

## 1. Regulation for the Organization of the Safety Management System MN-02-00

ORCA-MN-02-00  
Revision: 1  
Page: 1 of 1  
Date: 01 Feb,2018

**SMS Document No.: ORCA-MN-02-00**                      **Chapter: 2**  
**Issued by: The Designated Person**                      **Approved by: The President**  
**Title: Regulation for the Organization of the Safety Management System**

### 1. Purpose

This regulation is to define the responsibilities and authorities of Departments and personnel implementing the SMS. It also clarifies the reciprocal relationship between them in order to ensure that the Company's management activities comply with the regulations of safety operation and environmental protection.

*(snipped)*

#### 4.5 The IT Manager

4.5.1 The IT Manager is responsible for the following jobs;

- (1) To ensure the proper operations of IT systems onboard ships and ashore;
- (2) To watch, assess, and assist to response to IT related incidents;
- (3) To proceed necessary training and education related to IT systems;
- (4) To control data related to IT systems;
- (5) To catch up cyber risks in IT fields;

4.5.2 The Company may contract with outside IT expert or consultant to support IT matters, if so required.

*(snipped)*

ORCA CO., LTD.

2. Chart of Organization for the Safety Management System MN-02-00A

ORCA-MN-02-00A  
Revision: 0  
Page: 1 of 1  
Date: 01 Feb,2018

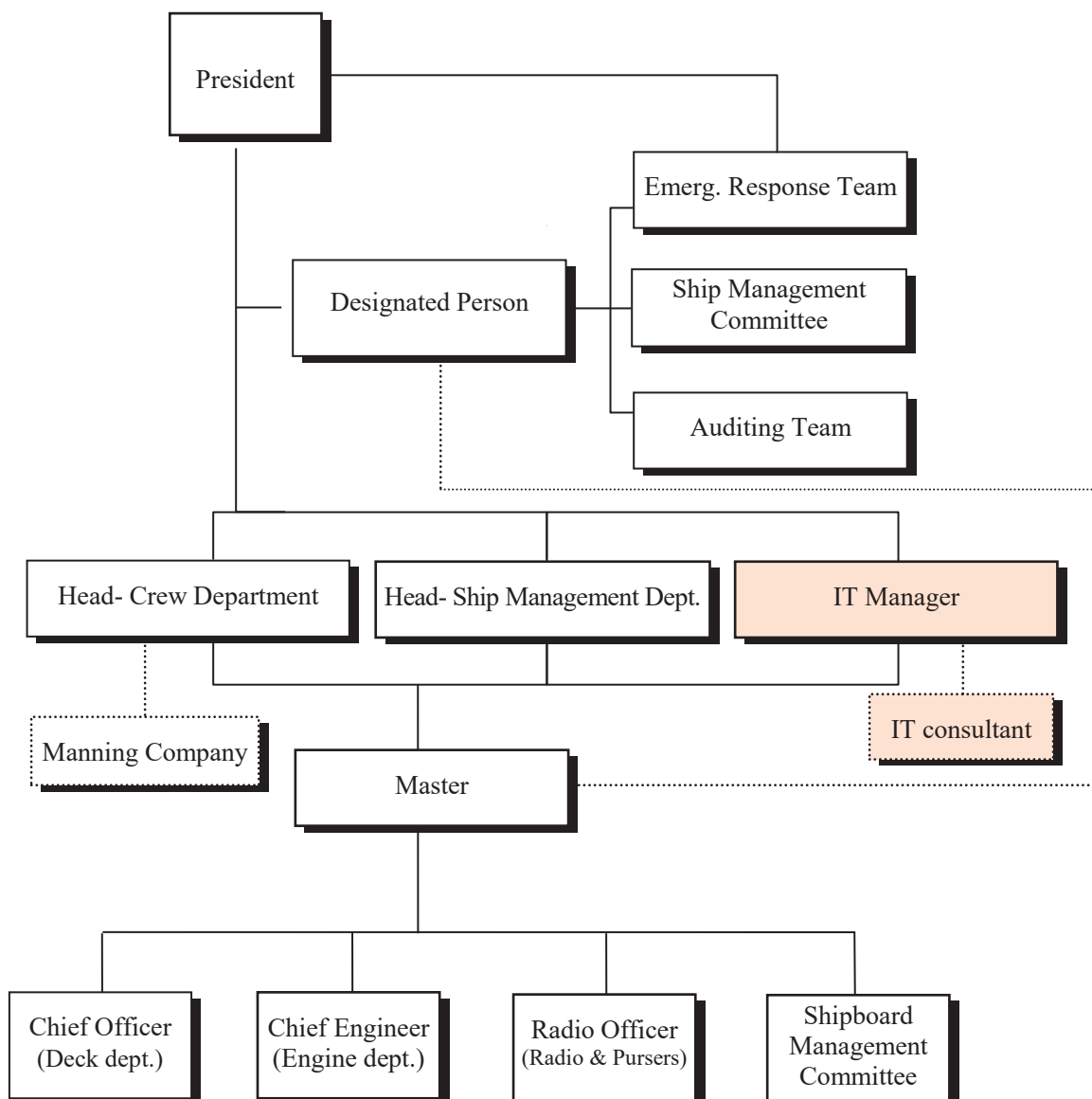
SMS Document No.: ORCA-MN-02-00A

Chapter: 2

Issued by: The Designated Person

Approved by: The President

Title: Chart of Organization for the Safety Management System



ORCA CO., LTD.

### 3. Regulation for management of IT systems MN-20-00

ORCA-MN-20-00  
Revision: 0  
Page: 1 of 5  
Date: 01 Feb. 2018

**SMS Document No.: ORCA-MN-20-00**

**Chapter: 20**

**Issued by: The Designated Person**

**Approved by: The President**

**Title: Regulation for management of IT systems**

#### **1. Purpose**

This regulation is prepared to specify the arrangement and management of IT systems in the Company and onboard ships for the proper implementation of SMS, including to response to possible cyber risks.

#### **2. Application**

This regulation is applicable to the Company and all vessels under management of the Company.

#### **3. Reference regulations**

SOLAS XI-2  
MSC-FAL-1/Circ. 3

#### **4. Definition**

##### **4.1 IT system**

“IT system” is a computer-based system used for all kind of operations. The system can be total packaged equipment or install based software for PC. Any device, equipment or services based on computer are defined as a part of "IT System".

##### **4.2 Cyber-risk**

“Cyber-risk” is a potential risk to lead operation failure of the IT systems, which will cause financial loss, disruption or damage to the reputation of an organization. Cyber-risk includes external factors (such as computer virus, Trojans, or attack over network, etc.) and internal factors (malfunction, miss-operation, or system bug, etc.).

##### **4.3 IT incident**

“IT incident” is an occurrence, which actually or potentially results in adverse consequences to IT systems, includes all deficiencies and non-conformities involving to the IT systems.

ORCA CO., LTD.

#### 4.4 Cyber risk management

“Cyber risk management” is the process of identifying, analyzing, assessing, and communicating a cyber related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level; taking into consideration the costs and benefits taken by the Company.

### 5. Requirements

#### 5.1 Design of IT standard

For a smooth and effective implementation of the SMS, the Company shall set-up an IT Standard, and, accordingly, construct IT Systems in the Company and on-board ships under management of the Company. IT Standard is to be recorded on the “Records for IT Standard Design” ([ORCA-SM-07-50](#)), and to be annually reviewed for any improvement by the IT Manager. For details, refer to the “Procedure for Management of IT Systems” ([ORCA-MN-20-01](#)).

#### 5.2 Operation of IT systems

Under the direction of the Designated Person and the Head of the Shipmanagement Department, the IT Manager must integrate the specified IT Systems and network systems properly and supervise and direct the relevant personnel to operate IT systems in accordance with IT Standard or makers’ instructions.

#### 5.3 Identification of IT systems

5.3.1 The IT manager should identify all IT systems onboard and ashore using the “List of IT Systems” ([ORCA-SM-07-51](#)).

5.3.2 The IT manager should process the risk assessment regarding cyber-risk for each IT systems and prepare for countermeasure if so required.

5.3.3 During the risk assessment, if a part of the IT systems had already assessed in the IT standard, the part of risk assessment can be omitted.

5.3.4 In case of addition, replacement, or abolition of the IT system had been taken, the IT manager must re-process risk assessment to the part of modification.

#### 5.4 Maintenance of IT systems

In order to ensure the proper operation of IT systems, the IT Manager shall set up a maintenance plan (on the OMPS software) for the periodic maintenance of IT systems, including its important elements as well as associated software. The maintenance plan should include the following factors:

- (1) Maintenance operation designated by each IT system vender.
- (2) Minor software update.
- (3) Backup operation of data.
- (4) Condition check of each IT systems.

Maintenance of the IT systems should be processed in reference to the “Regulation for Maintenance of Hull, Machinery and Equipment”

#### **5.5 Hardware Replacement of IT systems**

5.5.1 Due to service life, hardware of the IT systems required replacement.

5.5.2 The IT manager should plan the hardware replacement considering following factor;

- (1) Recommendation of the hardware vender
- (2) Condition report of the IT systems
- (3) Improvement of new hardware tolerance for cyber-risk

5.5.3 Plan for replacement should include following operation;

- (1) Replacement of the client PC due to deterioration
- (2) Replacement of the peripherals due to deterioration
- (3) Replacement of the hardware which has newer countermeasure to handle cyber-risks.
- (4) Replacement of the hardware which considered being required for appropriate operation of the IT systems.

#### **5.6 Version control for firmware or software of IT Systems.**

5.6.1 The IT manager should control version tables of firmware or software of the IT systems.

5.6.2 If any update version has been released, the update should be applied as possible.

5.6.3 However, major update might affect to compatibility or connectivity among other IT systems. In this case, sufficient verification and risk assessment must be done by the IT manager before applying the update.

5.6.4 The IT manager should judge if the update is major or minor appropriately.

## **5.7 Handling of incidents of IT systems**

- 5.7.1 The IT manager should handle and solve incidents in relation to the IT system onboard and ashore.
- 5.7.2 The IT manager should record the incidents for future analyzing, to improve tolerance for cyber-risk.
- 5.7.3 If the incident is considered as critical, the IT manager must report this to the Designated person according to “Regulation for emergency preparedness” .
- 5.7.4 After solution of the critical incident, the IT manager must proceed risk investigation for recurrence prevention.
- 5.7.5 The “Procedure for Cyber Risk Management” ([ORCA-MN-20-02](#)) must also be referred to.

## **5.8 Education and training regarding to the operation of IT systems.**

- 5.8.1 The IT manager should ensure that all personnel involved in the Company's SMS have an adequate understanding of the IT systems and cyber-risks.
- 5.8.2 The IT manager should plan appropriate education or training in relation to the operation of the IT systems.
- 5.8.3 The education or training plan should be processed in reference to “Regulation for Education and Training” .
- 5.8.4 The IT manager should timely release a newly appeared cyber-risk to the relevant departments and vessels for prevention purpose.

## **5.9 Data Management of IT systems.**

- 5.9.1 The IT manager should properly manage the data which is operated in the IT systems.
- 5.9.2 Regarding the data management, following factor should be considered;
  - (1) Availability the data can be used in proper timing.
  - (2) Integrity to prevent data loss or falsification
  - (3) Confidentiality the data will not be leaked to any unauthorized party.
- 5.9.3 The IT manager should clarify about ownership of intellectual property for the data.
- 5.9.4 In case of transfer of management of a ship, the IT manager should correct or delete the data in reference to “List of the IT systems” ([ORCA-SM-07-51](#)).

## **5.10 Monitoring of unknown cyber-risks.**

- 5.10.1 The IT manager should try to find out new unknown cyber-risks.

5.10.2 Master or each Department of the Company must inform the IT manager for any newly identified cyber-risk.

### **5.11 Management review regarding to IT systems**

5.11.1 The IT manager should provide following information to the safety management committee during management review;

- (1) Analyze report of the IT incidents
- (2) Newly found cyber-risk and risk assessment report
- (3) Trend information of IT fields
- (4) Update information of software and hardware.
- (5) Revision plan of IT standard with risk assessment
- (6) Revision plan of IT systems list with risk assessment.

5.11.2 The Designated Person should investigate this information and review the IT management in reference to "Regulation for Internal Audits and Management Reviews" ([ORCA-MN-11-00](#)).

### **5.12 Contract with IT consultant or IT expert**

5.12.1 Operation of IT system which connected to Internet using TCP/IP, requires high knowledge and experience regarding IT.

5.12.2 In order to support the IT manager, the Company may contract with external IT consultant or IT expert.

## **6. Applicable procedures**

Procedure for Management of IT Systems ([ORCA-MN-20-01](#))

Procedure for Cyber Risk Management ([ORCA-MN-20-02](#))

## **7. Applicable records:**

The Company and the ship:

Records for IT Standard Design ([ORCA-SM-07-50](#))

List of IT Systems ([ORCA-SM-07-51](#))

Records for Risk Assessment of IT Systems ([ORCA-SM-07-52](#))

Maintenance Plan for Hull, Machinery and Equipment

#### 4. Procedure for management of IT systems MN-20-01

**SMS Document No.: ORCA-MN-20-01**

**Section: 20-1**

**Issued by: The Designated Person**

**Approved by: The President**

**Title: Procedure for Management of IT Systems**

### 1. Area of application

This procedure defines the guidance for the management of IT systems onboard and ashore and apply to the Company and vessels under the management of the Company

### 2. References

ORCA-MN-20-00 Regulation for Management of IT systems

### 3. Procedure to setup IT Standard

3.1 The IT manager should design IT Standard using “Record for IT Standard Design” (ORCA-SM-07-50) to standardize the IT system integration.

3.2 In order to prevent any problem in connection of software and hardware, following factor should be verified;

- (1) Compatibility
- (2) Convertibility
- (3) Conflict
- (4) System response speed

3.3 The IT manager should prepare IT Standard for vessel and company.

3.4 The IT manager should categorize the IT system as following;

Company Category	Effects
A	Those systems, failure of which will not directly affect to commercial shipping operation.
B	Those systems, failure of which could eventually impact to commercial shipping operation.
C	Those systems, failure of which could immediately cause an impact to commercial shipping operation.

3.5 Regarding Category B and C, The IT manager should prepare a specific measure to ensure those systems working continuously.



3.6 The ship manager should also categorize the IT system defined by NK TEC-1145 as followings;

Class Category	Effects
I	Those systems, failure of which will not lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
II	Those systems, failure of which could eventually lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.
III	Those systems, failure of which could immediately lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment.

3.7 The ship manager should process risk assessment regarding IT standard.

**4. Procedure for risk assessment of IT SYSTEM**

- 4.1 The IT manager should process risk assessment regarding identified risks on IT systems using the “Record for Risk Assessment of IT Systems” ([ORCA-SM-07-52](#)).
- 4.2 If any connection had made among multiple IT systems, risk of the connection should be also verified.
- 4.3 Following factors should be assessed for each risk;
  - (1) Possibility
  - (2) Frequency
  - (3) Damage
- 4.4 In conclusion of the assessment, following option should be selected;
  - (1) Accept the risk
  - (2) Measures required
  - (3) To be re-evaluate later
- 4.5 If any countermeasure required, the IT manager should plan a measure and process it with approval of the Designated Person.
- 4.6 As risk assessment requires highly knowledge and experience of IT, it is preferable to have an advice from IT consultant or IT expert.

**5. Procedure for review of IT Standard**

- 5.1 The IT manager should review the IT standard annually.
- 5.2 If any modification such as revision, addition, deletion has been made in IT standard, the IT manager must process risk assessment on such modification.
- 5.3 Even if no modification had been made, the IT manager still has to process risk assessment considering following factor;
  - (1) Change of shipping operation environment and requirement
  - (2) Improvement of IT technology
  - (3) Trend of new cyber-risks
- 5.4 Update of IT Standard must be submitted to the Designated Person for approval.
- 5.5 If update of the IT Standard had been approved, the IT manager should prepare a plan to update each IT system of vessel and shore side.

#### **6. Preparation of IT systems in newly management vessels.**

- 6.1 The IT manager shall refer to the IT standard and integrate IT systems onboard the ship with reference to the “Guideline for IT System Integration” ([ORCA-MN-20-01A](#)) and record the same on the “list of IT Systems” ([ORCA-SM-07-51](#)).
- 6.2 The IT manager should process risk assessment for each IT systems using “Record for Risk Assessment of IT Systems” ([ORCA-SM-07-52](#)).
- 6.3 In this assessment, if the IT system is already assessed in IT Standard, assessment of this part can be omitted.
- 6.4 Also, if the IT system is categorized as Category II or III in NK TEC-1145, and the system is operated as standalone, assessment of this part can be omitted. These systems should be assessed by the system vender.
- 6.5 The IT manager should prepare a maintenance plan including following tasks;
  - (1) Maintenance operation which instructed by the system vender.
  - (2) Minor update of software/firmware which approved by the IT manager
  - (3) Backup of the data
  - (4) Condition check
- 6.6 These preparations should be approved by the Designated Person.

#### **7. Procedure for handling of IT systems by the termination of vessel management.**

- 7.1 The IT manager should correct or delete the data of every IT systems onboard, referring “List of IT Systems” ([ORCA-SM-07-51](#)).

## **8. Procedure for modification of IT system**

- 8.1 In case of IT system modification such as addition, replacement, or abolition is planned, the IT manager should verify following factors;
- (1) Compatibility
  - (2) Convertibility
  - (3) Conflict
- 8.2 The IT manager should also process risk assessment for the new connection of IT systems.
- 8.3 If any risk or problem has been found the IT manager should prepare a countermeasure to operate new system integration or postpone the modification.
- 8.4 The conclusion should be approved by the Designated Person.

## **9. Procedure for handling IT incident**

- 9.1 The IT manager should handle IT incident occurred both onboard and ashore.
- 9.2 In case of following situation, the IT manager must report the occurrence to the Designated Person as critical incident.
- (1) The incident can directly affect to the vessel’s safety navigation.
  - (2) Or, the incident can lead to commercial damage to outside of the company.
  - (3) Or, delay of the solution may lead to situation (1) or (2).
- 9.3 In case of critical incident, the Designated Person must setup Emergency Response Team to handle the situation in reference of “Regulation of Emergency Preparedness” ([ORCA-MN-10-00](#)).
- 9.4 The Designated Person can contact IT consultant or IT expert for advice, if so required.
- 9.5 The “Procedure for Cyber Risk Management” ([ORCA-MN-20-02](#)) must also to be referred to.

## **10. Relevant forms and information**

Guideline for IT System Integration ([ORCA-MN-20-01A](#))  
Procedure for Cyber Risk Management ([ORCA-MN-20-02](#))

Records for IT Standard Design ([ORCA-SM-07-50](#))

List of IT Systems ([ORCA-SM-07-51](#))

Records for Risk Assessment of IT Systems ([ORCA-SM-07-52](#))

Maintenance Plan for Hull, Machinery and Equipment (the OMPS)

## 5. Guideline for IT system integration MN-20-01A

ORCA-MN-20-01A  
Revision: 0  
Page: 1 of 4  
Date: 01 Feb. 2018

### **Appendix** **Guideline for IT system integration**

#### **Client PC**

- (1) Following points should be considered for selection of client PC model.
  - (a) Sufficient CPU power, memory, HDD space to operate the IT systems.  
Especially, security software requires these resources.
  - (b) PC model which has enough reliability to operate onboard.
- (2) Language model might affect to the IT systems. The IT manager must verify it if PCs are supplied from different countries.

#### **OS**

- (1) In order to apply necessary security update, “auto update function” should be ON as possible.
- (2) However, major updating of OS might affect to the other IT systems or peripherals.  
If the IT manager decides to update the OS’s version, sufficient verification and risk assessment must be taken.

#### **Basic software**

- (1) “Basic software” is software which acts as system requirements of each IT systems, such as MS-Office, PDF reader, etc.
- (2) Major update of basic software might affect to related IT systems. So if the IT manager decides to update the version of basic software, sufficient verification and risk assessment must be taken.

#### **Application software**

- (1) All application software should be verified in IT standard environment by the IT manager before installation.
- (2) If the application software has a communication function, detail of the function (communication port, destination IP, etc.) must be clarified. If communication detail of the software is not disclosed, the software shall not be adopted.
- (3) Application software might have conflict to the other applications. In order to prevent conflicts, the IT manager must proceed sufficient verification before adoption.

ORCA CO., LTD.

#### **Anti-virus software**

- (1) Anti-virus software (or any kind of security software) must be installed to all operational official PCs.
- (2) The IT manager should prepare an appropriate method to update definition files (or pattern files) to keep Anti-virus software operational.
- (3) Especially, in the vessel which has an ability to access to the Internet in the ocean, “online updating function” is required.

#### **Communication infrastructure**

- (1) In order to ensure communication reliability, it is preferred to have more than two different kinds of communication infrastructure.
- (2) The IT systems onboard are preferred to operate as “Open system” which will not be affected by any specific communication infrastructure. The IT systems onboard should be independent from communication.
- (3) To control the latest cyber-risks, maintaining the version of OS and applications by auto is very crucial. If the vessel has no ability to apply “auto updating” via satellite, shore side communication such as 4G should be adapted.

#### **Vessel Local Network (LAN)**

- (1) Vessel LAN should be designed to suit each IT systems can be operate appropriately.
- (2) Vessel LAN can be separated to multiple sub-network to control packet traffics.
- (3) Following IT systems are preferred to be separated into sub-network due to their traffic volume.
  - (a) Internet connection for crew welfare
  - (b) CCD monitoring camera system
- (4) For any IT system identified its importance, the system should be placed into independent sub-network to ensure traffic reliability.
- (5) For crew welfare network, it is preferred to have Wi-Fi access points. So, crew can connect his private device to them. In order to avoid network conflict, Ethernet connection should not be provided to crew network.

#### **Peripheral equipment**

- (1) The IT manager must clarify the detail of communication function of all LAN connected peripheral equipment on board (port, destination IP, etc.). If the

communication details are not disclosed, the equipment shall not be adopted.

#### **Crew private device and private internet connection**

- (1) Most of cyber-risks are coming from crew private device and private connection such as “rental 4G in port”.
- (2) To bring this kind of situation under control, the IT manager must prepare appropriate countermeasure such as;
  - (a) Train and educate crew to have adequate IT literacy.
  - (b) Identify the difference of management policy between official IT systems and private devices.
  - (c) Prepare specific method to block this kind of cyber-risks which come from crew private devices and Internet connections.
- (3) One of the better solutions is to supply controlled Internet connection for crew officially. Then, IT manager can arrange appropriate filters and sub-network settings to prevent this kind of cyber-risks.

#### **SNS or private E-mail access**

- (1) SNS or private E-mail access of crew might have security-risks.
- (2) The IT manager should identify which onboard-information should be secured.
- (3) The IT manager should train the crew for handling of secured information.

#### **License compliance**

- (1) The IT manager must ensure that all software and hardware have appropriate license.
- (2) In order to avoid unknown cyber risks, following systems are prohibited.
  - (a) Illegal copy
  - (b) Pirated edition
  - (c) A hardware which have unauthorized modification.
  - (d) Any illegal network devices.

#### **Network router**

- (1) It is preferred to have a network router independent from communication infrastructure. So, the vessel LAN can be operated without dependency.
- (2) Network router should have an ability to switch multiple communication infrastructures.

- (3) Network router should have a function to control internal network traffic.
- (4) In order to avoid un-controlled traffic or cyber-attack from outside, un-necessary port must be closed in filter settings.



## 6. Procedure for Cyber Risk Management MN-20-02

ORCA-MN-20-02  
Revision: 0  
Page: 1 of 2  
Date: 01 Feb. 2018

**SMS Document No.: ORCA-MN-20-02**                      **Section: 20-2**  
**Issued by: The Designated Person**                      **Approved by: The President**  
**Title: Procedure for Cyber Risk Management**

### 1. Area of application

This procedure defines the guidance for taking necessary measures to response to cyber security incidents of IT systems apply to the Company and all ships under the management of the Company.

### 2. References

[ORCA-MN-20-00](#)      Regulation for Management of IT systems

### 3. Authorities and responsibilities

- 3.1 The Head of the Shipmanagement Department, under the direction of the Designated Person, is responsible for cyber risks management, including IT systems, onboard ships and the shore-based Company.
- 3.2 The IT Manager is responsible for the smooth operation of IT systems and, supervise, monitoring, and timely response to cyber incidents.
- 3.3 The Master onboard is responsible for the smooth operation of IT systems and, supervise, monitoring, and report any deficiency, non-conformity or cyber incident to the Company in accordance with the "Procedure for Management of Deficiencies and Non-conformities" ([ORCA-MN-13-01](#)).

### 4. Procedure

- 4.1 Identify threats- The IT Manager, under the direction of the Head of the Shipmanagement Department, and the Designated Person, is to take measures to make all relevant personnel understand the external cyber security threats to the ship and the Company and to understand the internal cyber security threat posed by inappropriate use and lack of awareness.
- 4.2 Identify vulnerability- The IT Manager is to develop inventories the Company and shipboard systems with direct or indirect communication links with referring to the "List of IT Systems" ([ORCA-SM-07-51](#)) and understand the consequences of a cyber security threat on these systems also understand the capabilities and limitations of existing protection measures.

ORCA CO., LTD.

- 4.3 Assess risk exposure- The IT Manager is to assess and determine the likelihood of vulnerabilities being exploited by external threats, by inappropriate use, and the security and safety impact of any individual or combination of vulnerabilities being exploited. The form "Records for Risk Assessment of IT Systems" ([ORCA-SM-07-52](#)) is to be applied.
- 4.4 Develop protection and detection measures- The IT Manager, under the direction of the Head of the Shipmanagement Department, and the Designated Person, is to take measures to the likelihood of vulnerabilities being exploited through protection measures also to reduce the potential impact of a vulnerability being exploited.
- 4.5 Establish contingency plans- The IT Manager shall develop a response plan to reduce the impact of the treats under the approval and direction by the Designated person in accordance with the "Procedure for Management of Deficiencies and Non-conformities" ([ORCA-MN-13-01](#)).
- 4.6 Response to and recover from cyber security incidents- After recover cyber security incidents by using the response plan, the IT Manager shall assess the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities.
- 4.7 Investigating cyber incidents- The IT Manager, under the direction of the Head of the Shipmanagement Department, and the Designated Person, is to investigate cyber incidents in order to archive a better understanding of the potential cyber risks, identification of lessons learned also updates to technical and procedural measures to prevent a recurrence.
- 4.8 Response to cyber incidents of IT systems - The IT manager shall assess its vulnerability and impact and give a response in accordance with the "Procedure for Management of Deficiencies and Non-conformities" ([ORCA-MN-13-01](#)), and coordinate with the makers of the operational technology system to ensure its safety and security.

## **5. Relevant forms and information**

Records for IT Standard Design ([ORCA-SM-07-50](#))

List of IT Systems ([ORCA-SM-07-51](#))

Records for Risk Assessment of IT Systems ([ORCA-SM-07-52](#))

7. Record for IT Standard design SM0750

**Record for IT Standard Design**

Standard type:  
 Date of Record:  
 IT Manager:  
 Designated Person:

This IT Standard will be value from :

I. Client PC Conditions				Remark
<b>(1) Hardware</b>				
	Number of PCs			
	Type (Laptop PC/Desktop PC)			
	CPU			
	Memory			
	HDD			
<b>(2) Software</b>	<b>Basic Software</b>			
	OS			
	MS-OFFICE (version)			
	MS-OFFICE (Applications)			
	Acrobat Reader			
	AntiVirus Software			
<b>(3) Software</b>	<b>Application Software</b>	<b>Applications</b>	<b>Suppliers</b>	
<b>(4) Network Diagram</b>	<b>Detail of PC setting</b>			
	Detail of PC setting	<b>(Refer to the second sheet)</b>		
<b>II. Peripheral Device</b>				
<b>(1) Printer</b>				
	<b>Laser Printer</b>			
	* Number of them			
	* Single or Multiple function			
	* Black/White or Color			
	<b>Inkjet Printer</b>			
	* Number of them			
	* Single or Multiple Function			
	* Black/White or Color			
<b>(2) Scanner</b>				
	* Number of them			
	* Flatbed/Stand			
<b>(3) NAS set</b>				
	* Model			
<b>III. Network</b>				
<b>(1) Router</b>				
	Type of Router			
	Supplier			
<b>(2) Sub Network</b>				
	Purpose of Sub Network			
<b>(3) Wifi Access Point</b>				
	Number of Wifi Access Point			
<b>(4) Network Diagram</b>				
	Network Diagram	<b>(Refer to the third sheet)</b>		

**PC setting detail**

	PC01	PC02	PC03	PC04	PC05	PC06
<b>Location or Main Usage</b>						
Location(Bridge, Master, etc.)						
Type (Desktop, Laptop)						
Main Usage(Mail, SMS-MAIN, SMS-SUB, Office Work)						
E-mail Function(MAIN/SUB/NO)						
Use LAN? (Y/N)						
<b>Softwares</b>						
ORCA SMS SYSTEM(MAIN/SUB/StandAlone/NO)						
MS-OFFICE						
<b>Peripherals</b>						
<b>Laser Printer</b>						
Single or Multipul function, B/W or Color						
<b>Inkjet Printer</b>						
Single or Multipul function, B/W or Color						
<b>Scanner install</b>						
Install Driver/standard soft/quality adjust						
Printer						
Scanner						

Network Diagram Plan  
(Free Form)



