MyriadSea

Information Security Management System

CONTENTS

1 Information Security Management

1.1 Purpose

This procedure shall ensure that we will be able to identify the cyber risks and to mitigate their impact to Company's business by applying respective precaution measures based on Information Security Risk Assessment.

1.2 Scope

The Information Security Management System (ISMS) includes inventories of THE ENTITY's Information Technology (IT) and Operations Technology (OT) Systems, specifies the general rules and controls which will protect Corporate and Vessels Operations from cyber threats.

1.3 Senior Roles

The Company Cyber Security role is to be assigned by THE ENTITY

The Ship Cyber Security Officer role is to be assigned by the ships master.

1.4 Responsibilities

Note: Segregation of duties and areas of responsibility reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

The Company Cyber Security Officer shall support Ship Cyber Security Officers.

The Ship Cyber Security Officer shall do the following:

1) Implement, test, and review an organization's information security in order to protect information and prevent unauthorized access.
2) Inform crew about security measures
3) Explain potential threats
4) Install software
5) Implement security measures
6) Monitor networks
7) Be Emergency Response Team Member
8) Manage incidents onboard and fill in incident form

1.5 Regulations and Restrictions

The ISMS is an outcome of below applied international standards and guidelines:

- BS ISO/IEC 27001
- GCHQ 10 STEPS
- UK CYBER ESSENTIALS
- UK ICO PRETECTING DATA
- NIST 800-53 REV.4
- BIMCO
- IMO Guidelines
- ISPS Code

1.6 Definitions

THE ENTITY	MyriadSea GmbH
Authorized User **User (or Client)**	Any employee, contractor, agent, temporary worker, vendor and any person in a position to know or obtain information about computers or devices on the Local Area Network (LAN)
Back up process	Method of protecting the Company against data loss, in cases of sever system malfunctions or inadvertent misuse of applications.
Critical IT /OT systems	any vessel's equipment and installed software which considered integral part of Company' property. Information and Operation Technology Systems include, but not limited to, network, communication, bridge, propulsion systems, workstations together with applications such as email, internet and charts software
Data Owner	Data Owner is the person that can authorize or deny access to certain data, and is responsible for its accuracy, integrity and timeliness. The data owner is responsible for understanding what information is brought into a system, assigning meanings to data collections and constructing and modifying data models.
Firewall infrastructure	Hardware or software device which protects the ports of computer on the LAN Remote access to the Local Area Network from any location outside the firewall by any method, including but not limited to Virtual Private Network (VPN), dial-in modem, frame-relay, SSH, cable-modem and any other method of accessing the LAN from outside the firewall. Firewall located between Internet and THE ENTITY's internal network.
Information Technology Systems	Systems designed to collect, process, store, and distribute information.
IT/OT Change	Change is any task or action that can alter the organization's IT /OT production environment.
LAN	Local Area network
Operational Technology Systems	The hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices
Patch management	Patch Management is a method of protecting the Company against numerous of security threats regarding IT systems
Remote access	Any access to THE ENTITY's network through a non-ENTITY controlled network, device, or other medium
Sensitive Information	The Username or password of computer equipment and of each individual application and networking infrastructure (e.g. Firewall name or IP address, dial-in numbers, etc.).
Third Party	Third party (contractors, providers, consultant etc) is any person not directly employed by THE ENTITY.
Virus	Virus: It is a small program that executes and replicates itself, and often it places itself in the execution path of the computer. Some viruses are programmed to damage the computer programs, delete files, or re-format and totally destroy the hard disk. Others are designed not to damage, but replicate themselves and make their presence known by presenting text, video and audio messages. A virus can significantly degrade the performance of computers and generally result to unpredictable computer behaviour.
WAP	Wireless Access Point

2 Policies Statement

All Users of THE ENTITY shall comply with the following policies:

Information Security and Acceptable Use policy	• Use these assets only with appropriate authorization and only for approved business and operational purposes • Comply with system operating policies and procedures • Ensure that third parties using onboard operational systems comply with Company's set security standards • Protect data, software and documentation in your custody from unauthorized access, copying or distribution • Assure that you maintain the confidentiality, integrity and availability of information for business processes • Comply with legislative and regulatory requirements as defined in Information Security Management System • Ensure attendance of information security awareness training course • Report promptly of any suspicious or harmful activities, related to Company systems
Access Policy	This system operating policy requires that you will take all actions to secure and control access to Company's IT systems, guided by the Access Procedures noted in Section 4
Antivirus Policy	Ensure that proper technical and business practices are in place to identify and eliminate computer virus infections from THE ENTITY computer and onboard operational equipment systems, guided by the Antivirus and Patch Management Procedure noted in Section 5
Internet Security Policy	Ensure appropriate protection and usage of the Company's Computing system, including the onboard operational equipment and telecommunication network, as guided by Network and Internet Security Procedures noted in Section 6
Information Security Policy	Handle all THE ENTITY's sensitive information and operational data in a proper way, whether transmitted within organization or to a trusted third party, as guided by Information Security Procedure noted in Section 7
Back up Policy	Guarantee Company's business continuity through back up THE ENTITY's data on a regular basis
Information System Management and Malfunction Handling Policy	Manage IT and OT assets properly and solve malfunctions in a timely manner with the guidance of IISO and IT department
Information Security and Technology Change Management Policy	Manage fault-free changes with minimal business impact to IT and OT systems.
Information Security Risk Assessment policy	Ensure that identify and manage the risks which have impact to THE ENTITY IT systems ashore and onboard

3 Asset Management

3.1 Purpose

The objective is to identify the organizational assets (IT systems and devices) along with the appropriate ownership. Also, to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

3.2 Scope

It includes the inventory, ownership and return of assets

3.3 Asset Management Procedures

IT Dept. personnel shall ensure the following:

1) Develop a list of IT systems and information processing facilities, with below information:
    a. Asset Name
    b. Product
    c. Vendor Name
    d. Asset State, category and type
2) Collect all information for such inventory including related ownership and version details
3) Maintain up-to-date inventory lists by reviewing appropriateness of Asset, and availability, on an annual basis
4) Ensure that the asset Owner has acknowledged the Information and Acceptable Use policy

4 Access Procedures

4.1 Purpose

The purpose is to ensure Authorized User Access (network and physical) and Prevent unauthorized access to systems, services and information processing facilities.

4.2 Scope

Access includes network, internet, password security, physical security, remote access and access control procedures.

4.3 Password Security Procedures

IT Dept. personnel (or Master) shall do the following:

1) Provide a temporary username/password to first-time vessel users
2) Provide a temporary username/password to those requiring password reset
3) Implement authentication mechanisms on all IT systems
4) Set password principles such as:
    a. Consist of at least eight characters
    b. Contain at least three different character types: Lower case, upper case, digit or special character
    c. Differ from the last eight passwords that used
    d. Expire every six months at the latest, in line with Corporate Policy
5) Maintain log files of user activities in all IT systems
6) Monitor available logs periodically such as active directory logs (failed login attempts)

All Authorized Users shall do the following:

1) Do not use passwords with the following characteristics:
    a. First or last names, or combinations thereof;
    b. Names of an Authorized User's children or pets
    c. Words found in dictionary, combinations of dictionary words with a sound alike digit (second2, etc.)
    d. Use of words or variants on the word password, admin, update, access, login, computer, terminal, workstation, work, home etc.
2) Change immediately after the first login for making it unique for the user, if system permits

Note: System locks User Account after three (3) failed logon attempts (faulty logon ID both password), as applicable. The lockout period depends on the system. ie the account lockout duration for Microsoft Windows is 15 min.

Caution: Change the password immediately if accounts or passwords compromised

3) Report the incident to Ship Cyber Security Officer

    Caution: Do not leave a written password in proximity to the computer or device which the password access

4) Do not ever provide your login or email password to anyone, including family members and allow another user to log on using their system identification
5) Do not attempt to access an area, ie folders, not authorized for your use
6) Do not leave your computer terminal logged on in your absence

4.4 Physical Security Procedures

Ensure restrictions to the physical access to IT facilities as follows:

1) Guard entrance to secure and restricted areas
2) Ensure that visitors are always escorted while within the facilities
3) Restrict access to IT facilities to approved personnel

4.5 Remote Access Procedures

All Authorized Users shall do the following:

1) Remote access to vessel network and systems is allowed in accordance with the Remote Access policy.

Caution: Do not send Company's email using third party email services such as Gmail, Hotmail etc.

4.6 Access Control Procedures

IT Department restricts the access to IT systems for Authorised Personnel as follows:

1) Establish different levels of access (user profiles) to view and update data
2) Give only sufficient rights to all systems to enable them to perform their job function.

Note: Keep always User rights to a minimum. Where possible no one person will have full rights to any system

3) Do not assign to non-IT members, on the operating systems, databases of Company's Infrastructure
4) Control network/server administrator account.
5) Review Super Users access every two years
6) Issue or remove the employee's rights to all systems, if change occurs
7) Limit the access for third parties to the vessels network and applications to the information, services and computing resources required for the fulfilment of the third party job functions.

5 Antivirus and Patch Management Procedure

5.1 Scope

It includes the following procedures:

- Antivirus Network Infrastructure Procedures
- Antivirus Scanning Procedures
- Patch Management Procedures

5.2 Antivirus Network Infrastructure Procedures

IT Dept. personnel shall do the following:

1) Use approved antivirus software and End Point Protection
2) Configure all Ship's computers, including fixed workstations and laptops, with anti-virus software at the time the computer issued
3) Ensure personal computers are segregated from the Ship Network via a non-connected LAN

Warning - users must not attempt to install any other anti-virus software

4) Provide capability of approved antivirus software to receive the latest updated versions

5.3 Antivirus Scanning Procedures

IT Dept. personnel shall do the following:

1) Implement version and patch level controls using centralized configuration management
2) Ensure implementation of scanning method for all office computers
    a. Automatic scan for every file placed on User's computers
    b. Weekly full scans on Managed clients and daily full scans for servers

5.4 Users' Prevention Rules

All Authorized Users shall take additional measures as follows, since even though the antivirus software proven to be effective at detecting and stopping virus infections, it cannot be considered "fool proof":

1) Be suspicious of any unexpected e-mail or file attachments – even if the e-mail comes from someone you know and trust. E-mail and attachments are currently the most common virus delivery mechanism and the e-mail containing them is often generated automatically without the sender even being aware that it is happening.
2) Be cautious when downloading files from the Internet. Most reputable businesses include anti-virus measures on their websites, but very few will make guarantees that downloads from their site are "virus free".
3) Not disable virus protection on their equipment for any reason
4) Do not forward to anyone, either within the vessel network or outside the Company spam, chain letters, or other junk mail
5) Ensure that the automatic update functionality of the anti-virus software is working and that the computer has the latest upgrades and patches.

5.5 Patch Management Procedures

IT Dept shall do the following:

1) Update the operating system where possible
2) Run up-to-date antivirus protection
3) Schedule and distribute patches within Company's computers and applications

Warning - do not use obsolete or unsupported operating systems and software i.e. Windows XP

6 Network and Internet Security Procedure

6.1 Purpose

The Internet access facilities provided by the Company to its employees are the property of the Company. These access facilities are intended to be used for conducting business on behalf of the Company.

6.2 Scope

The aim is to adequately manage and control the Company's networks in order to protect them from threats. Also, to maintain the security for the systems and applications using network, including information in transit.

6.3 Network and Internet Security Procedures

IT Dept. personnel shall do the following:

1) Conduct layered defences such as:
    a. Penetration tests and vulnerability scanning
    b. Security protection on wireless networks
    c. Network segmentation
    d. Utilise the services of a recognised maritime service provider to manage threats at the perimeter of the network, for example KVH's Cybersecurity Program or similar security-based offerings
2) Use internet firewall infrastructure to ensure an effective protection against suspicious incoming and outgoing traffic according to vendor guidelines where applicable

6.4 Restrictions

Some limited use of these internet facilities for personal purposes is permitted, however, provided such use does not:

- Interfere with the employee's ability to perform their expected duties
- Cause undue slowdowns or performance degradations for other users
- Expose the Company to harm or embarrassment

Management authorize IT Dept. Personnel to do the following:

1) Block access to any Internet site which may be inappropriate or pose a risk to the integrity of the Company's networks or reputation
2) Monitor employee usage of the Company's Internet access facilities for compliance

End Users shall not do the following:

3) Change the network connection of a business computer
4) Connect a non-approved computer to the business network
5) Activities which deem unproductive by Company
    a. Use foul/obscene/offensive language/material
    b. Harassing, insulting others
    c. Violation of laws (copyright and others)
    d. Accessing sex/pornography/offensive and other improper materials
    e. Hacking, damaging computers
    f. Misrepresenting yourself / facts or others
6) Access/upload/download materials which could be abusive to other employee
    a. These include, but not limited to material such as jokes, harassments or discrimination of a certain group of people based on:
        - Sex;
        - Race;
        - National origin;
        - Ethnic;
        - Age;
        - Physical Ability/Appearance;
        - Sexual Orientation;
        - Religion;
        - Political Affiliation;
        - Marital/Family/Social Status;
        - Language;
        - Disability;
        - Medical Status/Conditions; or
        - Any other action that prohibited by law

7 Information Security Procedure

Management urge all Employees/Users to comply with the following procedures referring to sensitive data and IT related information:

1) Treat as suspicious any request from any third party not personally known, even it may seem inconvenient or rude.
2) Avoid to upload/save/send Company's confidential and/or sensitive material to the public or any locations which considered not appropriate or insecure.
3) Store paper and removable computer media containing THE ENTITY's confidential data in lockable storage when not used

Note: Any caller not personally known to the Employee who requests Sensitive Information must be referred to the appropriate department head or Partner, without giving such person the name of such appropriate department head or Partner. If such referral is not possible or practical, then the Employee must request from the caller a call-back number, to be given to the appropriate department head or Partner, without giving such person the name of such appropriate department head or Partner

Caution: Never tell Third party or a Caller, even the most seemingly innocuous detail about the THE ENTITY Information Technology "Sensitive Information" such as:

- any details including but not limited to server names, Internet Service Providers, telephone provider, email server information (including email server name), printer type, computer brand, router type or brand;
- the name of your Information Technology specialist, whether that Information Technology person is in-house or contracted;
- the name of any Wireless Access Point (WAP) SSID; never confirming the presence of a Wi-Fi WAP

8 Removable Media Security Procedure

Removable media usage onboard should be in accordance with the guidelines below:

1) Only company issued USBs can be used on vessel computers – personal USB keys and mobile phones must not be connected to vessel computers and OT systems
2) USBs should be used for their dedicated usages, such as ECDIS chart update, and should be labelled as such
3) USBs used for OT, such as ECDIS or engine monitoring, should be scanned for viruses immediately before connection to the OT system
4) Always check with ship master if not sure whether a USB stick can be used.
5) USB devices are automatically scanned by the Antivirus software

9 Back Up

9.1 Back Up Procedures

Perform regular back-ups of critical data on reliable media, as follows:

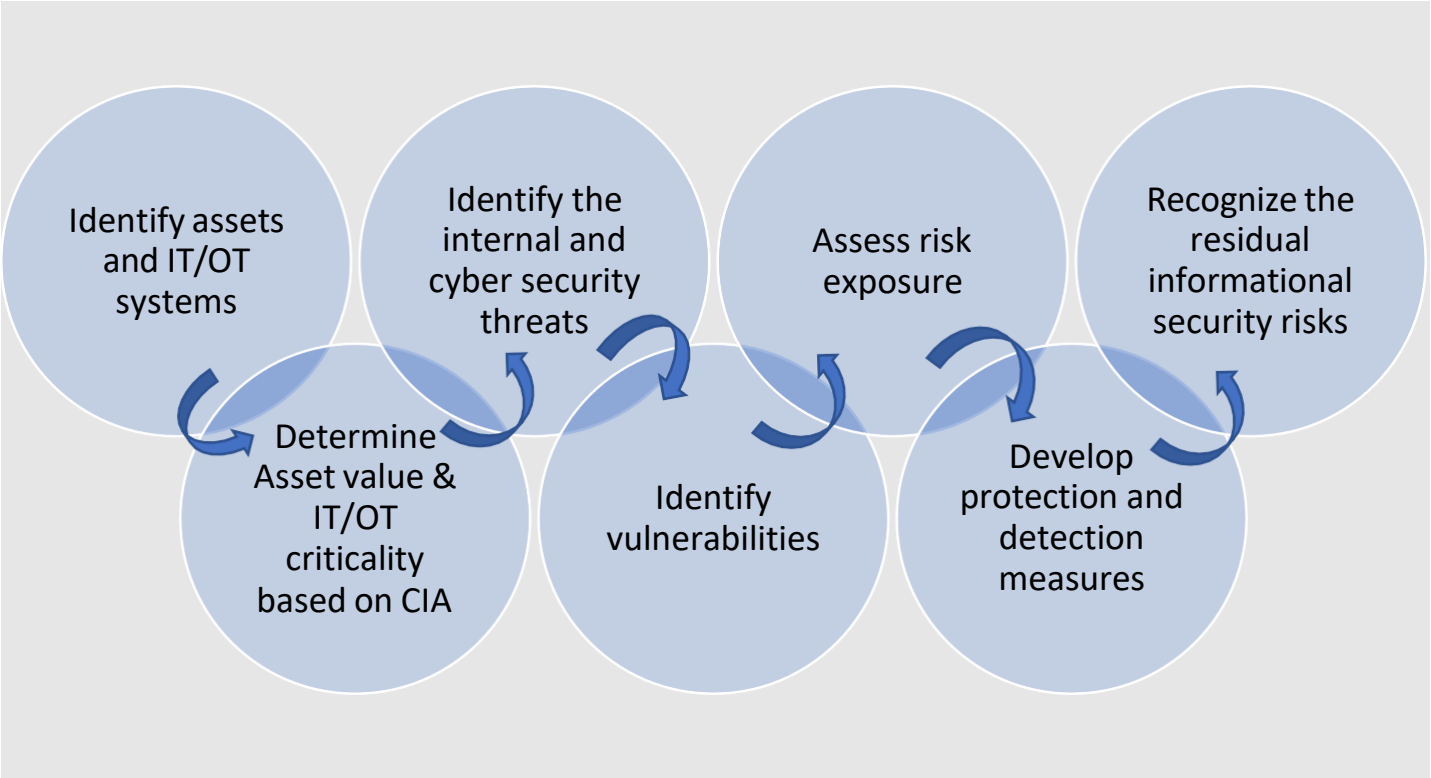
1) Perform back-ups according to defined frequency
2) Store data at a location with a limited access to only Authorized personnel
3) Perform tests to ensure safe restorage of the data backed up, if needed

Location/Type	Frequency	Action
THE ENTITY Vessels	Daily Backup	Perform automatically daily back to SMS, common data and email
	Weekly Backup	Perform backup replication of vessel's servers (as applicable)
	Monthly Backup	Perform Image backup of critical IT/OT systems (ie. Email Server, Electronic charts workstation, loading computer)

10 Information Security Risk Assessment

10.1 Purpose

The objective of Company's Safety Management System is to provide a safe working environment by establishing appropriate safe practices and controls on a risk-based and business-focused approach. Risk assessment cycle is as follows:



10.2 Scope

Information Security Risk assessment process is in line with Company's Risk assessment procedures in general terms but additional elements added to meet the scope of Confidentiality, Integrity and Availability.

10.3 Risk Assessment and Treatment Procedures

ICT Dept. Personnel in collaboration with Ship Manager shall do the following:

1) Identify assets and map with IT/OT systems and functions
2) Evaluate asset value and conclude on criticality of IT/OT systems based on critical risk factors
3) Determine Confidentiality, Integrity and Availability of IT/OT systems concluding on Asset Security Impact
4) Identify the internal and cyber security threats posed to ship
5) Identify vulnerabilities by:
    a. Developing inventories of onboard systems with direct and indirect communication links
    b. Understanding the consequences of security threats on these systems
    c. Understanding the capabilities and limitations of existing protection measures
6) Assess risk exposure by:
    a. Determining the likelihood of vulnerabilities by external and internal threats
    b. Determining the security and safety impact of any individual or combination of vulnerabilities exploited
7) Develop protection and detection measures
8) Assign mitigation measures to reduce the likelihood of vulnerabilities
9) Assign mitigation measures to reduce potential impact vulnerabilities
10) Recognize the residual informational security risks
11) Obtain Risk Owner’s approval and acceptance
12) Closely monitor and manage vulnerabilities to achieve that they remain on acceptable risk level on annual basis and as deem necessary
13) Share risk assessment results with all masters across the fleet
14) Enforce annual onboard study and review of the risk register and encourage feedback for further improvements

11 Organization of Information Security

11.1 Communication procedures

Ship Cyber Security Officer shall do the following:

1) Facilitate redistribution of cyber security related learning materials to the crew, from reputable sources
2) Keep updating the Users for potential cyber threats, security events by sending emails
3) Maintain communication with local authorities as per indicated in Ship Security manual (SSP)

12 Documentation

12.1 Purpose

ISMS documentation will follow Company's guidelines and procedures including distribution, access, retrieval, control of changes, retention and disposition.

12.2 Scope

It includes the creation, maintenance, and management of ship IT and OT system logs

12.3 Documentation records

ICT Dept. Personnel retain and records the following:

- Antivirus exceptions
- Back up Records
- Windows logon/logoff Audit Logs
- Alerts
- Inventory Lists

13 Training and Competence

13.1 Purpose

THE ENTITY understands the value that properly trained and competent individuals will contribute to recognize and manage any potential risk to IT Systems. Security is not an option.

13.2 Objectives

The Objectives of the awareness and training program are to:

1) Make personnel aware of the value and importance of data resources and assets
2) Reduce the risk of human error causing the failure of any installed security measures
3) Make personnel aware of information security responsibilities

13.3 Scope

The security framework contains specific direction and instructions on the requirements to ensure that all Users shall attend an awareness training even as electronic material or in classroom. The specific details of such training scheme exist in Company's training matrix.

13.4 Training Requirements

Ship Master should ensure all onboard crew receive the training below:

- Cyber Security online training defined by the Company
- Information shared by Fleet IT team

14 Monitoring, Measurement, Analysis and Evaluation

14.1 Purpose

The Review process thoroughly analyses ongoing risk management (incidents, disaster events, policy exception request, monitors threats and trends, possible changes to IT systems and information facilities, changes in laws and regulations) and ongoing program effectiveness (compliance self-assessments, audit findings, Security Plans) to ensure that meet the overall objectives.

14.2 Scope

It includes the following procedures:

- Internal Audit procedures
- Management Review meetings

15 Internal Audit Procedures

15.1 Scope

Internal Audit scope is to verify that onboard personnel is familiar with relevant information security procedures and comply with set standards as well as infrastructure remains at the proper condition to meet such requirements.

15.2 Auditors Qualifications

Auditors shall do the following;

- Have the minimum amount of knowledge about the process and the segregation of duties allows it
- Validate that onboard personnel comply with all identified security controls and operations processes in correct and efficient way in their daily job.

15.3 Auditors Process

The quality audit process for ISMS follow Company's Internal procedure as described in System. In case of any non-compliance occur during any type of internal audit, auditors advise Ship Cyber Security Officer and Departmental Manager accordingly and record it for further follow up and close out.

15.4 Management Review Procedures

Management Review is an integral part of Company's Review Process. The Ship Cyber Security Officer shall do the following:

1) Compile information and data minimum but not the least:
    a. From onboard potential threats and issues
    b. Suppliers questionnaires compliance status
    c. Potential contract and project Management interrelated issues
    d. Compliance with product and service requirements
    e. New Rules, Guidelines
    f. Audits Results
    g. Trend Analysis of the data
    h. Status of improvements and innovations
    i. Inventories update
    j. Tickets results
2) Review appropriate security policies, standards and any other security requirements achieving comments within Manager's area of responsibility
3) Review of Risk Assessment and security posture (assets, threats, vulnerabilities, applied controls)

16 Business Continuity

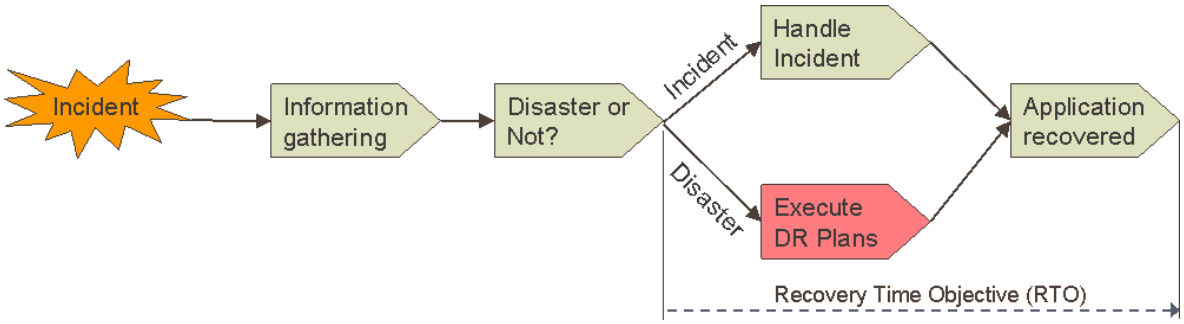
16.1 Redundancy Procedures

Responsible personnel shall do the following:

1) Store back up media in a safe location
2) Perform back up restoration periodically
3) Validate status of back up process upon completion by checking logs or automated emails

16.2 Definition of Disaster

A sudden, unplanned incident causing great damage or loss i.e. any event that creates an inability on an organizations part to provide critical business functions for a period of time. During this period the business and IT divert from normal production responses and execute the disaster recovery plan.



Examples of incidents that may result in disaster are:

- Unavailability of all onboard computers
- Physical damage to one or more computer disks and/or CPU's

16.3 Emergency Response / Incident Management Procedures

ICT Manager shall do the following:

1) Receive initial notification from captain and review incident form

Note: Notification must include how incident occurred, which IT system affected and how, the impact extent to the business, to what extent any threat to systems remain

2) Identify the issue /declare the disaster if it is information security incident
3) Try to clean, recover restore systems and data with the aim to make them operational
4) In case that IT/OT cannot reverse to operational condition, activate the IT emergency plan
    a. Inform all emergency team members
    b. Establish Communication channels with all parties as described in emergency plan
5) Assign investigation team
6) Gather information to support decision on actions for recovery and restore system following the main principles of Company's incident investigation procedures
7) Implement Plan actions
8) Provide updates to Management along with disaster status and recovery level
9) Prevent reoccurrence by addressing any inadequacies in technical and procedural procedures
10) Share Lesson Learnt internally