Security On-board Ship v.4

Protect

a) Implement technical measures against a cyber-event addressing the identified threats and vulnerabilities:

- Configure networks (see section ***Network Security Manager*** of chapter ***“4.5 Communication and Operation Management”***)
- Control access to networks and systems
- Defend communication and boundaries

b) Plan for contingencies to ensure continuity of shipping operations for failures/losses of critical equipment and data such as:

- Electronic navigational equipment
- External data sources including but not limited to GNSS (GPS)
- Connectivity to shore including but not limited to GMDSS
- Control systems including propulsion and auxiliaries

c) Treat any loss of IT/OT (Operational Technology) system same as any other equipment failure

d) Keep Contingency Plans and related information available in a non-electronic form

Detect

a) Develop and implement technical activities to detect a cyber-event in a timely manner:

- Use protection and detection software
- Administrator profiles given only to senior officers
- Direct alerts to responsible personnel

Respond

a) Develop procedural activities and plans to provide resilience against cyber –events:

- Training and awareness (see chapter *"3.7 Training and Awareness"*)
- Maintain / upgrade software (see chapter *"4.5 Communication and Operation Management"*)
- Equipment disposal policies if containing sensitive data
- Control access to the on-board systems for visitors and during drydocks, layups or when taking over a new/existing ship

b) Implement the above to restore impaired systems necessary for operations

Recover

a) Identify measures to back-up cyber systems necessary for impaired shipping operations (see section **Backup** of chapter *"4.5 Communication and Operation Management"*)

b) Restore above systems

c) Investigate cyber-vents as incidents

3.2 Standing Instruction

These instructions details the Company's requirements for the on-board use and management of computer systems. Computers supplied to the vessel by the Owner, or third parties are supplied to facilitate on-board management tasks. These computers are normally provided with the software pre-loaded and configured for use on-board the vessel. Misuse of shipboard computer systems must be avoided as it can result in:

- Loss of functions
- Delays to the vessel
- Expensive repairs
- Threats to environment, property or life

The equipment included in the shipboard computer systems is wide ranging. It included but is not limited to:

- Stability computer
- Pax and crew management computer
- Engine management systems computer
- Alarm/performance monitoring computer
- Any other engine room based computer system
- Navigation computer
- ARPA/radar computer system
- Electronic navigation, Charting and position systems
- Communications computers

- Any other navigational computer based system
- Shipboard servers
- Any Computer workstations, laptop, thin client terminals and tablets, supplied to the vessel by the Owner, Manager or third party for any purpose.

Old computer systems present a serious cyber risk as they can provide vulnerabilities targeted by malware and cyber attacks. To maintain full product support and system updates compatibility, there must be in place budget provision for shipboard computer systems to be replaced on average within their 4th year of service. This will include for replacement of any manufacturer End of Support software. e.g. Operating Systems, Anti-Virus software etc.
The Company will undertake periodical inspections of shipboard computer systems, to confirm that these instructions are being complied with.

It is in breach of the companies operating procedures:

- Use as personal computers.
- Attempt to connect any personal electronic devices to the ships network, or any other computer systems that are part of the ships business or operational systems, for example connecting a dedicated loading computer to the network.
- Attempt to connect any personal electronic devices to the ships communication terminals any direct method for example into VSAT/FBB terminals, Modems or networking components. Where permitted pax and crew personal computers or portal devices may be connected to a pax and crew Wi-Fi or dedicated pax and crew network with express permission of the Master as advised by the company.
- Attempt to install any other software application on a computer system which has not been authorised by the Company.
- Attempt to enter the set-up parameters of a computer. If a user has inadvertently entered the set-up programme, it is required to follow the incident management procedure (see chapter ***"4.4 Information Security Incident Management"***)
- Use the master or any other disks containing program files to re-install shipboard software applications without prior permission from the Company.
- Reformat or copy files onto master disks or any other disk containing programmes files.
- Use utility software (e.g. Disk managers, Memory makers/managers, Shell Environment, Anti-virus)

Removable Media

Viruses are often spread through portable media such as external USB data devices, CD-ROMs and other removable media. To reduce the spread of email viruses, personnel should avoid connecting external USB data devices or CD ROMs to equipment (see also section **Information Transfer** of chapter ***"4.5 Communication and Operation Management"***).

Handover

The Masters (through IT Officer/ ETO) must confirm the following in their handover notes:

- The purpose and condition of each computer system (confirming that the equipment has been properly secured).

- Ensure that the joining IT Officer is fully instructed regarding the Company's requirements for the use of these computer systems.
- Ensure that the joining IT Officer changes the password of the shared user account assigned at the first log-in.
- Confirmation that the officers using the system has been clearly advised to give the relief officers full instruction on the computer use.

System Support

The IT Vessel Support team will provide assistance to vessels with problems concerning shipboard computer based systems.
Note: All problems/calls received from vessels are logged and documented in the IT Helpdesk system and assigned to a member of the core team who can then re-allocate to the split role engineers, if relevant.

Updates and resolutions of helpdesk tickets are emailed to the ship via the helpdesk system.

3.3 Identify Vulnerabilities

To identify the vulnerabilities, an analysis of the applications, systems, and procedures is carried out by the Application Owner in conjunction with the IT Department (that is also responsible of all systems managed directly by the IT e.g. network, firewalls, servers, …) to uncover weaknesses that might be leveraged by potential threats (see section ***Identify*** in chapter *"3.1 Cyber-Risk Based Management Process"*).
The goal of the ship's network and its systems and devices assessment is to identify any vulnerabilities that might compromise or result in the loss of confidentiality, integrity or availability of data and systems required to operate the equipment, system, network, or even the ship. Example of vulnerabilities and weaknesses categories:

- Temporary exposures such as software defects, outdated or unpatched systems
- Design such as access management or unmanaged network interconnections
- Implementation errors for example misconfigured firewalls
- Procedural or other user errors

Common Vulnerabilities
Common cyber vulnerabilities which may be found on-board existing/new build ships:

- Unsupported and obsolete operating systems
- Unpatched system software
- Missing or outdated antivirus software and protection from malware
- Inadequate security configurations and best practices, including ineffective network management and the of default administrator accounts and passwords
- Shipboard computer networks, which lack boundary protection measures and segmentation of networks
- Safety critical equipment or systems always connected with the shore side

- Inadequate access controls to cyber assets, networks for third parties including contractors and service providers
- Staff inadequately trained and/or skilled to manage cyber risks
- Missing, inadequate or untested contingency plans and procedures.

Asset Inventory
An **asset inventory**, is regularly updated as to list all the IT and OT systems identified (see chapter **"4.2 Asset Management"**).

3.4 Assessing the likelihood

The **likelihood** of a cyber security event happening is the product of the threat and the vulnerability. Here the scale adopted:

Likelihood	Meaning	Value
Very frequent	Likely to occur multiple times (has occurred very frequently)	6
Frequent	Likely to occur many times (has occurred frequently)	5
Occasional	Likely to occur sometimes (has occurred infrequently)	4
Remote	Unlikely to occur, but possible (has occurred rarely)	3
Improbable	Very unlikely to occur (not known to have occurred)	2
Extremely improbable	Almost inconceivable that the event will occur	1

Table 3. *Likelihood*

3.5 Impact Assessment

The impact assessment is carried out by the Application Owner in conjunction with the IT Department (that is also responsible of all systems managed directly by the IT e.g. network, firewalls, servers, …) for every system on-board. For OT systems, the impact assessment include also the equipment and technical systems, the sudden operational failure of which may more or less promptly result in hazardous situations.
As well, the potential impact for IT systems is assessed with the support of the primary users/owner applications. Consequences of a degrading or loss of IT systems can be very disruptive to the ship's operations, regulatory compliance and even safety performance and should not be underestimated.
Here the impact scale adopted:

Level	Severity	Impact Description
1	Minor	Can operate safely without, would have **minor** impact on: safety, loss of data, health effect/injuries, environment, assets, finances, or to company's reputation.

2	Moderate	Would have a **moderate** impact on: safety, loss of data, health effect/injuries, environment, assets, finances, or to company's reputation.
3	Severe	Would have **severe** impact on: safety, loss of data, health effect/injuries, environment, assets, finances, or to company's reputation.
4	Major	Would have **major**, but local, impact on: safety, loss of data, health effect/injuries, environment, assets, finances, or to company's reputation.
5	Critical	Would have **critical**, and widespread, impact on: safety, loss of data, health effect/injuries, environment, assets, finances, or to company's reputation.
6	Disastrous	Would have **disastrous**, fatal or permanent, impact on: safety, loss of data, health effect/injuries, environment, assets, finances, or to company's reputation.

Table 4. *Impact Description*

3.6 Risk Evaluation

The Master is required to verify that a Vessel IT Risk Assessment is carried out by the Application Owner in conjunction with the IT Department and maintained on-board periodically (or if there is change to computer based systems). This is done using the **Silversea Vessel_IT_RA**. Risk assessments apply to existing ships as well as new-builds and second-hand ships entering the fleet. Therefore a specific risk assessment is required for each different vessels.
The risk assessment is carried out system by system and is therefore based on the system documentation described in chapter *"3.5 Impact Assessment"*.
To calculate the risk for a given system, the likelihood and the impact should be assessed:

Likelihood (scale 1 – 6)

6	**6**	**12**	**18**	**24**	**30**	**36**
5	**5**	**10**	**15**	**20**	**25**	**30**
4	**4**	**8**	**12**	**16**	**18**	**24**
3	**3**	**5**	**9**	**12**	**15**	**18**
2	**2**	**4**	**5**	**8**	**10**	**12**
1	**1**	**2**	**3**	**4**	**5**	**6**
	1	**2**	**3**	**4**	**5**	**6**

Impact (scale 1 – 6)

Risk Score Matrix (scale 1-36)

Risk Score	Description
From 20,1 to 36	**Extreme**
From 12,1 to 20	**High**
From 6,1 to 12	**Medium**
From 1 to 6	**Low**

The activities performed during the assessment include also specific audit campaigns to review the configuration of all computers, servers, routers, and cyber security technologies including firewalls. It could also include reviews of all available cyber security documentation and procedures for connected IT and OT systems and devices.

The principal purpose of this audit is to:

- Identify each piece of Computer Equipment or Systems on-board the vessels
- Identify cyber risk associated with the equipment
- Allow risk mitigation steps to be provided

The report will be treated as an inspection report to ensure that:

- the equipment is managed under this policy
- Cyber Security guidelines are followed.

▶▶ See - Silversea Vessel IT RA

Furthermore, to provide an objective review of the vessel's cyber security awareness. The **Cyber Security Checklist** should be completed by the Master periodically and any issues reported your vessel control group immediately.

▶▶ See - IT 03 Cyber Security Checklist

3.7 Training & Awareness

An appropriate level of awareness of cyber risks at all levels on-board (and ashore) should be ensured as appropriate to roles and responsibilities (see also chapter ***"2.3 Responsibilities"***). Training and awareness are key supporting elements to an effective approach to cyber risk management.

Personnel have a key role in protecting IT and OT and must be trained to pay attention on how the perform their daily activities that involve the use of systems.

A formalized training and awareness program should be tailored to the appropriate levels for:

- on-board personnel (Master, officers, and crew);
- shore side personnel, who support the management, loading, stowage and operation of the ship.

New hired personnel is provided with guidelines to enhance awareness on the following topic:

- risks related to emails and how to behave in a safe manner against phishing attacks (see section **Email**);
- risks related to internet usage (including social media and chat);
- risks related to geolocation data (publicly available data);
- risks related to the use of own devices (see chapter *"3.2 Standing Instruction"*);
- risks related to installing and maintaining software on company hardware (see chapter *"3.2 Standing Instruction"*);
- risks related to poor software and data security practices, where no anti-virus checks, or authenticity verifications are performed;
- risk related to removable media and data transferring between systems (see section **Removable Media** of chapter *"3.2 Standing Instruction"* and section **Information Transfer** of chapter *"4.5 Communication and Operation Management"*);
- safeguarding user information, passwords and digital certificates (see section **Password Policy** of chapter *"4.1 Access Control"*);
- cyber risks in relation to the physical presence of non-company personnel (e.g. where third party technicians are left to work on equipment without supervision);
- detecting suspicious activity or devices and how to report a possible cyber incident (see chapter *"4.4 Information Security Incident Management"*);
- awareness of the consequences or impact of cyber incidents to the safety and operations of the ship;
- understanding how to implement preventative maintenance routines such as anti-virus and antimalware, patching, backups, and incident-response planning and testing.

Email

Prevent virus outbreaks and spam

Viruses are often spread through email and instant messaging, reduce the spread of email viruses by:

- only opening email only from trusted sources;
- only open attachments you're expecting;
- do not open unsolicited, but if you do, do not click on web links in the message unless it is from a trusted vendor;
- if you know that a mail is junk, spam or fraudulent delete without reading;
- do not forward virus hoaxes or chain messages, these are simply spam in another guise and should be deleted on receipt;
- non-solicited e-mail of any type should be deleted without opening;
- any offensive material should be reported;
- any "virus warnings" received from third parties should be referred to local IT team staff and not forwarded to any other recipients.

While emails are normally automatically filtered for viruses and by type of attachments, potentially some messages will get through. If you are unsure about opening an attachment, please forward it to helpdesk unopened and request assistance.

Avoid publishing your company or vessel-mail email address on websites or submitting it to every site or organization that requests it. You company address is for business e-mail only please do not use it for personal purposes.

Do not subscribe to websites and newsletters that you are unsure of or that do not have a business purpose.

Avoid phishing attacks

Phishing scams are designed to steal user personal information. They often use doctored and fraudulent email messages to trick recipients into divulging private information, such as credit card numbers, account usernames, passwords, birth dates or even possibly releasing details of other crew members on-board.

Phishing messages often display real logos and appear to have come from the actual organization, but those messages are frequently nothing more than copyright infringements and faked addresses. If you suspect a message does not possess any credibility, you are much safer calling the company directly — preferably at a telephone number printed on a paper statement or invoice — and talking to an authorized representative. Contact your fleet control group if you are unsure about authenticity of a message.

4 Policy

4.1 Access Control

Requests for users' accounts and access privileges must be formally documented and appropriately approved by following the instruction included in the **Access Control Policy.**

▶▶ See – Access Control Policy

On board normally functional accounts are used instead of personal accounts due to the rotation of personnel (e.g. SPCaptain@silversea.com or SMChiefEngineer@silversea.com). Each account is associated to a specific person for a specific period of time (usually a few months) but to know who used the account the crew journal should be updated regularly. Exceptions may apply and must be tracked (overlapping periods when 2 people are on board with the same functional role).

Other accounts (both shore and shipside) are generic and indicate a group of people (e.g. Reception@silversea.com or invoices@silversea.com). In this case the responsibility of the user is shared among the members of the teams and these logins should not have high privileges.

In case a shared login has high privileges (e.g. administrator) the usage of the login by each owner should be tracked in a specific journal.

4.2 Asset Management

To provide a proper Asset Management, the following guidelines must be observed:

- **Identification**: all information systems must be properly identified;
- **Ownership and Responsibility**: all information systems must have an appointed owner who has full responsibility on their management;

- **Documentation**: all information systems must be documented and updated in a properly redacted Asset Inventory (see section **Asset Inventory** in chapter ***"3.3 Identify Vulnerabilities"***).

All systems assets must have a responsible holder who must be clearly stated. The holder must be considered responsible for:

- Definition and communication of the guidelines put in place for asset assignment, proper use and disposal;
- Validating that asset configuration follows Company policies
- Alerting Information System Security for situations where IT assets might have been compromised

The asset register includes:

- Inventory hardware assets:
    - inventory asset number;
    - asset owner;
    - device characteristics (e.g. type, model, serial number, …);
    - usage data (e.g. assignee, date of assignment, designated owner, …);
    - accounting data (e.g. supplier, contract reference, acquisition date, …);
    - asset status (active, inactive, ….).
- Software inventory (information on product, version/release, software license, supplier, contract reference, date of installation)
- Inventory of servers, network services:
    - IP addresses;
    - non IP addresses;
    - non Ethernet access points;
    - desktops and servers;
    - connectors and communicating field devices
- Communication devices

On-board systems includes but are not limited to:

- **Bridge systems**
- **Propulsion and machinery management and power control systems**
- **Access control systems**
- **Passenger servicing and management systems**
- **Passenger facing public networks**
- **Administrative and crew welfare systems**
- **Communication systems**
- **Core Infrastructure systems**
- **On-board business computers**

4.3 Third Party Management

Every Third party must be properly register and the contract must include the requirements for information security and responsibilities, appropriate clauses, obligations and service level, to ensure that the relations with third parties are maintained consistent with the required Company information protection levels.

In every contract the following requirements must be included:

- **Non-Disclosure Agreement**: must always be part of any third party contractual relationship.
- **Information Use**: third party must use Company information only to perform the activities agreed in the contract.
- **Information Security**: third party must ensure the implementation of information security measures, as needed. Maintenance of a secure processing environment includes but is not limited to the timely application of patches, fixes and updates to operating systems and applications as provided by vendor or open source support.
- **Data Availability**: the Company required level of information availability must be included in contractual agreement.
- **Data Retention**: third party is required to comply with its recordkeeping or audit requirements or if required by law and agrees that any and all data associated with Company transactions shall be irreversibly destroyed after a period of 3 years from the date of last use or recording.
- **Audit Rights**: audit activities on the third party information protection system must be agreed with Company and included in the contract agreements, as needed.
- **Security Organization**: third party must appoint a responsible person as a contact for any information security issue (security incidents, audits and reporting)

In addition, it must tracked at least failed and successful access and, where possible, actions performed on its information. Any incident that occurs to third party systems that handles Company information must be properly reported (See chapter ***"4.4 Information Security Incident Management"***).
Upon termination of the period established by the company third party shall erase, destroy, and render unrecoverable all Company data and certify in writing that these actions have been completed upon the request of an agent of Company.

4.4 Information Security Incident Management

Information Security Incident Management Process has four stages:

- **Incident Reporting:** detection and reporting of any actual or suspected information security incident to all the involved parties in a timely manner.
- **Incident Analysis:** collection and assessment of the information associated with information security events to determine whether or not an incident has actually occurred.
- **Incident Response:** responding promptly to information security incidents in order to restore affected system and services and to return to conditions of normality.
- **Incident Closing:** learning from information security incidents to make improvements to the overall approach to information security incident management.

Any incident that may be cyber related should in the first instance be reported to **IT Vessel Support** team by telephone **(insert)** or email (vesselitsupport@silversea.com). In the event of a system

being suspected of compromise, if possible the system should first be disconnected from any network access and left switched on. This may allow the management to investigate further and to escalate if necessary. The first responder should always be concerned with containment, for example by isolating the system to prevent further spread of malware or use of compromised media.
For major maritime cybersecurity events/incidents, a report is prepared by the management. This will provide information on events and impact, probable cause and lessons learned.
Periodically the incident management team (CISO, if appointed, or CIO and VP Audit) perform analysis on major incident detected and share the results with relevant parties. Cyber incident awareness is part of the training program (see chapter ***"3.7 Training and Awareness"***)

4.5 Communication and Operation Management

Backup

Essential information and software-adequate backup facilities should be available to help ensure recovery following a cyber incident. OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber incident.
A full operational backup for all systems must be performed during the ship's night time. The backup must be stored. The disks must be properly controlled in case of critical failures and must be timely replaced or repaired.

Network Security Manager

The Network access must be properly isolated and accessible only from the ship. This must be obtained by a proper use of Virtual Private Network (VPN) such that the data traffic should be encrypted to an acceptable international standard. Shipboard network systems, where they exist, are categorized into three main areas:

- IT (Information Technology): This is the ships business network and allows communication between the administrative systems such as e-mail, Shipsure, business tools
- OT (Operational Technology): This network will allow network enabled functional devices and systems such as CCTV, alarms and sensors
- Crew: This network must only contain crew personal devices where internet services are provided

This network must only contain crew personal devices where internet services are provided. It is important to recognize and assess the cyber risks from equipment in all three vessel networks.

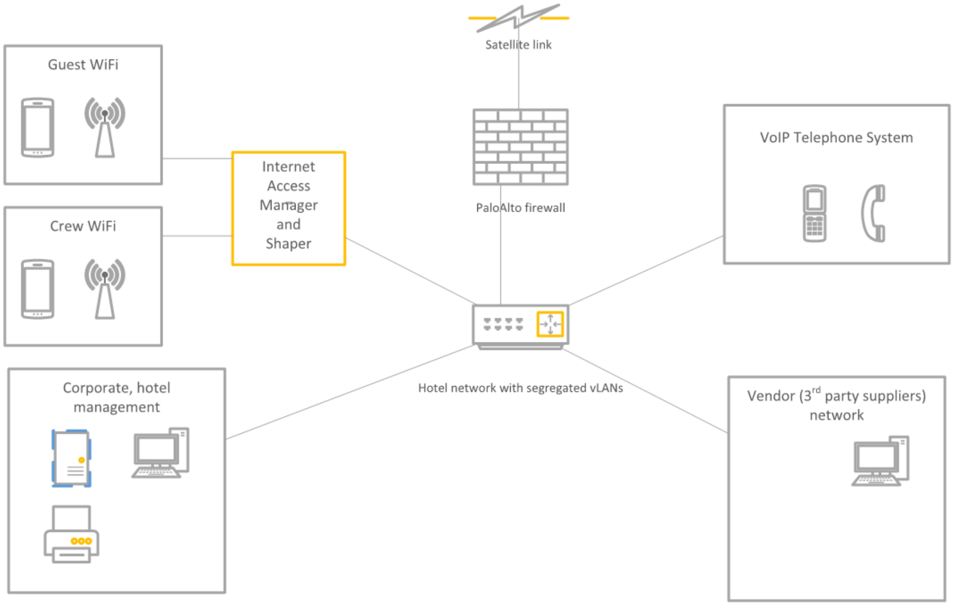

Satellite link
Guest WiFi
Internet Access Manager and Shaper
PaloAlto firewall
VoIP Telephone System
Crew WiFi
Hotel network with segregated vLANs
Corporate, hotel management
Vendor (3rd party suppliers) network

Figure 2: *Vessel Network Segregation*

On-board computers that are connected either or indirectly to the Internet via the Ships satellite or terrestrial communications network must be protected by a firewall. This firewall must be designed and configured to protect the Ships network for external cyber-attack and limit inbound traffic to recognized protocols and providers only. In addition, access to external internet based resources from the vessel should be restricted to professional use of the business network. Cross-over for the business network to any crew based network on-board is forbidden and the firewall or network must be configured accordingly.

Furthermore, the following guidelines should be observed:

- No system should allow bridged connections, e.g. a laptop connected to IT network AND also connected to Crew Wi-fi network.
- No attempt should be made by Ships colleagues to connect any other systems to the ship network, for example connecting a dedicated loading computer to the network.

Protection from Malware

Controlled networks are designed to prevent any security risks from connected devices by use of firewalls, security gateways and Antivirus software. The firewall must be designed and configured to protect the Ships network for external cyber-attack and limit inbound traffic to recognized protocols and providers only. In addition, access to external internet based resources from the vessel should be restricted to professional use of the business network. If Network is not controlled then it should be considered unsafe. Antivirus and Firewall must always be updated to the last version.

To avoid cyber attacks from malwares, a Phishing awareness program must be performed at least once a year, in order to instruct users on what to do when receiving a suspicious mail (see chapter *"3.7 Training & Awareness"*). A control software must be installed to perform a multi-tiered approach to protect Simple Mail Transfer Protocol (SMTP) and make sure only legitimate e-mail gets through the filters.

Information Transfer

Access to hardware must be properly secured only to the authorized personnel. In order to prevent the creation of uncontrolled data flows, USB ports of critical systems must be either disabled or restricted in their access. It is suggested to transfer information through the mail system since it should be properly controlled and monitored in order to avoid phishing and malwares.

4.6 Information Systems Acquisition, Development and Maintenance

Properly designated security controls must be put in place for all the life cycle of an information system, covering system development, upgrades, maintenance, dismission and disposal. This policy must be included in any contract or agreement whenever third parties are involved in Information Systems Acquisition, development and maintenance.

Any business department must always discuss any new system implementation or enhancements to already existing systems with the IT Department at the initiation stage of the project. In addition to the functional requirements, security vulnerabilities are to be identified through a risk assessment and proper information security requirements must be developed.

Security Controls in Information Systems Development and Maintenance

Implementation and maintenance of software applications must be properly controlled based on the following requirements:

- **System Security requirements and documentation**: the documentation must be produced for all Company information systems under development, including the description of system security requirements and the controls in place, or planned for meeting the requirements;
- **Separate development, testing, and production environments**: System development, testing and production should be performed in separate environments;
- **System test**: before being transferred to the production environment all softwares must be tested and formally accepted by both the business owner and the IT Department;
- **Change controls:** if any change is to be implemented it must be properly controlled to minimize the risk of any unauthorized change to information or information systems. Formal approval is required for the implementation of the change.
- **Protection of system test data**: testing should not be performed on real data, but on copies with any existing confidential data appropriately masked. If Company data that requires real

or confidential data is used during testing it must be protected by suitable security controls, including but not limited to:

- Authorization process;
- Removal of all real data from the test system after their use;
- Audit trail of related activities.

Any personal information, if used, must be depersonalized. If it is not possible to depersonalize the information then its use must conform to applicable Data Privacy Policy.

- **Third Party software**: the third party supplier must provide the possibility to test the system's security controls by Company or an independent third party, if needed (see chapter *"4.3 Third Party Management"*).

The IT Officer is held responsible for the following process:

- Monitor every software on-board
- Perform regular assessment on company system to ensure that, where possible, manufactures recommended security have been applied (e.g. the use of Windows Services Update to update Microsoft Operating Systems and software)
- Ensure company approved anti-virus system is installed on computers
- Ensure databases and electronic files are regularly backed up
- Store master disks in a dedicated safe place. (Obtain permission from office before releasing disks from the safe place)
- Ensure difficulties found with computer programs are first reported to the office
- Ensure users of shipboard computer system advises their relief on the full operation and control of the system

Furthermore, if vessel is seasonally laying up, protect systems from:

- Unauthorized use
- Theft
- Cold/Hot weather

4.7 Physical and Environmental Security

To prevent unauthorized access, damage, interference to information system assets and interruption to business activities, company must implement controls and safeguards. Physical and environmental security control must follow all appropriate regulations. Physical access to Data Center on-board must be properly authorized on an "as needed" basis.

Physical Security

The Data Center on-board must be located in an area where access is properly prevented. On selected vessels, the Data Center is oversaw by security cameras located outside of the room to be able to identify who enters the room.

Physical access to Data Center must be restricted only to authorized personnel, to ensure it a physical entry control must be implemented. All individuals with granted physical access to Data Center must not share the entry procedure to others. Third party access must be properly authorized and monitored. An access log must be retained (with information on visitor identity, date, entry time and leaving time).

Access rights and authorization to Data Center must be reviewed and revalidated periodically.

Environmental Security

Data Center must be protected from environmental threats and power outages. The equipment must be protected by fire extinguisher system and an air conditioner system isolated from the air conditioner system used by the rest of the vessel. The systems must be maintained by authorized personnel in accordance to supplier's recommendations. An audit trail of maintenance and test activities must be retained.