| QUALITY STANDARD SYSTEM MANUAL | HALCYON MARINE HEALTHCARE SYSTEMS | DOCUMENT NO. MIS 4.0 | EFFECTIVITY DATE: September 19, 2018<br>REVISION NO.: 2 |
|---|---|---|---|
| | | PREPARED BY:<br>Marilar F. De Guzman, MD<br>QAM | APPROVED BY:<br>Glennda E. Canlas, MD<br>Medical Director |

**SUBJECT: HMHS IT SECURITY POLICY AND STANDARDS**

## 1.0 OBJECTIVES

- To protect Halcyon Marine Healthcare Systems business information, clients and customer information within its custody by safeguarding its confidentiality, integrity and availability;
- To establish safeguards to protect Halcyon Marine Healthcare Systems information resources from theft, abuse, misuse and any form of damage;
- To establish responsibility and accountability of Information Security in Halcyon Marine Healthcare Systems;
- To encourage management and staff to maintain awareness, knowledge and skills to minimize the occurrence of severe Information Security incidents;
- To continually strengthen and improve the overall capabilities of the Information Security Management System;
- To increase professional skills in Information Security Management and Technology.

## 2.0 I.T. SECURITY POLICY AND STANDARDS

IT Security Policy and Standards are designed to protect Halcyon Marine Healthcare Systems Inc, employees, customers and partners from harm, caused by the misuse of IT systems and data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of systems can be severe. Potential damages includes but not limited to malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and loss of productivity resulting to network downtime.

Employees are responsible for the security of IT systems and the data. They must ensure that they adhere to the guidelines of this policy at all times.

## 3.0 COMPLIANCE TO POLICY

### 3.1 Compliance Measurement

The MIS Department, Quality Assurance Department and Internal Auditors will verify the compliance of this policy through various methods, including but not limited to business tool reports, internal and external audits, and feedback to the policy owner.

### 3.2 Exceptions

Any exception to the policy must be approved by the MIS Team.

### 3.3 Non-Compliance

An employee that violates this policy may be subjected to disciplinary action.

## 4.0 POLICIES AND STANDARDS

### 4.1 General Security Policy

#### A. Acceptable Use Policy

The intention of Management Information Systems for publishing an Acceptable Use Policy is not to impose restrictions contrary to Halcyon Marine Healthcare Systems established culture of openness, trust and integrity. Management

Information Systems is committed to protect the employees, partners and the company from illegal action of individuals either knowingly or unknowingly.

The Internet, Intranet and Extranet-related systems that include but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of Halcyon Marine Healthcare Systems. These systems are used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee of Halcyon Marine Healthcare Systems and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines to conduct their activities accordingly.

**1. Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at Halcyon Marine Healthcare System. These rules are in place to protect the Halcyon Marine Healthcare System and its employees. Inappropriate use of computer exposes Halcyon Marine Healthcare System to risks including virus attacks, compromise of network systems and services and legal issues.

**2. Scope**

This policy applies to the use of information, electronic and computing devices and network resources to conduct Halcyon Marine Healthcare

Systems' business or interact with internal networks and business systems either owned or leased by Halcyon Marine Healthcare Systems, employee or a third party. All employee, consultant, external provider and subsidiaries of Halcyon Marine Healthcare Systems are responsible for exercising good judgment in appropriate use of information, electronic devices and network resources in accordance to Halcyon Marine Healthcare Systems policies and standards, local laws and regulations.

This policy also applies to all employee, external provider, consultant, staff affiliated with third parties and equipment owned or leased by Halcyon Marine Healthcare Systems.

3. **Policy**

**3.1 General Use and Ownership**

**3.1.1** Halcyon Marine Healthcare Systems proprietary information stored in electronic and computing devices either owned or leased by an employee or a third party remains the sole property of Halcyon Marine Healthcare Systems. It must ensure that the legal and technical proprietary information is protected in accordance to *Data Protection Policy*.

**3.1.2** Employees have the responsibility to report theft, loss and unauthorized disclosure of Halcyon Marine Healthcare Systems proprietary information.

**3.1.3** Employees may access, use and share Halcyon Marine Healthcare Systems proprietary information if it is authorized and necessary to fulfill their assigned duty.

**3.1.4** Employees are responsible for exercising good judgment in reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet, Intranet and Extranet systems. In the absence of such policies, employees should be guided by departmental policies for personal use and if there is any uncertainty, employees should consult their supervisor or manager.

**3.1.5** For security and network maintenance purposes, authorized individuals within Halcyon Marine Healthcare Systems may monitor equipment, systems and network traffic at all time as per IT Security *Audit Policy and Server Audit Policy*.

**3.1.6** Halcyon Marine Healthcare Systems reserves the right to audit networks and systems on a periodic basis to ensure compliance to this policy.

**3.2 Security and Proprietary Information**

**3.2.1** All mobile and computing devices that are connected to the internal network must comply within the *Network Security Policy*.

**3.2.2** System level and user level passwords must comply with the Password Construction Guidelines and *Password Protection Policy*. Providing access to another individual either deliberately or through failure to secure its access is prohibited.

**3.2.3** All computing devices must be secured with a password-protected screen saver with an automatic activation feature that is set at 10 minutes or less. Screen must be locked or user must be logged off from the device if unattended.

**3.2.4** Posts from employees to newsgroups using the Halcyon Marine Healthcare Systems email address should contain a disclaimer stating that "the opinions expressed are strictly of their own and not necessarily from Halcyon Marine

Healthcare Systems" unless the posts are in line with their business duties.

**3.2.5** Employees must be in extreme caution when opening an e-mail attachment received from an unknown sender. These e-mails may contain malware.

### 3.3 Unacceptable Use

The following activities are in general and prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., Systems Administration Staff needs to disable the network access of host if the host is disrupting the production services). Under no circumstances, an employee of Halcyon Marine Healthcare Systems is authorized to engage in any activity that is illegal under local, state or international law while utilizing Halcyon Marine Healthcare Systems owned resources.

The lists below are by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

#### 3.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1) The violation of rights of any person or company protected by copyright, trade secret, patent or other intellectual property, similar laws or regulations, including but not limited to the installation or distribution of "pirated" or other software products that are not licensed for the use of Halcyon Marine Healthcare Systems.

2) Unauthorized copying of copyrighted material including but not limited to digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and installation of any copyrighted software which the Halcyon Marine Healthcare Systems or end user does not have an active license is strictly prohibited.
3) Accessing data, server or an account for any purpose other than conducting Halcyon Marine Healthcare Systems business even if you are authorized is strictly prohibited.
4) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is

illegal. The appropriate management should be consulted prior to export of any material. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5) Revealing the account password or allowing other employee to use your account. This includes family and other household members when work is being done at home.
6) Using of Halcyon Marine Healthcare Systems computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7) Making fraudulent offers of products, items or services originating from any Halcyon Marine Healthcare Systems account.
8) Making statements about warranty, expressly or implied unless it is part of normal job duties.
9) Effecting security breaches or disruption of network communication. Security breach include but not limited to accessing data which the employee is not the intended recipient and logging to the

server or account that the employee is not expressly authorized to access unless these duties are within the scope of their regular duties. For purposes of this section, "disruption" includes but not limited to network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10) Port scanning or security scanning is expressly prohibited unless prior notification to MIS personnel is made.
11) Executing any form of network monitoring which intercepts data that are not intended to employee's host unless this activity is part of the employee's normal job/duty.
12) Circumventing user authentication or security of any host, network or account.
13) Introducing honeypots, honeynets, or similar technology in Halcyon Marine Healthcare Systems network.
14) Interfering with or denying service to any user other than the employee's host (e.g, denial of service attack).

15) Use of any program, script, command or sending messages of any kind with the intent to interfere with, or disable the user's terminal session via any means locally or via the Internet, Intranet and Extranet.
16) Providing information about Halcyon Marine Healthcare Systems employees to other parties outside Halcyon Marine Healthcare Systems.

### 3.3.2 Email and Communication Activities

When using the company resources to access Internet, users must remember that they represent the company. Whenever the employees state an affiliation to the company, they must also clearly indicate that "the opinion expressed are my own and not necessarily those of the company".

Questions may be addressed to the MIS Department.

1) Sending unsolicited email messages, including sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3) Unauthorized use or forging of email header information.
4) Solicitation of email for other email addresses using the poster's account with the intent to harass or to collect replies.
5) Creating or forwarding "chain letters", "Ponzi" and any type of "pyramid" schemes.
6) Use of unsolicited email which originates from Halcyon Marine Healthcare Systems networks or other Internet/Intranet/Extranet service providers on behalf of or to advertise any service hosted by Halcyon Marine Healthcare Systems or connected to Halcyon Marine Healthcare Systems network.
7) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### 3.3.3 Blogging and Social Media

Blogging of employees using Halcyon Marine Healthcare Systems property, systems and personal computer systems

are subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the company's systems to engage in blogging are acceptable provided that it is done in a professional and responsible manner, does not violate the company's policy and not detrimental to the company's best interests and does not interfere with the regular work duties of employees. Blogging from Halcyon Marine Healthcare Systems property is subject to monitoring.

1) Halcyon Marine Healthcare Systems' Confidential Information Policy also applies to blogging. Employees are prohibited to reveal any Halcyon Marine Healthcare Systems confidential and proprietary information, trade secrets or any other material covered by Halcyon Marine Healthcare Systems Confidential Information Policy.

2) Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Halcyon Marine Healthcare Systems and its employees. Employees are also prohibited in making any discriminatory, disparaging,

defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Halcyon Marine Healthcare Systems *Non-Discrimination and Anti-Harassment* policy.

3) Employees shall not attribute any personal statements, opinions or beliefs to Halcyon Marine Healthcare Systems when engaging in blogging. If an employee is expressing his/her beliefs and opinions, the employee may not expressly or implicitly represent themselves as an employee or representative of Halcyon Marine Healthcare Systems.

4) Aside from following all laws pertaining to handling and disclosure of copyrighted or controlled export materials, Halcyon Marine Healthcare Systems trademarks, logos and intellectual property may not be used in connection to any blogging activity.

**4. Related Standards, Policies and Processes**

- Data Classification And Access Control Policy

- Data Protection Standard
- Password Policy

**5. Definitions and Terms**

- **Blog** - is a discussion or informational site published in World Wide Web that consists of discrete entries ("posts") typically displayed in reversed chronological order (the most recent post appears first).
- **Honeypot / Honeynet** - is a computer system that set up to act as a decoy to lure cyber attackers and to detect, deflect or study attempts to gain unauthorized access to information systems.
- **Proprietary Information** - also known as trade secret, it is information that a company wish to keep confidential. Proprietary information includes secret formulas, processes, and methods used in production.
- **Spam** - irrelevant or inappropriate messages sent on the Internet to a large number of recipients.

**B. Clean Desk Policy**

A clean desk policy can be an import tool to ensure that all sensitive and confidential materials are removed from end user's work space and locked away when items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in

the workplace. Such policy can also increase the employee's awareness on how to protect sensitive information.

**1. Purpose**

The purpose of this policy is to establish the minimum requirements in maintaining a "clean desk" – where sensitive and critical information about our employees, intellectual property, customers and vendors are secured in locked areas and offsite. A Clean Desk policy is not only ISO 27001 compliant but, it is also part of the standard basic privacy controls.

**2. Scope**

This policy applies to all Halcyon Marine Healthcare Systems employees and affiliates.

**3. Policy**

3.1 Employees are required to ensure that all sensitive and confidential information in hardcopy or electronic form are secured on their work area at the end of the day and when they are expected to be gone for an extended period.

3.2 All Computers must be locked if the workstation is unoccupied.

3.3 All Computers in workstations must be completely shut down at the end of the day.

3.4 Any restrictive or sensitive information must be removed from the desk and locked in a drawer.

3.5 File cabinets that contain restrictive or sensitive information must be kept closed and locked if not in use or no one is in attendance.

3.6 Keys use to access restrictive or sensitive information must not be left lying around the work area.

3.7 Laptops must be either locked with a locking cable or locked in a drawer.

3.8 Passwords should not be written in sticky notes posted or under the computer or left in accessible location.

3.9 Printouts that contain restrictive or sensitive information must be immediately removed from the printer.

3.10 Restricted and sensitive documents must be shredded or placed in a locked disposal bins.

3.11 Whiteboard that contains restricted and sensitive information must be erased.

3.12 Lock the portable computing devices such as laptops and tablets.

3.13 Ensure that mass storage devices such as CDROM, DVD and USB drives are locked in a drawer.

3.14 All papers of printers and fax machines should be cleared to ensure that sensitive documents are kept confidential.

**C. Password Construction Guidelines**

Passwords are a critical component of information security. Passwords are served to protect the user accounts. However, a poorly constructed password may result to compromise of individual systems, data and network. This guideline provides the best practice in creating a secured password.

**1. Purpose**

The purpose of this guideline is to provide the best practice in creating a strong password.

**2. Scope**

This guideline applies to all employees, contractors and consultants of Halcyon Marine Healthcare Systems. It is also applies to all passwords including but not limited to user-level accounts, system-level accounts, web

accounts, e-mail accounts, screen saver protection, voice mail, and local router log ins.

**3. Statement of Guidelines**

All passwords should meet or exceed the following guidelines.

**Strong passwords have the following characteristics:**

- Contains at least 12 alphanumeric characters.
- Contains both upper and lower case letters.
- Contains at least one number (e.g, 0-9).
- Contains at least one special character (e.g,!$%^&*()_+|~-=\`{}[]:";'<>?,./).

**Poor/weak passwords have the following characteristics:**

- Contains less than eight characters.
- Can be found in dictionary including foreign language, exist in language slang, dialect and jargon.
- Contains personal information such as birth date, address, phone number, name of a family member, pet, friend and fantasy characters.
- Contains work-related information such as name of building, system commands, sites, companies and hardware/software.

- Contains number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contains common words that spelled backwards and followed by a number (e.g, terces, secret1 or 1secret).
- Some version of "Welcome123" "Password123" "Changeme123"

Never write down the password, instead try to create passwords that can easily remember. The other way to create a password is to base it in a song title, affirmation, or any phrase (e.g.'This May Be One Way To Remember" become TmB1w2R! or another variation)

(NOTE: Do not use either of these examples as passwords)

**Passphrases**

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between public key known by all and private key known only to the user. The user cannot access without the passphrase to unlock the private key, .

Passphrase is similar to password in use, however it is relatively long and construct of multiple words which provides a greater security against the dictionary attacks. Strong passphrases should follow the general password

construction guidelines to include upper and lowercase letters, numbers, and special characters (e.g. TheTrafficOnThe101Was*&!$ThisMorning!).

**D. Password Protection Policy**

The Password is an important aspect of computer security. A poorly chosen password may result to unauthorized access and exploitation of Halcyon Marine Healthcare Systems' resources. All users, contractors and vendors that have access in Halcyon Marine Healthcare Systems are responsible for taking the appropriate steps to select and secure their passwords.

1. **Purpose**

The purpose of this policy is to establish a standard strong password, protection of passwords and frequency of change.

2. **Scope**

Personnel is responsible for his/her account (or any form of access that supports or requires a password) that are connected with Halcyon Marine Healthcare Systems.

3. **Policy**

**3.1 Password Creation**

3.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

3.1.2 Users shall not use the same password for Halcyon Marine

Healthcare Systems' accounts (e.g. personal ISP account, option trading, benefits and etc.)

3.1.3 Users shall not use the same password for various Halcyon Marine Healthcare Systems' access.

3.1.4 User accounts that have system-level privileges granted through group memberships or program, such as sudo, must have a unique password for all other accounts held by user to access system-level privileges.

3.1.5 Simple Network Management Protocol (SNMP) is a community string that defines as something other than the standard defaults of public, private, and system. It must be different from the password used to log in interactively. SNMP community strings must meet the password construction guidelines.

**3.2 Password Change**

3.2.1 All system-level passwords (e.g. Root, enable, NT admin, application administration accounts, etc.) must be changed at least on a quarterly basis.

3.2.2 All user-level passwords (e.g. Email, web, desktop computer, and so on) must be changed at least every month. Data Privacy Officer must be given a copy of the changed password.

3.2.3 No repeating of previously used password

**3.3 Password Protection**

3.3.1 Password should keep in private. All passwords are treated as sensitive and confidential for Halcyon Marine Healthcare Systems' information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. *Refer to technical reference*

3.3.2 Password shall not be inserted into any email messages, Alliance cases or other forms of electronic communication.

3.3.3 Password shall not be revealed over the phone to anyone.

3.3.4 Do not reveal the password on questionnaires or any security forms.

3.3.5 Do not put any hint in the format of the password (e.g. My family name).

3.3.6 Do not share the Halcyon Marine Healthcare Systems' passwords to anyone, including the administrative assistants, secretaries, managers, coworkers while on vacation and to family members.

3.3.7 Do not write or place the passwords in office. Do not store in a computer system or mobile devices (phone/tablet) without encryption.

3.3.8 Do not use the "Remember Password" feature of

applications (e.g. Web browsers). Only the MIS personnel will approve the password manager application like Lastpass is allowed to use.

3.3.9 Any user suspecting that his/her password has been compromised, report the incident and advise to change all their passwords.

**3.4 Application Development**

Application developers must ensure that their programs contain the following security precautions:

3.4.1 Applications must support the authentication of individual users not groups.

3.4.2 Applications must not store passwords on a clear text or in any easily reversible form.

3.4.3 Applications must not transmit passwords in clear text over the network.

3.4.4 Applications must provide some sort of role management, such that one user can take over the functions of another without knowing their password.

**3.5 Use of Passwords and Passphrases**

Passphrases are generally used for public/private key authentication. The public/private key system defines a mathematical relationship between the public key known

by all and private key known only to the user. The user will be no access without the passphrase to "unlock" the private key. Passphrases are not the same with passwords. Passphrase is a secured longer version of the password. It is typically composed of multiple words, therefore, passphrase is more secured against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters, numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All rules that apply to passwords will be applied to passphrases.

**4. Related Standards, Policies and Processes**

- Password Construction Guidelines

**5. Definition of Terms**

- **Simple Network Management Protocol (SNMP)** - is a protocol for network management. It is used for collecting information and configuring network devices such as servers, printers, hubs, switches, and routers in an Internet Protocol (IP) network.

**E. Acceptable Encryption Policy**

**1. Purpose**

The purpose of this policy is to provide guidance on limiting the use of encryption to algorithms that receives substantial public review and proven to work effectively. In addition, this policy provides direction to ensure that IT regulations are followed. Legal authority is granted for the dissemination and use of encryption technologies.

## 2. Scope

This policy applies to all employees and affiliates of Halcyon Marine Healthcare Systems.

## 3. Policy

### 3.1 Algorithm Requirements

3.1.1 When using Ciphers, it must meet or exceed the set defined in "AES-compatible" or "partially AES-compatible" according to IETF/IRTF Cipher Catalog, or the set defined in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to date of implementation. The use of Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

3.1.2 When using Algorithms, it must meet the standards defined in NIST publication FIPS 140-2 or any superseding document according to date of implementation. The use of RSA and Elliptic Curve Cryptography (ECC) algorithms are strongly recommended for asymmetric encryption.

3.1.3 Signature Algorithms

| orithm | Length n) | ditional Comment |
|---|---|---|
| DSA | 56 | co Legal recommends RFC6090 compliance to avoid patent infringement. |
| | 8 | st use a secured padding scheme. PKCS#7 padding scheme is recommended. Message hashing is required. |
| VM | 256 | er to LDWM Hash-based Signatures Draft |

### 3.2 Hash Function Requirements

In general, Halcyon Marine Healthcare Systems adheres to the NIST Policy on Hash Functions.

**3.3 Key Agreement and Authentication**

3.3.1 Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE and Elliptic Curve Diffie-Hellman (ECDH).

3.3.2 End points must be authenticated prior to the exchange or derivation of session keys.

3.3.3 Public keys used to establish trust must be authenticated prior to use. Example of authentication includes transmission via cryptographically signed message or manual verification of the public key hash.

3.3.4 All servers used for authentication (e.g. RADIUS or TACACS) must install a valid certificate signed by known trusted provider.

3.3.5 All servers and applications using SSL or TLS must have a certificate signed by a known trusted provider.

**3.4 Key Generation**

3.4.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

3.4.2 Key generation must be seeded from an industry standard's Random Number Generator (RNG).

**4. Related Standards, Policies and Processes**

National Institute of Standards and Technology (NIST) publication FIPS 1402,

NIST Policy on Hash Functions

**5. Definitions of Terms**

- Proprietary Encryption

**F. End-user Encryption Key Protection Policy**

Encryption Key Management can lead to compromise and disclosure of private keys used to secure sensitive data if not properly done. All users should understand that it is important to encrypt certain documents and electronic communications.

**1. Purpose**

This policy outlines the requirements in protecting encryption keys under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outline includes the operational and technical controls such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

**2. Scope**

This policy applies to any encryption keys and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

- encryption keys issued by Halcyon Marine Healthcare Systems
- encryption keys used for Halcyon Marine Healthcare Systems business
- encryption keys used to protect data owned by Halcyon Marine Healthcare Systems

The public keys contains in digital certificates are specifically exempted from this policy.

**3. Policy**

All encryption keys covered by this policy must be protected to prevent unauthorized disclosure and subsequent fraudulent use.

**3.1 Secret Key Encryption Keys**

Keys used for secret key encryption are also called as symmetric cryptography. It must be protected, as they are distributed to all parties. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm that has the longest key length to authorize in Halcyon Marine Healthcare Systems' *Acceptable Encryption Policy*. It must be split, if the keys are for the strongest algorithm. Portions of key encrypted has a different key which has authorized the longest key length and each portion is transmitted using a different transmission mechanisms. The goal is

to provide stringent protection on key than the data encrypted with an encryption key.

Symmetric encryption keys must be protected with security measures as stringent used for distribution of keys.

### 3.2 Public Key Encryption Keys

Public Key Cryptography/Asymmetric Cryptography used public-private key pairs. The public key will be passed to certificate authority as an inclusion to digital certificate issued to end user. The digital certificate is available to everyone once issued. The private key will only be available to the end user to whom the corresponding digital certificate was issued.

#### 3.2.1 Halcyon Marine Healthcare Systems Public Key Infrastructure (PKI)

The public-private key pairs used by the Halcyon Marine Healthcare Systems' public key infrastructure (PKI) are generated in tamper-resistant smart card issued to every individual end user. The private key is associated with the end user's identity certificate, which only be used for digital signatures. It prevents MIS Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates

used to encrypt email and other documents, must be escrowed in compliance with Halcyon Marine Healthcare Systems' policies.

Access to private keys stored in Halcyon Marine Healthcare Systems' issued smart card will be protected by a Personal Identification Number (PIN) and known by the authorized person. The smart card software will be configured as a requirement in entering the PIN prior to any private key that contains in a smart card.

**3.2.2 Other Public Encryption Keys**

Another type of keys may be generated in software of the end user's computer and can be stored as files in hard drive or hardware token. If the public-private key pair is generated in smart card, the requirements for protecting the private keys are the same with private keys associated with Halcyon Marine Healthcare Systems' PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and may store any backup copies secured. The user is also required to create an escrow copy of any private keys used for

encrypting data and deliver the escrow copy to the local Information Security representative for a secure storage.

The MIS Team shall not escrow, any private keys associated with identity certificates. All backups, including escrow copies shall be protected with password or passphrase, in compliance with Halcyon Marine Healthcare Systems' Password Policy. MIS representatives will store and protect the escrowed keys.

**3.2.2.1 Commercial or Outside Organization Public Key Infrastructure(PKI) Keys**

In working with business partners, the relationship may requires the end users to use public-private key pairs generated to end user's computer software. In this case, the public-private key pairs is stored on hard drive of end users. The private keys are protected by the strength of a password or passphrase. When an end user requests a digital certificate from commercial PKI such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key will remain in the browser's certificate stored with a password. A web

to password in browser that stores, private keys will be configured require the user to enter the certificate store accessing a private key.

#### 3.2.2.2 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, e.g. a USB drive or a smart card. Since the protection of the private keys is passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

### 3.3 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as a sensitive company equipment as described in Halcyon Marine Healthcare Systems' *Physical Security policy*. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer if not in use. For

end users traveling with hardware tokens, it should not be stored or carried in the same container or bag.

**3.4 Personal Identification Numbers (PINs), Passwords and Passphrases**

All PINs, passwords and passphrases used to protect encryption keys must meet the complexity and length requirements as described in Halcyon Marine Healthcare Systems *Password Policy*.

**3.5 Loss and Theft**

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to the MIS Team. MIS personnel will direct the end user in any actions that will require with regards to revocation of certificates or public-private key pairs.

**4. Related Standards, Policies and Processes**

- Acceptable Encryption Policy
- Password Policy
- Physical Security policy

**5. Definition of Terms**

- **Digital certificate** - is an electronic document used to prove ownership of a public key.

- **Digital signature** - a type of electronic signature that encrypts documents with digital codes that are difficult to duplicate.
- **Key escrow** - is an arrangement in which the keys needed to decrypt encrypted data held in escrow. Under certain circumstances, an authorized third party may have an access to those keys.
- **Public key cryptography** - is an encryption technique that used in pairs public and private key algorithm for a secured data communication.
- **Public key pairs/Symmetric cryptography** - is a cryptography in which a pair of keys are used to encrypt and decrypt the message for security purposes.

**G. Security Response Plan Policy**

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as the coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/ remediation timelines. It requires the business units to incorporate the SRP as part of their business continuity operations, as new products or services developed

and prepared for release to consumers. It also ensures that when an incident occurs, swift mitigation and remediation ensues.

**1. Purpose**

The purpose of this policy is to establish the requirements of all business units supported by the MIS team to develop and maintain the security response plan. This policy also ensures that the security incident management team has all the necessary information to formulate a successful response once a specific security incident occurs.

**2. Scope**

This policy applies to any established and defined business unity or entity within Halcyon Marine Healthcare Systems.

**3. Policy**

The development, implementation and execution of a Security Response Plan (SRP) are the primary responsibility of a specific business unit for in cooperation of MIS Team and Quality Assurance Team. Business units are expected to facilitate the SRP as an accountable to products and services. The Business Unit Security Coordinator is expected to work with MIS Team in the development and maintenance of the Security Response Plan.

**3.1 Service and Product Description**

The product description in SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams and architecture which is useful.

### 3.2 Contact Information

The SRP must include contact information for dedicated team members that is available during non-business hours, incidents occur and escalation. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact of customer. The SRP document must include all phone numbers and email addresses.

### 3.3 Triage

The SRP must define the triage steps in coordination with the Security Incident Management Team in a cooperative manner and with the intended goal of swift security vulnerability mitigation. This step includes validation of reported vulnerability or compromise.

### 3.4 Identified Mitigation and Testing

The SRP must include a defined process for identifying and testing mitigation prior to deployment. These details should include short-term mitigation and remediation process.

**3.5 Mitigation and Remediation Timelines**

The SRP must include the levels of response to identified vulnerabilities that defines the expected timelines for repair based on the severity and impact to consumer, brand, and the company. These response guidelines should be mapped carefully to the level of severity, determined for the reported vulnerability.

**H. Disaster Recovery Plan Policy**

Since disasters rarely happen, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives Halcyon Marine Healthcare Systems a competitive advantage. This policy requires the management to support financially and diligently attends disaster contingency planning efforts.

**I. Removable Media Policy**

Removable media are a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

**1. Purpose**

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by Halcyon Marine Healthcare Systems

and to reduce the risk of acquiring malware infections on computers operated by Halcyon Marine Healthcare Systems.

**2. Scope**

This policy covers all computers and servers operating in Halcyon Marine Healthcare Systems.

**3. Policy**

The staffs of Halcyon Marine Healthcare Systems may only use the company's removable media on their work computers. Halcyon Marine Healthcare Systems' removable media may not be connected or used on computers that are not owned or leased without explicit permission of the MIS staff. Sensitive information should be stored on removable media only when required in the performance of assigned duties or when providing information required by other state or government. When sensitive information is stored on removable media, it must be encrypted in accordance with the Halcyon Marine Healthcare Systems' *Acceptable Encryption Policy*.

Exceptions to this policy may be requested on a case-to-case basis by Halcyon Marine Healthcare Systems' exception procedures.

**4. Related Standards, Policies and Processes**

- Acceptable Encryption Policy

**5. Definition of terms**

- **Encryption** - is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
- **Malware** - software that is intended to damage or disable computers and computer systems.
- **Removable media** - is any type of storage device that can be removed from a computer while the system is running. Example of removable media includes CDs, DVDs and Blu-Ray disks, as well as diskettes and USB drives.

**J. Social Engineering Awareness Policy**

The Social Engineering Awareness Policy bundle is a collection of policies and guidelines for employees of Halcyon Marine Healthcare Systems. The Employee Front Desk Communication Policy is part of the Social Engineering Awareness Policy bundle.

In order to protect Halcyon Marine Healthcare Systems' assets, all employees need to defend the integrity and confidentiality of Halcyon Marine Healthcare Systems' resources.

**1. Purpose**

This policy has two purposes:

2.1 To make the employees aware of (a) fraudulent social engineering attacks, and (b) procedures that employees may use to detect attacks.

2.1.0 Employees are should aware of techniques used for such attacks, and they are given a standard procedure to respond to attacks.

2.1.1 Employees should know who will contact in these circumstances.

2.1.2 Employees recognize that they are an important part of Halcyon Marine Healthcare Systems' security. The integrity of an employee is the best line of defense for protecting sensitive information regarding of Halcyon Marine Healthcare Systems' resources.

2.2 To create a specific procedure for employees to follow to help them make the best choice when:

2.2.0 Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect Halcyon Marine Healthcare Systems' sensitive information.

2.2.1 The employee is being "socially pressured" or "socially encouraged or tricked" into sharing sensitive data.

**2. Scope**

This includes all employees of Halcyon Marine Healthcare Systems, including the temporary contractors or part-time employees participating in help desk customer service.

**3. Policy**

3.1 Sensitive information about Halcyon Marine Healthcare Systems will not be shared to an unauthorized individual if he/she uses words and/ or techniques such as the following:

3.1.1 An "urgent matter"

3.1.2 A "forgotten password"

3.1.3 A "computer virus emergency"

3.1.4 Any form of intimidation from "higher level management"

3.1.5 Any "name dropping" by an individual which gives the appearance coming from legitimate and authorized personnel.

3.1.6 The requester requires the release of information that will reveal passwords, model, serial number, or brand or quantity of Halcyon Marine Healthcare Systems' resources.

3.1.7 The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.

3.1.8 The techniques are used by a person that declares to be "affiliated" with Halcyon Marine Healthcare Systems such as a sub-contractor.

3.1.9 The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.

3.1.10 The requester is using ego and vanity seducing methods. E.g. rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

**3.2 Actions**

3.2.1 All persons described in section 3.0 MUST attend the security awareness training within 90 days from the date of employment and annually thereafter.

3.2.2 If one or more circumstances described in section 4.0 is detected by a person described in section 3.0, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.

3.2.3 If the identity of the requester described in section 5.1.1 CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.

3.2.4 If the supervisor or manager is not available, that person MUST contact the security personnel.

3.2.5 If the security personnel is not available, the person described in section 3.0 MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

**K. Anti virus Guidelines**

Recommended processes to prevent virus problems:

- Always run the Corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" it by emptying the Trash.
- Delete spam, chain, and other junk email without forwarding, in accordance with Halcyon Marine Healthcare Systems *Acceptable Use Policy*.
- Never download files from an unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless it is a business requirement to do so.

- Always scan a removable media from an unknown source before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If business applications conflict with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software then run the application test. After the application test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g. email or file sharing.
- New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this recommended processes list for updates.

**L. Data Classification and Access Control Policy**

All employees who come into contact with sensitive Halcyon Marine Healthcare Systems' internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily Halcyon Marine Healthcare Systems' business activities. Sensitive information is either Confidential or Restricted information, and both are defined later in this document. Although this policy provides an overall guidance, to achieve consistent information protection, employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for Information Security for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

## 1. Purpose

The Halcyon Marine Healthcare Systems data classification system defined in this document is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and a demonstrable business needs to receive the information. This concept, when combined with the policies defined in this document will protect the Halcyon Marine Healthcare Systems' information from unauthorized disclosure, use, modification, and deletion.

## 2. Scope

This data classification policy is applicable to all electronic information which owned by Halcyon Marine Healthcare Systems.

## 3. Procedures

### 3.1 Access Control

**3.1.1 Need to Know**—Each of the policy requirements set forth in this document are based on the concept of need to know. If an employee is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know the concept. Information must be disclosed only to those people who have a legitimate business need for the information.

**3.1.2** **System Access Controls**—The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to Halcyon Marine Healthcare Systems' system and their resources. Remote access shall be controlled through identification and authentication mechanisms.

**3.1.3** **Access Granting Decisions**—Access to Halcyon Marine Healthcare Systems' sensitive information must be provided only after the approval of the Managers and MIS head. Access requests will be presented to the Managers and MIS Head uses the System Access Request form. Custodians of the involved information must refer all requests for access to the relevant owners or their delegates. Special needs for other access privileges will be dealt with on a request-by-request basis. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by relevant Data Owner in accordance with

the systematic review schedule approved by the Management.

**3.2 Information Classification**

**3.2.1 Owners and Product Information**—All electronic information managed by MIS Team must have a designated Owner. Product information is an information routinely used to accomplish business objectives. Owners should be at the Management level or above. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the Halcyon Marine Healthcare Systems' management team who act as stewards, and supervise the ways in which certain types of information are used and protected.

**3.2.2 RESTRICTED**—This classification applies to the most sensitive business information that is intended for use strictly within Halcyon Marine Healthcare Systems. Its unauthorized disclosure could seriously and adversely impact the Halcyon Marine Healthcare Systems' customers, business partners and suppliers.

**3.2.3** **CONFIDENTIAL**—This classification applies to less-sensitive business information intended for use within Halcyon Marine Healthcare Systems. Its unauthorized disclosure could adversely impact Halcyon Marine Healthcare Systems' customers, suppliers, business partners and employees.

**3.2.4** **PUBLIC**—This classification applies to information that has been approved by Halcyon Marine Healthcare Systems' management for release to the public. By definition, there is no such thing as an unauthorized disclosure of information and it may be disseminated without potential harm.

**3.2.5** **Owners and Access Decisions**—Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. MIS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

**3.3 Object Reuse and Disposal**

Storage media that contain sensitive (i.e. Restricted or confidential) information shall be completely empty before reassigning to a different user or disposing it when no longer used. Simply deleting the data from the media is not sufficient. A

method must be used that completely erases all data. It must be destroyed in a manner approved by the MIS Head when disposing of media containing data that cannot be completely erased.

**3.4.1** **Data Center Access**—Access to the data center must be physically restricted to a reasonable and appropriate manner.

**3.4.2** **Facility Access–**All network equipment (routers, switches, etc.) and servers located in the corporate office and in all facilities must be secured when no Halcyon Marine Healthcare Systems' personnel, or authorized contractors, are present. Physically secured is defined as locked in a location that denies access to unauthorized personnel.

**3.5 Special Considerations for Restricted Information**

If Restricted information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must conform to data access control safeguards approved by MIS team and the Management Team. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

**3.5.1 Data Encryption Software**— Halcyon Marine Healthcare Systems' employees and vendors must not install encryption software to encrypt files or folders without the express written consent of MIS Team.

**3.6 Information Transfer**

**3.6.1 Transmission Over Networks**—If Halcyon Marine Healthcare Systems' Restricted data are to be transmitted over any external communication network, it must be sent only in encrypted form. Such networks include electronic mail systems, the Internet, etc. All such transmissions must use a virtual public network or similar software as approved by the MIS Team.

**3.6.2 Transfer To Another Computer**—Before any Restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

**3.7 Software Security**

**3.7.1 Secure Storage of object and source code**—Object and source code for system software shall be securely stored

when not in use by the developer. Developers must not have access to modify program files that actually run in production. Changes made by developers must be implemented into production by Technical Operations. Unless access is routed through an application interface, no developer shall have more than read access to production data. Further, any changes to production applications must follow the change management process.

**3.7.2** **Testing**—Developers must at least perform unit testing. Final testing must be performed by the Quality Assurance team or the target user population.

**3.7.3** **Backups**—Sensitive data shall be backed up regularly, and the backup media shall be stored in a secure environment.

**3.8 Key Management**

**3.8.1** **Protection of Keys** —Public and private keys shall be protected against unauthorized modification and substitution.

**3.8.2** **Procedures** — Procedures shall be in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

**3.8.3 Safeguarding of Keys**—Procedures shall be in place to safeguard all cryptographic material, including certificates. MIS team must be given a duplicate key for safekeeping.

**M. Data Protection Policy**

The Halcyon Marine Healthcare Systems need to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people in an organization that has a relationship with or may need to contact.

This policy describes how personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

**1. Purpose**

This policy helps to protect the Halcyon Marine Healthcare Systems from security risks, including:

- Breaches of confidentiality. For instance, the information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

**2. Scope**

This policy applies to all Remote Users of Halcyon Marine Healthcare Systems including its employee, outside contractors, vendors, and other agents.

**3. Policy**

**3.1 Data Protection Law**

The **REPUBLIC ACT NO. 10173** also known as **Data Privacy Act of 2012** describes how organizations. including Halcyon Marine Healthcare Systems must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

**3.2 General Staff Guidelines**

- The only people able to access data covered by this policy should those who need it for their work.

- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Halcyon Marine Healthcare Systems will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorized people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the MIS if they are unsure about any aspect of data protection.

**3.3 Data Storage**

These rules describe how and where data should be safely stored.
Questions about storing data safely can be directed to the MIS Head.
When data is stored on paper, it should be kept in a secure place where Unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically, but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.

- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

**3.4 Data Use**

Personal data is no value to Halcyon Marine Healthcare Systems unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure that the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically. The MIS manager can explain how to send data to authorized external contacts.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

### 3.5 Data Accuracy

The law requires Halcyon Marine Healthcare Systems to take reasonable steps to ensure data is kept accurate and up to date.

The more important is that the personal data is accurate, the greater the effort of Halcyon Marine Healthcare Systems should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

- Halcyon Marine Healthcare Systems will make it easy for data subjects to update the information Halcyon Marine Healthcare Systems holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

**3.6 Providing Information**

Halcyon Marine Healthcare Systems aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data are being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals are used by the company.

## II. Network Security Policy

### A. Bluetooth Baseline Requirement Policy

Bluetooth enabled devices are exploding on the Internet at an astonishing rate. At the range of connectivity has increased substantially. Insecure Bluetooth connections can introduce a number of potential serious security issues. Hence, there is a need for a minimum standard for connecting Bluetooth enable devices

## 1. Purpose

The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the Halcyon Marine Healthcare Systems' network or owned devices. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential data of Halcyon Marine Healthcare Systems.

## 2. Scope

This policy applies to any Bluetooth enabled devices that are connected to Halcyon Marine Healthcare Systems' network or owned devices.

## 3. Policy

### 3.1 Version

No Bluetooth Device shall be deployed on Halcyon Marine Healthcare Systems' equipment that does not meet a minimum of Bluetooth v2.1 specifications without written authorization from the MIS Team. Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

### 3.2 Pins and Pairing

When pairing your Bluetooth unit to Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area wherein your PIN can be compromised.

If your Bluetooth enabled equipment asks to enter your pin after the initial paring, you must refuse the pairing request and report it Immediately to the MIS Team through Help Desk.

**3.3 Device Security Settings**

- All Bluetooth devices shall employ "security mode 3" which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
- Use a minimum PIN length of 8. A longer PIN may provide more security.
- Switch the Bluetooth device to hidden mode (non-discoverable)
- Only activate Bluetooth when it is needed.
- Ensure that device firmware is up-to-date.

**3.4 Security Audits**

The MIS Team may perform random audits to ensure compliance with this policy. In the process of performing such audits, MIS Team members shall not eavesdrop on any phone conversation.

**3.5 Unauthorized Use**

The following is the list of unauthorized use of the Halcyon Marine Healthcare Systems' owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
- Using the Halcyon Marine Healthcare Systems' owned Bluetooth equipment on non-owned Bluetooth enabled devices.
- Unauthorized modification of Bluetooth devices for any purpose.

### 3.6 User Responsibilities

- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth mode must be turned off when not in use.
- PII and/or Halcyon Marine Healthcare Systems' Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.
- Bluetooth users must only access the Halcyon Marine Healthcare Systems' information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.

- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems to the MIS team immediately.

**B. Remote Access Policy**

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions and LLC policy, we must mitigate these external risks to the best of our ability.

**1. Purpose**

The purpose of this policy is to define rules and requirements connecting to Halcyon Marine Healthcare Systems' network from any host. These rules and requirements are designed to minimize the potential exposure of Halcyon Marine Healthcare Systems from damages which may result in unauthorized use of Halcyon Marine Healthcare Systems' resources. Damages including the loss of sensitive or company confidential data, intellectual property, damage to public

image, damage to critical Halcyon Marine Healthcare Systems' internal systems, and fines or other financial liabilities incurred as a result of those losses.

**2. Scope**

This policy applies to all Halcyon Marine Healthcare Systems' employees, contractors, vendors and agents with a company's owned, personally-owned computer or workstation used to connect to the Halcyon Marine Healthcare Systems' network. This policy applies to remote access connections used to do work on behalf of Halcyon Marine Healthcare Systems, including reading or sending email and viewing of intranet web resources. This policy covers all technical implementations of remote access used to connect to Halcyon Marine Healthcare Systems' networks.

**3. Policy**

It is the responsibility of Halcyon Marine Healthcare Systems' employees, contractors, vendors and agents with remote access privileges to Halcyon Marine Healthcare Systems' corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Halcyon Marine Healthcare Systems.

General access to the Internet for recreational use through the Halcyon Marine Healthcare Systems' network is strictly limited to its employees, contractors, vendors and agents (hereafter referred as "Authorized Users"). When accessing the Halcyon Marine Healthcare Systems' network from a personal computer, Authorized Users are responsible for preventing access to any Halcyon Marine Healthcare Systems' computer resources or data by unauthorized Users. Performance of illegal activities through the Halcyon Marine Healthcare Systems' network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use Halcyon Marine Healthcare Systems' networks to access the Internet for outside business interests.

**3.1 Requirements**

3.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information, see the *Acceptable Encryption Policy* and the *Password Policy*.

3.1.2 Authorized Users shall protect their password from their family members.

3.1.3 While using a Halcyon Marine Healthcare Systems' owned computer to remotely connect to Halcyon Marine Healthcare Systems' corporate network, Authorized Users shall ensure that the remote host is not connected to any network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

3.1.4 Use of external resources to conduct Halcyon Marine Healthcare Systems' business must be approved in advance by MIS Team and the appropriate business unit Manager.

3.1.5 All hosts that connect to Halcyon Marine Healthcare Systems' internal networks via remote access technologies must use the up-to-date anti-virus software which includes personal computers. Third party connections must comply with the requirements as stated in the *Third Party Agreement*.

3.1.6 Personal equipment used to connect to Halcyon Marine Healthcare Systems' networks must meet the requirements of Systems-owned equipment for remote access as stated in the *Remote Access Standards*.

**4. Related Standards, Policies and Processes**

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Halcyon Marine Healthcare Systems' network:

- *Acceptable Encryption Policy*
- *Acceptable Use Policy*
- *Password Policy*
- *Third Party Agreement*
- *Remote Access Standards*

## C. Remote Access Standards

**1. Purpose**

The purpose of this policy is to ensure that all Remote Users must follow the security requirements set forth in this standard for any Remote Host accessing IT Resources prior to such access, as well as any guidelines, procedures, or other requirements issued by their departmental IT units and/or the owners of the IT Resource which are to be remotely accessed.

**2. Scope**

This standard applies to all Remote Users of Halcyon Marine Healthcare Systems including its employee, outside contractors, vendors, and other agents.

3. **Policy**

**Remote User Requirements:**

- Remote Users must ensure that they Remote Hosts used to access Halcyon Marine Healthcare Systems should meet all security expectations specified in the IT Security Policy prior to accessing any Halcyon Marine Healthcare Systems' resource.
- It is the responsibility of Remote Users to take reasonable precautions to ensure their remote access connections are secured from interception, eavesdropping, or misuse.

All Remote Users are responsible for following applicable Halcyon Marine Healthcare Systems' policy, including the Halcyon Marine Healthcare Systems' Data Handling Requirements, when handling any Halcyon Marine Healthcare Systems data remotely accessed within the course of the Remote User's job function at Halcyon Marine Healthcare Systems. Policies to follow and actions to perform include, but are not limited to:

- All Remote Users are expected to only remotely access data in accordance with Halcyon Marine Healthcare Systems IT security policies.

- Do not save or store Halcyon Marine Healthcare Systems sensitive or restricted data on the Remote Host used to access Halcyon Marine Healthcare Systems IT Resources.

**D. Remote Access Tools Policy**

Remote desktop software is also known as remote access tools, provides way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software includes LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the Halcyon Marine Healthcare Systems' network that can be used for theft, unauthorized access , or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used in Halcyon Marine Healthcare Systems' computer systems.

**1. Purpose**

This policy defines the requirements for remote access tools used in Halcyon Marine Healthcare Systems.

**2. Scope**

This policy applies to all remote access where either end of the communication terminates in Halcyon Marine Healthcare Systems' computer asset.

**3. Policy**

All remote access tools used to communicate between Halcyon Marine Healthcare Systems' assets and other systems must comply with the following policy requirements.

**3.1 Remote Access Tools**

Halcyon Marine Healthcare Systems provide mechanisms to collaborate between internal users, with external partners, and from non Halcyon Marine Healthcare Systems' computer systems. Because proper configuration is important to secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

a) All remote access tools or systems that allow communication to Halcyon Marine Healthcare Systems' resources from the Internet or external partner systems must

require multi-factor authentication. E.g. authentication tokens and smart cards that require an additional PIN or password.

b) The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.

c) Remote access tools must support the Halcyon Marine Healthcare Systems' application layer proxy rather than direct connections through the perimeter firewall.

d) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the Halcyon Marine Healthcare Systems' network encryption protocols policy.

e) All Halcyon Marine Healthcare Systems' antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard Halcyon Marine Healthcare Systems' procurement process, and must approved by the MIS department.

E. **Router and Switch Security Policy**

**1. Purpose**

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity in or on behalf of Halcyon Marine Healthcare Systems.

**2. Scope**

All employees, contractors, consultants, temporary and other workers of Halcyon Marine Healthcare Systems and its subsidiaries must adhere to this policy. All routers and switches connected to Halcyon Marine Healthcare Systems production networks are affected.

**3. Policy**

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.

2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
    a) IP directed broadcasts
    b) Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c) TCP small services
    d) UDP small services
    e) All source routing and switching
    f) All web services running on router
    g) Cisco discovery protocol on Internet connected interfaces
    h) Telnet, FTP, and HTTP services
    i) Auto-configuration

4. The following services should be disabled unless a business justification is provided:
    a) Cisco discovery protocol and other discovery protocols
    b) Dynamic Trunking
    c) Scripting environments, such as the TCL shell
5. The following services must be configured:
    a) Password-encryption

b) NTP configured to a corporate standard source

6. All routing updates shall be done using secure routing updates.
7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
9. Access control lists for transiting the device are to be added as business needs arise.
10. The router must be included in the corporate enterprise management system with a designated point of contact.
11. Each router must have the following statement presented in all forms of login whether remote or local:
    *"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."*

12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    a) IP access list accounting
    b) Device logging
    c) Incoming packets at the router sourced with invalid addresses such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    d) Router consoles and modem access must be restricted by additional security controls

**F. Wireless Communication Policy**

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

**SUBJECT: HMHS IT SECURITY POLICY AND STANDARDS**

## 1. Purpose

The purpose of this policy is to secure and protect the information assets owned by Halcyon Marine Healthcare Systems. Halcyon Marine Healthcare Systems provides a computer devices, networks, and other electronic information systems to meet the mission, goal and initiative. Halcyon Marine Healthcare Systems grant access to these resources as a must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to Halcyon Marine Healthcare Systems network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Management Information Systems Department are approved for connectivity to a Halcyon Marine Healthcare Systems network.

## 2. Scope

All employees, contractors, consultants, temporary and other workers at Halcyon Marine Healthcare Systems, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Halcyon Marine Healthcare Systems must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a Halcyon Marine Healthcare Systems' network or reside on a Halcyon Marine Healthcare Systems' site that provide wireless connectivity to endpoint

devices, including, but not limited to laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

**3. Policy**

**3.1 General Requirements**

All wireless infrastructure devices that reside on Halcyon Marine Healthcare Systems' site, network, or provide access to information classified as Halcyon Marine Healthcare Systems Confidential, or above must:

- Abide by the standards specified in *Wireless Communication Standard*.
- Be installed, supported, and maintained by MIS team.
- Use *Halcyon Marine Healthcare Systems'* approved authentication protocols and infrastructure.
- Use *Halcyon Marine Healthcare Systems'* approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

**3.2 Isolated Wireless Device Requirements**

All wireless infrastructure devices that provide access to Halcyon Marine Healthcare Systems' Confidential or above, must adhere to section 3.1 above. Isolated wireless devices that do not provide general network connectivity to the Halcyon Marine Healthcare Systems' network must:

- Be isolated from the corporate network (it must not provide any corporate connectivity).
- Not interfere with wireless access deployments maintained by other support organizations.

**3.3 Home Wireless Device Requirements**

3.3.1 Wireless infrastructure devices that provide direct access to the Halcyon Marine Healthcare Systems' corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.

3.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the Halcyon Marine Healthcare Systems' corporate network. Access to the

Halcyon Marine Healthcare Systems' corporate network through this device must use standard remote access authentication.

**4. Related Standards, Policies and Processes**

- Wireless Communication Standard

**5. Definition of Terms**

- **MAC Address** - A media access control address (MAC address), also called as physical address, is a unique identifier assigned to network interfaces for communications on the physical network segment.

G. **Wireless Communication Standard**

**1. Purpose**

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to Halcyon Marine Healthcare Systems' network. Only those wireless infrastructure devices that meet the requirements specified in this standard are granted an exception by the MIS Team are approved for connectivity to Halcyon Marine Healthcare Systems' network.

Network devices, including but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by the Management Information Systems.

**2. Scope**

All employees, contractors, consultants, temporary and other workers of Halcyon Marine Healthcare Systems and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of Halcyon Marine Healthcare Systems, must comply with this standard. This standard applies to wireless devices that make a connection to network and all wireless infrastructure devices.

MIS Team must approve exceptions to this standard in advance.

**3. Policy**

**3.1 General Requirements**

All wireless infrastructure devices that connect to Halcyon Marine Healthcare Systems' network or provides access to Halcyon Marine Healthcare Systems' confidential and restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

**3.2 Isolated Wireless Device Requirements**

- Device Service Set Identifier (SSID) must be different from the *Halcyon Marine Healthcare Systems'* production device SSID.

- Broadcasting of device SSID must be disabled.

**3.3 Home Wireless Device Requirements**

All home wireless infrastructure devices that provide direct access to a Halcyon Marine Healthcare Systems network, such as those

behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

**4. Definitions of terms**

- **AES** - Advanced Encryption Standard or AES is a symmetric block cipher used to protect classified information and is implemented in software and hardware to encrypt sensitive data.

- **EAP-FAST** - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a publicly accessible IEEE 802.1X EAP type that provides protection from a variety of network attacks, including man-in-the-middle, authentication forging, weak IV attack (AirSnort), packet forgery (replay attack), and dictionary attacks.

- **EAP-TLS** - The Protected Extensible Authentication Protocol, is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel.

- **PEAP** - PEAP (Protected Extensible Authentication Protocol) is a version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. PEAP is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control.
- **SSID** - A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). An SSID is sometimes referred to as a "network name."

- **TKIP** - TKIP (Temporal Key Integrity Protocol) is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to

provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP), the original WLAN security protocol.

- **WPA-PSK** - Short for Wi-Fi Protected Access 2 - Pre-Shared Key, and also called WPA or WPA2 Personal, it is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server.

### H. Analog/ISDN Line Security Policy

#### 1. Purpose

This document explains the Halcyon Marine Healthcare Systems' analog/ISDN line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/ISDN lines: lines that are to be connected for the sole purpose of fax sending and receiving, and lines that are to be connected to computers.

#### 2. Scope

This policy covers only those lines that are to be connected to a point inside the Halcyon Marine Healthcare Systems' building and testing sites. It does not pertain to ISDN/phone lines that are connected into employee's homes, PBX desktop phones, and those lines used by Telecom for emergency and non-corporate information purposes.

## 3. Policy

### 3.1 Scenarios & Business Impact

There are two important scenarios that involve analog line misuse, which we attempt to guard against this policy. First scenario is an outside attacker who calls a set of analog line numbers in hoping of connecting to a computer that has a modem attached. If the modem answers (most computers today are configured out-of-the-box to auto-answer) from inside of Halcyon Marine Healthcare Systems' premises, then there is a possibility that the Halcyon Marine Healthcare Systems' internal network will be breached using that computer. Information held on that computer can be compromised. This potentially results in the loss of millions of dollars worth of corporate information.

The second scenario is the threat of anyone with physical access to Halcyon Marine Healthcare Systems' facility, being able to use a modem-equipped laptop or desktop computer. In this case, the intruder would be able to connect to the trusted network of Halcyon Marine Healthcare Systems through the computer's Ethernet connection, and then calls out to an unmonitored site using the modem, with the ability to siphon Halcyon Marine Healthcare Systems' information to an unknown location. This

could also potentially result in the substantial loss of vital information.

Specific procedures for addressing the security risks inherent in each of these scenarios follow.

### 3.2 Facsimile Machines

As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.
- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a centralized administrative area designated for departmental use, and away from other computer equipment.
- A computer which is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

Waivers for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and the security posture of the request.

Use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- When in use, the computer is to be physically disconnected from Halcyon Marine Healthcare Systems' internal network.
- The line will be used solely for Halcyon Marine Healthcare Systems' business, and not for personal reasons.
- All downloaded material, prior to being introduced into Halcyon Marine Healthcare Systems' system and networks, must have been scanned by an approved anti-virus utility (e.g., Sophos Antivirus) which has been kept current through regular updates.

**3.3 Computer-to-Analog Line Connections**

The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within Halcyon Marine Healthcare Systems will not be approved for

security reasons. Analog and ISDN lines represent a significant security threat to Halcyon Marine Healthcare Systems, and active penetrations have been launched against such lines by hackers. Waivers to the policy above will be granted on a case by case basis.

Replacement lines, such as those requested because of a move, fall under the category of "new" lines. They will also be considered on a case to case basis.

**3.4 Requesting an Analog/ISDN Line**

Once approved by Manager, the individual requesting of analog/ISDN line must provide the following information to Telecom:

- A clearly detailed business case of why other secure connections available on Halcyon Marine Healthcare Systems cannot be used,
- The business purpose for which the analog line is to be used,
- The software and hardware to be connected to line and used across the line,
- What external connections that the requester is seeking to access.

The business case must answer, at a minimum, the following questions:

- What business needs to be conducted over the line?
- Why is that Halcyon Marine Healthcare Systems' equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?
- Why is that Halcyon Marine Healthcare Systems' current dial-out access, pool unable to accomplish the same tasks as an analog line?

In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:

- Will the machines that are using the analog lines be physically disconnected from Halcyon Marine Healthcare Systems' internal network?
- Where will the analog line to be placed? A cubicle or lab?
- Is dial-in from outside of Halcyon Marine Healthcare Systems is needed?
- How many lines are being requested and how many people will use the line?

- How often will the line be used? Once a week or 2 hours a day?
- What is the earliest date that the line can be terminated from service?
- The line must be terminated when not in use.
- What other means will be used to secure the line from unauthorized use?
- Is this a replacement line from an old location? What was the purpose of the original line?
- What type of protocols will be run over the line?
- Will a Halcyon Marine Healthcare Systems -authorized anti-virus scanner be installed on the machine(s) using the analog lines?

I. **Extranet Policy**

**1. Purpose**

This document describes the policy under third party organizations connected to Halcyon Marine Healthcare Systems' networks for the purpose of transacting business related to Halcyon Marine Healthcare Systems.

**2. Scope**

Connections between third parties that require access to non-public Halcyon Marine Healthcare Systems resources fall under this policy, regardless of whether a Telco circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access to Halcyon Marine Healthcare Systems or to the Public Switched Telephone Network do NOT fall under this policy.

## 3. Policy

### 3.1 Pre-Requisites

#### 3.1.1 Security Review

All new extranet connectivity will go through a security review with the MIS and Security Consultant. The reviews are to ensure that all access matches the business requirements in a best possible way, and that the principle of least access is followed.

#### 3.1.2 Third Party Connection Agreement

All new connection requests between third parties and Halcyon Marine Healthcare Systems require that the third party its representatives agree to sign the *Third Party Agreement*. This agreement must be signed by the President of the Sponsoring Organization as well as the

representative from third party who is legally empowered to sign on behalf of the third party. The signed document is to be kept on file with the relevant extranet group. Documents pertaining to connections into Halcyon Marine Healthcare Systems are to be kept on file with the MIS team.

### 3.1.3 Business Case

All production of extranet connections must be accompanied by a valid business justification, in writing, that is approved by a project manager in the extranet group. Lab connections must be approved by the MIS head. Typically this function is handled as part of the *Third Party Agreement*.

### 3.1.4 Point Of Contact

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the *Third Party Agreement* that pertain to it. In the event that the point of contact changes, the relevant extranet Organization must be informed promptly.

**3.2 Establishing Connectivity**

Sponsoring Organizations within Halcyon Marine Healthcare Systems that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage MIS to address security issues inherent in the project. If the proposed connection is to terminate within Halcyon Marine Healthcare Systems, the Sponsoring Organization must engage the [name of the team responsible for security of labs]. The Sponsoring Organization must provide full and complete information as to the nature of the proposed access to the extranet group and MIS team as requested.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will Halcyon Marine Healthcare Systems rely upon the third party to protect its network or resources.

**3.3 Modifying or Changing Connectivity and Access**

All changes in access must be accompanied by a valid business justification, and are subject to security review.

Changes are to be implemented via corporate change management process. The Sponsoring Organization is responsible for notifying the extranet management group and/or MIS team when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

### 3.4 Terminating Access

When access is no longer required, the Sponsoring Organization within Halcyon Marine Healthcare Systems must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and security teams must conduct an audit on their respective connections annually to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections found to be depreciated is no longer used to conduct Halcyon Marine Healthcare Systems' business and will be terminated immediately. Security incident or findings that a circuit has been deprecated is no longer used to conduct on Halcyon Marine Healthcare Systems' business

necessitate a modification of existing permits, or termination of connectivity, the MIS or extranet team will notify the POC or the Sponsoring Organization of the change prior to taking any.

J. **Virtual Private Network (VPN) Policy**

**1. Purpose**

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to Halcyon Marine Healthcare Systems' corporate network.

**2. Scope**

This policy applies to Halcyon Marine Healthcare Systems' employees, contractors, consultants, temporaries, and other workers, including all personnel affiliated with third parties utilizing VPNs to access the Halcyon Marine Healthcare Systems' network. This policy applies to implementation of VPN that are directed through IPSec Concentrator.

**3. Policy**

Approved Halcyon Marine Healthcare Systems' employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating

installation, installing any required software, and paying associated fees. Further details may be found on *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed to access to Halcyon Marine Healthcare Systems' internal networks.

2. Use of the VPN is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.

3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.

4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

5. VPN gateways will be set up and managed by Halcyon Marine Healthcare Systems' MIS team.

6. All computers connected to Halcyon Marine Healthcare Systems' internal networks via VPN or any other technology must use the

most up-to-date anti-virus software, this includes personal computers.

7. VPN users will be automatically disconnected from Halcyon Marine Healthcare Systems' network after thirty minutes of inactivity. The user must then login to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.

9. Users of computers that are not Halcyon Marine Healthcare Systems' owned equipment must configure the equipment to comply with Halcyon Marine Healthcare Systems' VPN and Network policies.

10. Only MIS team will approve VPN clients may be used.

11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Halcyon Marine Healthcare Systems' network, and as such are subject to the same rules and regulations that apply to Halcyon

Marine Healthcare Systems' owned equipment, i.e., their machines must be configured to comply with MIS Security Policies.

## III. Server Security Policy

### A. Database Credentials Coding Policy

Database authentication credentials are necessary for authorizing application to connect to internal databases. However, incorrect use of storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

#### 1. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Halcyon Marine Healthcare Systems' networks.

Software applications running on Halcyon Marine Healthcare Systems' networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

**2. Scope**

This policy is directed at all system implementer and/or software engineers who may be coded applications that will access a production database server on the Halcyon Marine Healthcare Systems' Network. This policy applies to all software programs, modules, libraries or APIS that will access the Halcyon Marine Healthcare Systems' multi-user production database. It is recommended that similar requirements are in place for non-production servers and lab environments since it don't always use sanitized information.

**3. Policy**

**General**

In order to maintain the security of Halcyon Marine Healthcare Systems' internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this

authentication must not reside in the main, executing body of the pored in a location that can be accessed through a web server.

**Specific Requirements**

Storage of Data Base user names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writable.

- Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process on the authentication server. In this case, there is no need for programmatic use of database credentials.
- Database credentials may not reside in the document tree of a web server.

- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

**Retrieval of Database User Names and Passwords**

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory that contains the user name and password must be released or cleared.
- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code, but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.
- For languages that execute from source code, the credentials' source file must not reside in the same browse able or executable file directory tree in which the executing body of code resides.

**Access to Database User Names and Passwords**

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

**4. Policy Compliance**

The violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Halcyon Marine Healthcare Systems.

Any program code or application that is found to violate this policy must be re-mediate within 90 day period.

**5. Related Standards, Policies and Processes**

- Password Policy

6. **Definitions of terms**
   - **Credentials** - A user's authentication information—typically a password, token, or certificate.
   - **Hash Function** - A hash function usually means a function that compresses, meaning the output is shorter than the input. Often, such a function takes an input of arbitrary or almost arbitrary length to one whose length is a fixed number, like 160 bits.
   - **LDAP** - LDAP (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

**B. Information Logging Standard**

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although the logging information may not be viewed on a daily basis, it is critical to have from a forensic standpoint.

**1. Purpose**

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to

generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

## 2. Scope

This policy applies to all production systems on Halcyon Marine Healthcare Systems Network.

## 3. Policy

### 3.1 General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?

2. Who performed the activity, including where or what system does the activity was performed?
3. What activity was performed on (object)?
4. When the activity performed?
5. What tool(s) does the activity was performed with?
6. What was the status (such as success vs. failure), outcome, or result of the activity?

### 3.2 Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
2. Create, update, or delete information not covered in #1;
3. Initiate the network connection;
4. Accept the network connection;
5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;

7. System, network, or service configuration changes, including installation of software patches and updates, or other installed software changes;
8. Application process startup, shutdown, or restart;
9. Application process abort, fail, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
10. Detection of suspicious/malicious activity such as Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

**3.3 Elements of the Log**

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirect" means unambiguously inferred.

1. Type of action – e.g. authorized, create, read, update, delete, and accept network connections.
2. Subsystem performs the action – e.g. process or transaction name, process or transaction identifier.
3. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine the record accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
5. Before and after values when the action involves updating a data element, if feasible.
6. The date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
7. Whether the action was allowed or denied by access-control mechanisms.

8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

**3.4 Formatting and Storage**

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include, but are not limited to the following:

1. Microsoft Windows Event Logs collected by a centralized log management system;
2. Logs in a well-documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system;
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
4. Other open logging mechanisms supporting the above requirements, including those based on CheckPointOpSec, ArcSight CEF, and IDMEF.

**C. Server Security Policy**

**SUBJECT: HMHS IT SECURITY POLICY AND STANDARDS**

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

1. **Purpose**

   The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Halcyon Marine Healthcare Systems. Effective implementation of this policy will minimize unauthorized access to Halcyon Marine Healthcare Systems proprietary information and technology.

2. **Scope**

   All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Cisco or registered under a Cisco-owned internal network domain.
   This policy specifies requirements for equipment on the internal network. For secure configuration of equipment external to network to the DMZ, see the Internet *DMZ Equipment Policy*.

## 3. Policy

### 3.1 General Requirements

3.1.1 All internal servers deployed on Halcyon Marine Healthcare Systems must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by MIS Team. Operating groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by MIS Team. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version

- Main functions and applications, if applicable

- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes to production servers must follow the appropriate change management procedures

3.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor the audit equipment, systems, processes, and network traffic as per Server *Audit Policy*.

**3.2 Configuration Requirements**

3.2.1 Operating System configuration should be in accordance with approved MIS guidelines.

3.2.2 Services and applications that will not be used must be disabled where practical.

3.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

3.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being

when the immediate application would interfere with business requirements.

3.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

3.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

3.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

3.2.8 Servers should be physically located in an access-controlled environment.

3.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

**3.3 Monitoring**

3.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.

- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

3.3.2 Security-related events will be reported to MIS Team, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts

Anomalous occurrences that are not related to specific applications on the host.

**4. Related Standards, Policies and Processes**

- Server Audit Policy
- Internet DMZ Equipment Policy

5. **Definitions of terms**

- **DMZ** - demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical sub-network that contains and exposes an organization's external-facing services to a larger and distrusted network, usually the Internet.

**D. Software Installation Policy**

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during an audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

1. **Purpose**

The purpose of this policy is to outline the requirements around installation software on Halcyon Marine Healthcare Systems' owned computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Halcyon Marine Healthcare Systems' computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

2. **Scope**

This policy applies to all Halcyon Marine Healthcare Systems' employees, contractors, vendors and agents with a Halcyon Marine Healthcare Systems' owned mobile devices. This policy covers all computers, servers, smart phones, tablets and other computing devices operating within Halcyon Marine Healthcare Systems.

**3. Policy**

- Employees may not install software on Halcyon Marine Healthcare Systems' computing devices operated within the Halcyon Marine Healthcare Systems' network.
- Software requests must first be approved by the requester's Manager and then be made to the Information Technology department or Helpdesk in writing or via email.
- Software must be selected from an approved software list, maintained by the MIS department, unless no selection on the list meets the requester's need.
- The MIS Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

**E. Technology Equipment Disposal Policy**

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of Halcyon Marine Healthcare Systems' data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data are marked for deletion, but are still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

1. **Purpose**

   The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Halcyon Marine Healthcare Systems.

2. **Scope**

   This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Halcyon Marine Healthcare Systems including, but not limited to, the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners,

typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All Halcyon Marine Healthcare Systems' employees and affiliates must comply with this policy.

## 3. Policy

### 3.1 Technology Equipment Disposal

3.1.1 When Technology assets have reached the end of their useful life they should be sent to the MIS Department for proper disposal.

3.1.2 The MIS Team will securely erase all storage mediums in accordance with current industry best practices.

3.1.3 All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of

the machine with zero-filled blocks, meeting Department of Defense standards.

3.1.4 No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).

3.1.5 No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around Halcyon Marine Healthcare Systems. These can be used to dispose of equipment. The MIS Team will properly remove all data prior to final disposal.

3.1.6 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

3.1.7 Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or

any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

3.1.8 Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

**3.2 Employee Purchase of Disposed Equipment**

3.2.1 Equipment which is working, but reached the end of its useful life to Halcyon Marine Healthcare Systems, will be made available for purchase by employees.

3.2.2 A bidding system will be used to determine who has the opportunity to purchase available equipment.

3.2.3 All equipment purchases must go through the bidding process. Employees cannot purchase their office computer directly, or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.

3.2.4 Finance and Information Technology will determine an appropriate cost for each item.

3.2.5 All purchases are final. No warranty will be provided with any equipment sold.

3.2.6 Any equipment not in working order or remaining from the bidding process will be donated or disposed of according to current environmental guidelines.

3.2.7 Halcyon Marine Healthcare Systems has contracted with several organizations to donate or properly dispose of outdated technology assets.

Prior to leaving Halcyon Marine Healthcare Systems' premises, all equipment must be tagged from the Centralized Inventory Database System as "Disposed".

**F. Workstation Security Policy**

**1. Purpose**

The purpose of this policy is to provide guidance for workstation security for Halcyon Marine Healthcare Systems' workstations in order to ensure the security of information on the workstation and information the

workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

**2. Scope**

This policy applies to all Halcyon Marine Healthcare Systems' employees, contractors, workforce members, vendors and agents with a Halcyon Marine Healthcare Systems' owned or personal-workstation connected to the Halcyon Marine Healthcare Systems' network.

**3. Policy**

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

3.2 Halcyon Marine Healthcare Systems will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

3.3 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with Halcyon Marine Healthcare Systems' *Password Policy*.
- Complying with all applicable password policies and procedures. See Halcyon Marine Healthcare Systems' *Password Policy*.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Baseline *Workstation Configuration Security Standard*

- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hour updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).

If a wireless network access is used, ensure access is secure by following the *Wireless Communication policy*

**4. Related Standards, Policies and Processes**

- Password Policy
- Wireless Communication Policy
- Workstation Configuration Security Standard

**G. Workstation Configuration Security Standard**

Improper configured computer systems can be compromised and have their data destroyed or stolen; used to store illegal data; relay spam e-mail; or attack other systems. Departments are responsible for maintaining secure workstations.

**1. Scope**

This policy applies to all Halcyon Marine Healthcare Systems' employees and affiliates.

## 2. Policy

### 2.1 WORKSTATION HARDENING:

All workstations must, to the extent possible for the operating system (OS), application, and function, be configured in a way that reduces the risk to the system through the elimination of unneeded services and their vulnerabilities. Actual hardening techniques vary according to the OS, but some issues involved in hardening include:

- Physically securing the workstation and console operations
- Patching and/or upgrading vulnerable applications and services
- Eliminating unnecessary services
- Eliminating programs or services which cause unnecessary security risks or are not used
- Managing file permissions
- Establishing restrictions on user accounts and access

### 2.2 ACCESS CONTROL:

A local user account passwords must conform to the established password standard, which includes password complexity and account lockout configurations. The workstations must be configured in a manner to require interactive user authentication instead of an automatic login where the password is stored on the workstation. If possible, avoid storing passwords or shadow files on the workstation. If passwords are stored locally, then they should be encrypted. Workstations must have password-protected screen savers, which automatically lock the workstation after a period of inactivity. An automatic screen saver workstation lock should be set to 15 minutes or less, except under unusual circumstances.

**2.3 SHARED RESOURCES:**

Except for public Information Technology (IT) resources, all shared resources (e.g., mapped folders, drives, and devices) must have permissions set to allow only those individual accounts or groups that require access to that resource. These permissions must be reviewed on a regular basis (minimum of every 6 months) to ensure appropriate access levels are being maintained. Shared resources from a workstation are discouraged when a server is available.

**2.4 PATCH MANAGEMENT:**

If a centralized patch management system is available for the operating system, then it must be used. Desktop workstations, excluding mobile devices (notebooks, laptops, tablets, PDAs, etc.) must remain powered on at all times for after-hours patch management. Users of mobile devices must make their system available in order for security patches to be applied in a timely manner. If centralized patch management is not available, regularly scheduled manual or automated vendor updates must be implemented. The MIS department is responsible for ensuring necessary patches are applied as soon as possible, as well as accelerated patch deployment if the MIS Head elevates the threat level.

**2.5 OS AND APPLICATION MAINTENANCE:**

Operating systems and applications must be maintained by the MIS department at the most recent stable and institutionally-supported version that is compatible with the system's hardware and function, and critical security patches must be applied. Systems with operating systems or applications that cannot be upgraded due to hardware or functional restrictions must be removed from network access or replaced with newer systems. In cases where an older OS or application is required due to

hardware or functional restrictions, measures must be taken to limit access to the system (via host-based firewall, router access control, internal limitation of available services, or other measures) in order to reduce the exploitation risk of older vulnerabilities that cannot be mitigated. An exception may be requested by submitting a letter to the MIS Head for approval.

**2.6 SYSTEM LOGGING:**

Operating system event logging must be enabled for security events such as failed and successful logins, and unauthorized connections for any commonly used service. Applications on workstations which manage confidential high-risk information must implement event logging to record unauthorized access attempts and, if possible, to track configuration changes. The log should be configured to retain those events for at least 30 days.

**2.7 SYSTEM MONITORING:**

All departments who manage are required to implement procedures to regularly review logs to ensure access is authorized and information integrity is protected.

**2.8 WORKSTATIONS WITH MULTIPLE USERS:**

All user accounts must be uniquely identified and must require authentication. Account creation and authorization processes must be based on the principle of least privilege, with access to systems granted only to those who require it on a need-to-know basis. A user's access authorization shall be appropriately modified or removed when the user's employment or job responsibility within the company changes. Procedures must be in place for emergency termination of all domains, local, or other application user accounts. User accounts must be individually assigned and maintained except in cases where an application, hardware, or function requires that a single common account be used. Unused local accounts must be managed in a timely manner to prevent misuse of old accounts by intruders or users who no longer have the authority to access the system. If a user needs administrative access, they must be placed in an administrative group instead of logging in as administrator.

**2.9 DEFAULT ACCOUNT MANAGEMENT:**

Many operating systems and applications have default accounts and passwords built in or left over from the development or installation process. These accounts and passwords are a significant risk if left open and available for use; whenever

possible, default accounts must be disabled, renamed, or password will be changed.

**2.10 PHYSICAL SECURITY:**

Systems that contain sensitive information must be physically attached via a secure locking device to some relatively immobile object or housed in an area that uses access control systems (e.g., card-key, cryptolock), or otherwise provides strictly controlled access (e.g., system administrator and security guard only). Password-protected screen savers must be used for logged-in but unattended workstations.

**2.11 VIRUS AND MALWARE SCANNING:**

All workstations, whether connected to the systems network or standalone, must use the approved anti virus product. If a centrally managed client for the operating system is available, then it must be used. In such cases where installing anti virus would compromise or threaten the workstation's functionality, then it must be documented and other compensating controls must be put in place. Where possible in this scenario, at a minimum, a virus configuration should include:

- Scheduled daily or weekly signature updates
- Scheduled weekly scans of all files and file types

- Real-time protection enabled
- The anti virus application must be initiated on system start up
- If a virus is found, clean the threat first and quarantine the threat's second
- Protected from unauthorized configuration change

**2.12 INTRUSION DETECTION AND PREVENTION:**

All Halcyon Marine Healthcare Systems' owned workstations must use the Information Security approved firewall software and configuration. If a Halcyon Marine Healthcare Systems, centrally-managed firewall client for the operating system is available, then it must be used. Other host-based firewall products or any actions preventing the Information Security Function are prohibited.

**2.13 BACKUP:**

If a workstation stores file locally that contain primary critical information or contain primary sensitive information, those files should be transferred to a server. The level of backup required depends on the criticality of the data stored on the workstation. If possible, store file on a server. If the workstation is standalone and stores data, then local backup is required. The backup process

must be tested periodically for successful restorations.

Wherever possible, all workstations should have an established, documented, and consistently-used backup plan. The frequency of the backup schedule will depend on the data classification of the data stored on the workstation (Data Backup Policy).

**2.14 SEPARATION OF FUNCTION:**

The workstations must be designed in a way that allows functions, applications, and data to be grouped or separated according to data classification and function. In general, public-use workstations must not be used to access or store sensitive information. Also, servers, rather than workstations, must be used to house multiple user applications, databases, and/or shared resources.

**2.15 MISCELLANEOUS:**

- Where possible, joint computers to the Halcyon Marine Healthcare Systems' domain
- Common access of computers must require an individual authentication

- Workstations must use the Halcyon Marine Healthcare Systems' DNS settings
- If a wireless access is used on a mobile device, then the device must connect to MIS-approved wireless access point. Configuring portable devices in ad hoc mode or connecting to other non- Halcyon Marine Healthcare Systems' wireless access points is prohibited.
- Use of Halcyon Marine Healthcare Systems' domain user accounts is preferred instead of local system and non-domain accounts
- The use of insecure protocols (FTP and Telnet) to transmit confidential information is prohibited. The use of secure protocols (SSH and SSL) are the preferred method of data transfer, both inside and outside the Halcyon Marine Healthcare Systems. The exception for this policy are MIS system administrators.
- When possible, develop a consistent naming convention for the workstations in your department
- When possible, use a Halcyon Marine Healthcare Systems' standard desktop image
- When possible, use group policies, templates, or login scripts to maintain the security on Windows workstations and to simplify the administration

- When possible, save the confidential information on mobile devices in an encrypted format with an encryption scheme coordinated within the MIS and other department
- The use of host files (local files that override DNS settings) is prohibited except for development.
- Use of instant messaging other than Skype is discouraged
- Systems that use non-English character sets may not be supported by Halcyon Marine Healthcare Systems

**Exceptions:** Any exceptions to this standard must be documented, reviewed and approved by the MIS Department.

**H. Server Audit Policy**

**1. Purpose**

The purpose of this policy is to ensure that all servers are deployed in Halcyon Marine Healthcare Systems are configured according to the security policies. Servers deployed in Halcyon Marine Healthcare Systems shall be audited annually and prescribed by applicable regulatory compliance.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources

- Ensure conformance to Halcyon Marine Healthcare Systems' security policies

**2. Scope**

This policy covers all servers owned or operated by Halcyon Marine Healthcare Systems. It also covers any server present in Halcyon Marine Healthcare Systems' premises, but which may not be owned or operated by Halcyon Marine Healthcare Systems.

**3. Policy**

Halcyon Marine Healthcare Systems hereby provides its consent to allow Internal and External Auditors to access its servers to perform scheduled and adhoc audits of all servers at Halcyon Marine Healthcare Systems.

**3.1 Specific Concerns**

Servers used for Halcyon Marine Healthcare Systems, supports critical business functions and store company sensitive information. Improper configuration of servers could lead to the loss of confidentiality, availability and integrity of these systems.

**3.2 Guidelines**

Approved and standard configuration templates shall be used when deploying server systems to include:

- All system logs shall be sent to a central log review system
- All Sudo / Administrator actions must be logged
- Use a central patch deployment system
- Host security agent such as anti virus shall be installed and updated
- Network scan to verify only requires network ports and network shares should be in use
- Verify administrative group membership
- Conduct baselines when systems are deployed and upon significant system changes
- Changes to configuration template shall be coordinated with approval of change control board

**3.3 Responsibility**

Internal and External Auditors shall conduct audits to all servers owned and operated by Halcyon Marine Healthcare Systems. The Server and application owners are encouraged to perform this work when needed.

**3.4 Relevant Findings**

All relevant findings discovered shall be listed in the Halcyon Marine Healthcare Systems tracking system, to ensure prompt resolution and appropriate mitigating controls.

**3.5 Ownership of Audit Report**

All results and findings generated by the Internal and External Auditors, must be provided to Halcyon Marine Healthcare Systems' management within one week of project completion. This Audit report will become the property of Halcyon Marine Healthcare Systems and considered as confidential.

## I. Server Malware Protection Policy

Halcyon Marine Healthcare Systems is entrusted with the responsibility of providing professional management to clients' servers as outlined in each contract. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems that they cover.

### 1. Purpose

The purpose of this policy is to outline which server systems are required to have an anti-virus and/or anti-spyware applications.

### 2. Scope

This policy applies to all servers that Halcyon Marine Healthcare Systems is responsible to manage. This explicitly includes any system which Halcyon Marine Healthcare Systems has a contractual obligation to administer. This also includes all server systems set up for internal use of Halcyon Marine Healthcare Systems, regardless of whether Halcyon Marine Healthcare Systems retain an administrative obligation or not.

## 3. Policy

The Halcyon Marine Healthcare Systems' operations staff will adhere to this policy to determine which servers need to install an anti-virus and/or anti-spyware applications and deploy such applications as appropriate.

### 3.1 ANTI-VIRUS

All servers must have an anti-virus application installed that offers a real-time scanning protection to files and applications running on the target system, if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- NBT/Microsoft Share access is open to this server from the systems used by non-administrative users
- HTTP/FTP access is open from the Internet

- Other "risky" protocols/applications are available to this system from the Internet at the discretion of the Halcyon Marine Healthcare Systems' Security Administrator

All servers should have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Outbound web access is available from the system

**3.2 MAIL SERVER ANTI-VIRUS**

If the target system is a mail server, it must have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications may be disabled during backups, if an external anti-virus application still scans the inbound emails while the backup is being performed.

**3.3 ANTI-SPYWARE**

All servers MUST have an anti-spyware application installed that offers a real-time protection to the target system if it meet one or more of the following conditions:

- Any system where non-technical or non-administrative users have a remote access to the system and any outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own

**3.4 NOTABLE EXCEPTIONS**

An exception to the above standards will generally be granted with minimal resistance and documentation if one of the following notable conditions will apply to this system:

- The system is a SQL server
- The system is used as a dedicated mail server
- The system is not a Window based platform

**4. Definition of terms**

- **Malware** - A software that is intended to damage or disable computers and computer systems
- **Spyware** - A software that enables user to obtain covert information on other computer activities by transmitting data covertly from their hard drive

**J. Data Backup Policy**

| QUALITY STANDARD SYSTEM MANUAL | HALCYON MARINE HEALTHCARE SYSTEMS | DOCUMENT NO. MIS 4.0 | EFFECTIVITY DATE: September 19, 2018<br>REVISION NO.: 2 |
|---|---|---|---|
| | | PREPARED BY: Marilar F. De Guzman, MD QAM | APPROVED BY: Glennda E. Canlas, MD Medical Director |

**SUBJECT: HMHS IT SECURITY POLICY AND STANDARDS**

Halcyon Marine Healthcare Systems has a duty to ensure that all information and data which it is responsible for being secure and routinely backed up. The MIS department has a responsibility to ensure that information and data which has been backed up can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances.

## 1. Purpose

The purpose of this policy is to identify and establish processes, procedures and good working practices for the backup and timely recovery of the Halcyon Marine Healthcare Systems' information and data existing in both electronic and physical form.

## 2. Scope

The scope of this policy extends to the backup of all important information and data regardless of the form it takes, including the recovery of IT systems and supporting infrastructure.

## 3. Policy

### 3.1 BACKUP TYPES

Backup of servers will occur every day after regular business hours.

**Full backup:** Includes all the source files. This method ignores the file's archive bit until after the file is backed up. At the end of the job, all files that have been backed up have their archive bits turned off. Only one full backup will be done once a week, followed by differential and/or incremental.

**Differential backups:** Includes files that have been changed since the last Full (Clear Archive Bit) or Incremental backup. If the archive bit is on, the file is backed up, and archive bit is not turned off. The next time an incremental backup is done, this file is skipped (unless it is modified again).

**Incremental backups:** Includes only files that have changed since the last Full (Clear Archive Bit) or Incremental backup. The next time that an incremental backup is done, the file will skipped (unless it is modified again). MIS Department use the GFS (Grandfather-Father-Son) rotation for backups.

**Daily backups** (Son) take place on a five day rotation.

**Weekly backups** (Father) take place on a five week rotation.

**Monthly backups** of high availability servers occur during the last calendar day of the month and on a twelve month rotation.

**Special backups** may be made for longer retention periods during special situations such as system upgrades and major projects.

### 3.2 DATA BACKUPS

1. The Halcyon Marine Healthcare Systems' MIS administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed, in line with the Halcyon Marine Healthcare Systems' Disaster Recovery Procedures and departmental data retention policies.

2. All IT backup and recovery procedures must be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery.
3. All data, operating systems/domain infrastructure state data and supporting system configuration files must be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration.

4. Where ever practicable backup media (e.g. Tape) must be encrypted and appropriately labeled. Any system used to manage backed-up media should enable storage of date/s and codes/markings for easy identification of the original source of the data and the type of backup used on the media. All encryption keys should be kept secure at all times with clear procedures in place to ensure that the backup media can be promptly decrypted in the event of disaster.

5. A recording mechanism must be in place and maintained to record all backup information such as department, data location, date, type of backup (e.g. Incremental, Full etc.) including any failures or other issues relating to backup job.

6. Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed.

7. Backup media, which are retained on-site prior to being sent for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised.

**8.** Access to the on-site backup location and storage safe must be restricted to authorized personnel only.

9. All backups identified for long term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media.

**10.** Hard copy files that contains important information and data should be scanned and stored electronically, to ensure that digital copies are created which can be backed up by the MIS Team.

11. Regular tests must be carried out to establish the effectiveness of the Halcyon Marine Healthcare Systems' backup and restore procedures by restoring data/software from backup copies and analyzing the results. MIS Head should be provided with information relating to any issues with backup testing of their data

**3.3 USER RESPONSIBILITIES**

Halcyon Marine Healthcare Systems' information system users also have a responsibility to ensure its data if it is securely maintained and available for backup:

1. IT Users must not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows

operating system and other authorized software which requires 'caching' of files locally in order to function). Instead, Users must save data on their allocated areas, this could be an area within the EDRM system, a mapped drive or network shared folder that the user has an access. Data that stored "locally" will not be backed up and therefore be at risk of exposure, damage, corruption or loss.

2. If the Halcyon Marine Healthcare Systems' network becomes unavailable for whatever reason and work related data is at risk of being lost, users have no option but to save the data locally (i.e. computer being used) or on approved media storage such as a Halcyon Marine Healthcare Systems' owned encrypted Data stick (USB storage). Once the Corporate Network becomes available again, the data should be immediately transferred to the corporate network in order to backed up safely, and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored.

3. Only the Halcyon Marine Healthcare Systems purchased and encrypted USB data sticks should be used and any data stored must be for temporary purposes. All sensitive, business and

personal identifiable information should be removed from the USB data stick and moved to an appropriate data network location as soon as possible, to ensure that he data is made available to Halcyon Marine Healthcare Systems and can be successfully backed up.

4. Mobile phones (not smart phones) must not be used to store sensitive, business or personal identifying information. In the event of unforeseen or unavoidable situations leading to important data being stored on mobile phones, the data must be stored in a suitable network location and removed from the phone as soon as possible.

### 3.4 DATA RESTORES

The Halcyon Marine Healthcare System has a well established backup and restore routines in place. Data (file) restores are normally carried out by the MIS Support Team who will endeavor to restore files from a date specified by the user or from the nearest backed up date.

1. IT Users must request data to be restored by contacting the MIS, preferably by sending request to MIS Helpdesk system. Only files which the user is authorized to access will be provided from the restore

2. The MIS Team will need to verify that the user has the permission and authorization to view or obtain restored copies of the file. The content will be restored at the same source folder and area, any requestor will need an access to restore the file.

3. Users requesting for a restore, are required to provide as much information about the data as necessary. It will include:

    - The reason for the restore
    - The name of file and folder to be restored
    - Original location of file and folder - the MIS support will provide guidance to the user on how to restore
    - Date, day or time of deletion/corruption or nearest approximation
    - The last date, day or time which the user recalls the data being intact and accessed successfully

4. All backup and recovery procedures must be documented and made available for MIS' data storage, which is responsible for carrying out data restores.

5. Requests from a third party software/hardware vendors for a file or system restores for the purpose of system support, maintenance,

testing or other unforeseen circumstance should be made under the supervision of the MIS Support Team through Halcyon Marine Healthcare Systems' Helpdesk.

6. Personnel accessing backup media for the purpose of a restore must ensure that any media used are returned to a secure location when no longer required.

7. A log must be maintained, to record the use of backup media whenever it has been requested or used for secure storage

**K. Information Systems Audit Policy**

**1. Purpose**

The purpose of this audit policy is to provide the guidelines on security audit team in conducting a security audit on IT based infrastructure system at various departments of Halcyon Marine Healthcare Systems. Security Audit is done to protect the entire system from the most common security threats which includes the following:

- Access to confidential data
- Unauthorized access of the departmental computers
- Password disclosure compromises virus infections

- Denial of service attacks
- Open ports, which may be accessed from outsiders (Unrestricted modems unnecessarily open ports)

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Monitor all security measures in compliance with Halcyon Marine Healthcare Systems' security policies
- Investigate the security incidents recorded in a security log book

**2. Scope**

This policy applies to all Halcyon Marine Healthcare Systems' network, data and system resources.

**3. Policy**

It is the responsibility of all Departments of Halcyon Marine Healthcare Systems to place an appropriate system of internal audit, which provides an independent assessment of security policies. To execute these policies, internal audit should also be done and reports/documents based on these audit should be generated. The MIS Head will be responsible for auditing their department and its sub department. When requested and

for the purpose of performing an audit, any access needed will be provided on Internal and External Audit team. This access may include:

- User level and/or system level access to any computing or communication device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective Department's equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to reports/documents created during the internal audit.
- Access to interactively monitor and log traffic on networks.

## IV. Web Application and Internet Security Policy

### A. Automatically Forwarded Email Policy

#### 1. Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

#### 2. Scope

This policy covers the automatic email forwarding and the potentially inadvertent transmission of sensitive information of all employees, vendors, and agents operating on behalf of Halcyon Marine Healthcare Systems.

**3. Policy**

Employees must exercise utmost caution when sending any email from inside Halcyon Marine Healthcare Systems to an outside network. Halcyon Marine Healthcare Systems' email will not be automatically forwarded to external destination, unless it is approved by the Manager and MIS Team. Sensitive information, as defined in the *Data Classification and Protection Policy*, will not be forwarded by any means, unless the email is critical to business and encrypted in accordance with the *Acceptable Encryption Policy*.

**B. Employee's Internet Use Monitoring and Filtering Policy**

**1. Purpose**

The purpose of this policy is to define the standards for systems that monitors and limits the web use from any host within Halcyon Marine Healthcare Systems' network. These standards are designed to ensure that employees use the Internet in a safe and responsible manner, and that the employee's web use can be monitored or researched during an incident.

## 2. Scope

This policy applies to all Halcyon Marine Healthcare Systems' employees, contractors, vendors and agents with a Halcyon Marine Healthcare Systems' owned or personally owned computer or workstation connected to the Halcyon Marine Healthcare Systems' network.

This policy applies to all end user initiated communications between Halcyon Marine Healthcare Systems' network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

## 3. Policy

### 3.1 Web Site Monitoring

The MIS Department shall monitor Internet use from all computers and devices connected to the corporate network. For all the traffic, the monitoring system must record the source IP Address, date, time, protocol, and destination site or server. When possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for 180 days.

**3.2 Access to Web Site Monitoring Reports**

General trending and activity reports will be made available to any employee upon request to the MIS Department. MIS, Security and Quality Assurance Department may access all reports and data if necessary, to respond to a security incident. The Internet use reports that identifies specific users, sites, teams, or devices will only be made available to associates outside the Security team upon written or email request to the MIS Department from their Human Resource Representative.

**3.3 Internet Use Filtering System**

The Information Technology Department shall block access to Internet websites and protocols that are deemed inappropriate for Halcyon Marine Healthcare System's corporate environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear

- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spy ware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate

**3.4 Internet Use Filtering Rule Changes**

The MIS Department shall review and recommend changes to web and protocol filtering rules periodically. The Human Resource Department shall review the recommendations and decide if any changes are to be made. Changes in the web and protocol filtering rules will be recorded in Internet Use Monitoring and Filtering Policy.

**3.5 Internet Use Filtering Exceptions**

Employees may request the site be unblock if the site is restricted by submitting a ticket using the MIS helpdesk. The MIS personnel will review the request and unblock the site if it is for working purposes.

Employees may access the blocked sites with the permission of MIS Team and Managing Head, if the purpose is appropriate and necessary for business. If an employee needs an access to a blocked site, he/she must submit a request to the Human Resource representative. The HR Department will present all approved exception requests to the MIS Department through writing or email. MIS Personnel will also track the approved exceptions and report upon request.

**C. Internet DMZ Equipment Policy**

**1. Purpose**

The purpose of this policy is to define the standards of all owned and operated equipment located outside of the Halcyon Marine Healthcare Systems' corporate Internet firewalls. These standards are designed to minimize the potential exposure of Halcyon Marine Healthcare Systems from loss of sensitive/confidential data, intellectual property, damage to public image and etc.

Devices that are Internet facing and outside the Halcyon Marine Healthcare Systems' firewall are considered as part of the "de-militarized zone" (DMZ) and are subject to this policy. The Network and host are particularly vulnerable to attack from the Internet since it resides from outside the corporate firewalls.

The policy defines the following standards:

- Ownership responsibility
- Secure configuration requirements
- Operational requirements
- Change control requirement

**2. Scope**

All equipment or devices deployed in DMZ owned and/or operated by Halcyon Marine Healthcare Systems (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) owned by Halcyon Marine Healthcare Systems, must follow this policy.

This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "halcyonmarine.com.ph" domain or appears to be owned by Halcyon Marine Healthcare Systems.

All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from MIS Department. All existing and future equipment deployed in Halcyon Marine Healthcare Systems' untrusted networks must comply with this policy.

## 3. Policy

### 3.1 Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by MIS Department for DMZ system, application, and/or network management.

Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main function and application.
    - Password groups of privileged passwords.

- Network interfaces must have an appropriate Domain Name Server (DNS) records (minimum of A and PTR records).

- Password groups must be maintained in accordance with the corporate wide password management system/process.

- Immediate access to equipment and system logs must be granted to members of the MIS upon demand, per the *Audit Policy*.

- Changes to existing equipment and deployment of new equipment must follow and corporate governess or change management processes/procedures.

To verify the compliance with this policy, MIS Department will audit the DMZ equipment periodically as per the *Audit Policy*.

**3.2 General Configuration Policy**

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by the MIS Department as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches/hot-fixes recommended by the equipment vendor and MIS department must be installed. This applies

to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have a process in place to stay updated on appropriate patches/hot fixes.

- Services and applications that are not serving the business requirements must be disabled.
- Trust relationships between systems, may only be introduced according to business requirements. It must be documented and approved by MIS Department.
- Services and applications that are not for general access must be restricted by an access control list.
- Unsecured services or protocols determined by MIS Department must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over a secure channel (e.g., encrypted network connections using SSH or IPSEC) or console access that is independent from DMZ networks. When a methodology for secure channel connections is not available, one-time passwords must be used for all access levels.
- All host content updates must occur over secure channels.

- Security-related events must be logged and audit trails saved to MIS-approved logs. Security-related events includes but are not limited to the following:
    - User logs in failures.
    - Failure to obtain the privileged access.
    - Access policy violations.

- MIS Team will address non-compliance waiver requests on a case-to-case basis and approve waivers if justified.

**3.3 New Installations and Change Management Procedures**

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via *DMZ Equipment Deployment Process*.
- Configuration changes must follow the Corporate Change Management (CM) Procedures.
- MIS team must be invited to perform the system/application audits prior to the deployment of new services.

- MIS team must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

**3.4 Equipment Outsourced to External Service Providers**

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

**D. Internet Usage Policy**

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

Access to the Internet by personnel who is inconsistent with business needs results in the misuse of resources. These activities may adversely affect productivity due to time spent using the Internet. Additionally, the company may face loss of reputation and possible legal action through other types of misuse.

All information found on the Internet should be considered a suspect until confirmed by another reliable source. There is no quality control process on the Internet and a considerable amount of its information is outdated or inaccurate.

Access to the Internet will be provided to users to support the business activities and only as a needed basis to perform their jobs and professional roles.

**1. Purpose**

The purpose of this policy is to define the appropriate uses of the Internet by Halcyon Marine Healthcare Systems' employees and affiliates.

**2. Scope**

The Internet usage Policy applies to all Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. The company's Internet users are expected to be familiar and comply with this policy. It is also required to use their common sense and exercise their good judgment while using the Internet services.

**2.1 Internet Services Allowed**

*Internet access is to be used for business purposes only*.
Capabilities for the following standard Internet services will be provided to users as needed:

- E-mail - Send or receives E-mail messages using the Internet (with or without document attachments).

- Navigation - WWW services as necessary for business purposes using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.
- File Transfer Protocol (FTP) - Send files and receives inbound files necessary for business purposes.
- Telnet - Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into the company.

Management reserves the right to add or delete services as business needs change or warrant conditions.

***All other services will be considered unauthorized access to the Internet .***

**2.2 Request and Approval Procedures**

Internet access will be provided to users to support business activities and only needed to perform their jobs.

**2.2.1 Request for Internet Access**

As part of the Internet access request process, the employee is required to read both Internet usage Policy and the associated Internet/Intranet Security Policy. The

user must sign the statements that he/she understands and agrees to comply with the policies. Users that do not comply with these policies could be subject to disciplinary action or termination. Acknowledgment Form should be signed before access will be granted.

**2.2.2 Approval**

Users or user's manager requesting an Internet access is required to submit an ***Internet Access Request*** form to the MIS Department along with signed Internet usage Coverage Acknowledgment Form.

**2.2.3 Removal of privileges**

Internet access will be discontinued upon termination of employment, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In case of change in job function or transfer, the original access code will be discontinued and only be reissued if necessary. A new request for access is will be approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to

feedback from management, systems administrators must promptly revoke all privileges if no longer needed by users.

**3. Policy**

**3.1 Resource Usage**

Access to the Internet will be approved and provided only if the reasonable business needs are identified. Internet services will be granted based on employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new Internet access request must be submitted within 5 days. User's Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

**3.2 Allowed Usage**

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the MIS Department.

Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes;

- IT technical support downloading software upgrades and patches;
- Review of possible vendor web sites for product information;
- Reference regulatory or technical information;
- Research;

**3.3 Personal Usage**

Using the company's computer resources to access the Internet for personal purposes without the approval of the user's manager and MIS department, it may be considered a cause for disciplinary action or termination.

All users of the Internet should be aware that the company network creates an audit log,reflecting on the request for service, both inbound and outbound addresses.

The company is not responsible to any loss of information stored in wallet or any consequential loss of personal property to users who choose to store or transmit personal information such as private keys, credit card numbers, certificates or use of Internet "wallets".

**3.4 Prohibited Usage**

Information stored in the wallet, or any consequential loss of personal property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited includes, but are not limited to:

- Accessing company's information that is not within the scope of their work. This includes the unauthorized reading of customer's account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misuse, disclose, without proper authorization, or altering customer or personnel's information. This includes the making of an unauthorized changes to a personnel file or sharing of electronic data of customer/personnel with unauthorized personnel.
- Deliberate pointing or hyperlinking of company Web sites to other Internet/WWW sites whose content may be

inconsistent or in violation of the aims or policies of the company.

- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations of local, state, national or international law including without limitations control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices are state otherwise.
- Transmission of any proprietary, confidential, or sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to, comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
- Any form of gambling.

Unless specifically authorized under the provisions of section 3.3, the following activities are also strictly prohibited:

- Unauthorized downloading of any shareware programs or files used without authorization in advance from the MIS Department and user's manager.
- Any ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any online contest or promotion.
- Acceptance of promotional gifts.

Bandwidth within the company and connecting to the Internet is a shared finite resource. Users must make a reasonable effort to use this resource in any ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation and may ban the downloading of a particular file type.

**3.5 Software License**

The company strongly supports a strict adherence to software vendor license agreements. When at work or company computing or networking resources are employed, copying of software that is not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the MIS Department for review or to

request an approval from the management before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless the permission from the copyright owner is obtained, making copies of material from magazines, journals, newsletters, other publications and online documents are forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using of company's computer resources without the approval from the user's manager and the MIS Department to access the Internet, may be considered as a cause for disciplinary action and termination.

All users of the Internet should be aware that the company network creates an audit log, reflecting on the request for service of both inbound and outbound addresses and are periodically reviewed. Users who choose to store or transmit personal information such as private keys, credit card numbers, certificates or use of Internet "wallets" do so at their own risk.

**3.6 Review of Public Information**

All publicly-writable directories on Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information that are inconsistent with company business. Examples of unauthorized public information are pirated information, passwords, credit card numbers, and pornography.

### 3.7 Expectation of Privacy

#### 3.7.1 Monitoring

Users should consider that their Internet activities are periodically monitored and limit their activities accordingly. Management reserves the right to examine the E-mail, personal file directories, web access, and other information stored on the company computers any time and even without notice. This examination ensures the compliance with internal policies and assists the management with the company's information systems.

#### 3.7.2 E-mail Confidentiality

Users should be aware that the clear text E-mail is not a confidential means of communication. The company cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can depend on technology, be

forwarded, intercepted, printed and stored by others. Users should also be aware that once an E-mail is transmitted, it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which has been transmitted.

### 3.8 Maintaining the Corporate Image

#### 3.8.1 Representation

When using the company's resources to access and use the Internet, users must realize that they represent the company. Whenever an employee's state an affiliation to the company, they must clearly indicate that "the opinions are expressed on my own and not necessarily of the company". Questions may be addressed to the MIS Department.

#### 3.8.2 Company Materials

Users must not place the company material, e.g. internal memos, press releases, product or usage information, documentation, etc. on any mailing list, public news group or service. Any posting of materials must be approved by the employee's manager and the HR Department and will be placed by an authorized individual.

### 3.8.3 Creating Web Sites

All individuals and business units that are wishing to establish a WWW home page or site must develop a business, implementation, and maintenance plans. Formal authorization must be obtained through the MIS Department. This will maintain the publishing and content standards needed to ensure its consistency and appropriateness.

In addition, the contents of the material made available to the public through the Internet must be formally reviewed and approved before being published. All materials should be submitted to the Management for initial approval. All company pages are owned and the responsibility of Halcyon Marine Healthcare Systems.

All company web sites must be protected from unwanted intrusion through formal security measures which can be obtained from the MIS department.

## 3.9 Periodic Reviews

### 3.9.1 Usage Compliance Reviews

To ensure the compliance with this policy, periodic reviews will be conducted. These reviews will include the degree of compliance with usage policies.

**3.9.2 Policy Maintenance Reviews**

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to suit the company's information needs.

**E. Web Application Security Policy**

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application will be assessed for vulnerabilities and any vulnerabilities will be re-mediated prior to production of deployment.

1. **Purpose**

The purpose of this policy is to define the web application security assessments within Halcyon Marine Healthcare Systems. Web application assessments are performed to identify the potential or weaknesses as a result of inadvertent misconfiguration, weak authentication, insufficient error handling, sensitive information leakage and etc. Discovery and subsequent mitigation of these issues will limit the attack surface of

Halcyon Marine Healthcare Systems' services available in both internal and external as well as the compliance with any relevant policies in place.

**2. Scope**

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management and change control of technologies in use at Halcyon Marine Healthcare Systems.

All web application security assessments will be performed by delegating security personnel either employed or contracted by Halcyon Marine Healthcare Systems. All findings are considered as confidential and to be distributed to persons on a "need to know" basis. Distribution of any findings outside of Halcyon Marine Healthcare Systems is strictly prohibited unless approved by the Management.

Any relationships with multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

**3. Policy**

3.1 Web applications are subject to security assessments based on the following criteria:

a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.

b) Third Party or Acquired Web Application – will be subject to a full assessment after which it will be bound to policy requirements.

c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.

e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be

designated by the MIS Head or Manager who has been delegated this authority.

3.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate the fix and/or mitigation strategies of any discovered issues in Medium risk level or greater.

a) **High** - Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit the exposure before deployment. Applications with high risk issues are subject to taken offline or denied release into the live environment.

b) **Medium** – Medium risk issues should be reviewed to determine the required mitigation and schedule accordingly. Applications with medium risk issues may be taken offline or denied the release to live environment based on the number of issues which increase the risk to be in unacceptable levels. Issues should be fixed in a patch/point release unless other mitigation strategies will limit the exposure.

c) **Low**–Issue should be reviewed to determine the requirements in correcting the issue and schedule accordingly.

3.3 The following security assessment levels shall be established by the MIS team or other designated organization that will be performing the assessments.

a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use a manual penetration testing techniques to validate the discovered vulnerabilities in determining the overall risk of all.
b) Quick – A quick assessment will consist of a (typically) automated application scan for the OWASP Top Ten web application security risks at a minimum.
c) Targeted – A targeted assessment is performed to verify the vulnerability remediation changes or new application functionality.

3.4 The current approved web application security assessment tools which will be used for testing are:

- <Tool/Application1>
- <Tool/Application2>
- …

Other tools and/or techniques may be used depending on the default assessment found and validity/ risk that are subject to the discretion of the MIS team.

**4. Definition of Terms**

- **OWASP** - (Open Web Application Security Project) is an organization that provides unbiased, practical and cost-effective information on computer and Internet applications.

## V. Laptop and Mobile Security Policy

### A. Mobile Device Encryption Policy

Mobile devices such as smart phone and tablets, offers a great flexibility and improved productivity for employees. However, they can also create added risk

and potential targets for data loss. As such, there use must be in alignment with appropriate standards and encryption technology should be used when possible.

**1. Purpose**

This document describes the Information Security requirements for encrypting data on Halcyon Marine Healthcare Systems' mobile devices.

**2. Scope**

This policy applies to any mobile devices issued by Halcyon Marine Healthcare Systems or used for business which contains stored data owned by the company.

**3. Policy**

All mobile devices that contain stored data owned by Halcyon Marine Healthcare Systems must use an approved method of encryption to protect data. Mobile devices are defined to include laptops, PDAs, and cell phones.

Users are expressly forbidden from storing of data to non issued devices of Halcyon Marine Healthcare Systems.

**3.1 Laptops**

Laptops must employ full disk encryption with an approved software encryption package. No Halcyon Marine Healthcare Systems data may exist on a laptop in plain text.

**3.2 PDA and Cell phones**

Any Halcyon Marine Healthcare Systems' data stored on a cell phone or PDA must be saved to an encrypted file system using the company's approved software. Halcyon Marine Healthcare Systems shall also employ the remote wipe technology to remotely disable and delete any data stored in Halcyon Marine Healthcare Systems' PDA or cell phone which is reported as lost or stolen.

**3.3 Keys**

All encryption keys and pass-phrases must meet complexity requirements described in Halcyon Marine Healthcare Systems' *Password Protection Policy*.

**3.4 Loss and Theft**

The loss or theft of any mobile device containing Halcyon Marine Healthcare Systems' data must be reported immediately.

**4. Related Standards, Policies and Processes**

- Password Protection Policy

**5. Definition of Terms**

- **Full Disk Encryption** - Full-disk encryption (FDE) is the encryption of all data on a disk drive, including the program that encrypts the bootable OS partition. It is performed by disk encryption software or hardware that is installed on the drive during manufacturing or via an additional software driver.
- **Remote Wipe** - Remote wipe is a security feature that allows a network administrator or device owner to send a command to a computing device and delete data.

B. **Mobile Employee Endpoint Responsibility Policy**

**1. Purpose**

This document describes the Information Security's requirements for employees of Halcyon Marine Healthcare Systems that work outside the office.

**2. Scope**

This policy applies to any mobile device, or endpoint computer issued by Halcyon Marine Healthcare Systems or used for Halcyon Marine Healthcare Systems' business which contains stored data owned by Halcyon Marine Healthcare Systems.

**3. Policy**

All employees shall assist in protecting devices issued by the Halcyon Marine Healthcare Systems or storing Halcyon Marine Healthcare Systems' data. Mobile devices are defined to include desktop systems in a telework environment, laptops, PDAs, and cell phones.

Users are expressly forbidden from storing Halcyon Marine Healthcare System data on devices that are not issued by Halcyon Marine Healthcare Systems, such as storing Halcyon Marine Healthcare Systems' email on a personal cell phone or PDA.

**3.1 Anti-Virus and Endpoint Security Software**

The Halcyon Marine Healthcare Systems will issue a computers with installed Anti-virus and Endpoint security. Employees will notify the MIS department immediately if they see an error messages for these products. Employees shall run on online malware scanner at least once a month.

**3.2 Browser Add-ons**

In general, Halcyon Marine Healthcare Systems does not recommend the use of Browser Add-ons, however, the company does not forbid the use of this tool if it enhance the productivity. After installing the Browser Add-on, employees shall run a browser testing tool.

## C. Personal Communication Devices and Voice mail Policy

### 1. Purpose

This document describes the Information Security's requirements for Personal Communication Devices and Voice Mail of Halcyon Marine Healthcare Systems.

### 2. Scope

This policy applies to any use of Personal Communication Devices and Voice Mail issued by Halcyon Marine Healthcare Systems.

### 3. Policy

#### 3.1 Issuing Policy

Personal Communication Devices (PCDs) will be issued only to Halcyon Marine Healthcare Systems' personnel with duties that requires to be the immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include hand-held wireless devices, cellular telephones, laptop wireless cards and pagers. Effective distribution of the various technological devices must be limited to persons whom the productivity gained is appropriate in relation to the costs incurred.

Hand-held wireless devices may be issued to Halcyon Marine Helathcare Systems' personnel for operational efficiency. These employees are generally in the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

**3.2 Bluetooth**

Hands-free enabling devices, such as the Bluetooth, may be issued to the authorized Halcyon Marine Healthcare Systems' personnel who received an approval. Care must be taken to avoid being recorded when peering Bluetooth adapters, Bluetooth 2.0 Class 1 devices have a range of 330 feet.

**3.3 Voice Mail**

Voice Mail boxes may be issued to Halcyon Marine Healthcare Systems' personnel who require to leave messages when they are not available. Voice Mail boxes must be protected by a PIN which must never be the same as the last four digits of the Voice Mail box's telephone number.

**3.4 Loss and Theft**

Files containing a confidential or sensitive data may not be stored in PCDs unless protected by an approved encryption. Confidential or sensitive

data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or services may be the responsibility of the employee, as determined on a case-to-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported.

**3.5 Personal Use**

PCDs and voice mail are issued for Halcyon Marine Healthcare Systems' business purposes. Personal use should be limited to minimal and incidental use.

**3.6 PCD Safety**

Conducting of telephone calls or utilizing PCDs while driving should be a safety hazard. Drivers should use PCDs when parked or out of the vehicle. If employees used a PCD while driving, Halcyon Marine Healthcare Systems' require the use of hands-free enabling devices.

**D. Remote Access on Mobile Computing Storage Policy**

With advances in computer technology, mobile computing and storage devices become a useful tool for the business of Halcyon Marine Healthcare Systems. These devices are susceptible to loss, theft, hacking, and distribution of malicious software, because these are portable and can be used anywhere. As

mobile computing became more widely used, it is necessary to address security to protect the information resources of Halcyon Marine Healthcare Systems.

1. **Purpose**

   The purpose of this policy is to establish an authorized method of controlling mobile computing and storage devices that accessed the information resources of Halcyon Marine Healthcare Systems.

2. **Scope**

   The Halcyon Marine Healthcare Systems' employees, consultants, vendors, contractors, students, and others who used a mobile computing and storage devices on the network of Halcyon Marine Healthcare Systems.

3. **Policy**

**3.1 General Policy**

It is the policy of Halcyon Marine Healthcare Systems that there must be an approval before accessing the information resources of Halcyon Marine Healthcare Systems. It pertains to all devices connecting to the network of Halcyon Marine Healthcare Systems, regardless of ownership.

Mobile computing and storage devices include, but are not limited to laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial

Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, hand-held wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or owned by Halcyon Marine Healthcare Systems, that may connect or access the information system of Halcyon Marine Healthcare Systems. A risk analysis for each new media type shall be conducted and documented prior to its use or connection to the network of Halcyon Marine Healthcare Systems unless the media type has already been approved by the MIS Department. The MIS Team will maintain a list of approved mobile computing and storage devices.

Mobile computing and storage devices can be easily lost or stolen, presenting a high risk for unauthorized access and introduction of malicious software to the network of Halcyon Marine Healthcare Systems. These risks must be mitigated to acceptable levels.

Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive information about Halcyon Marine Healthcare Systems must use an encryption or equally strong measures to protect the data while it is being stored.

Unless written approval has been obtained from the MIS Head and Management, databases or portions thereof, which reside on the network at the Halcyon Marine Healthcare Systems, shall not be downloaded to mobile computing or storage devices.

**3.2 Procedures**

To report the lost or stolen mobile computing and storage devices, call for the MIS Helpdesk support. For further procedures on lost or stolen hand-held wireless devices, please see the Procedures section.

The MIS Team shall approve all new mobile computing and storage devices that will connect to information systems of Halcyon Marine Healthcare Systems.

Any non-departmental owned device that may connect to Halcyon Marine Healthcare Systems' network must be approved by technical personnel. Refer to the Mobile Media Standards for detailed information.

**3.3 Roles and Responsibilities**

Users of mobile computing and storage devices must diligently protect such devices from loss and disclosure of private information that belong and maintained by Halcyon Marine Healthcare Systems. Before

connecting a mobile computing or storage device to Halcyon Marine Healthcare Systems' network, users must ensure that the equipment is on the list of approved devices issued by the Halcyon Marine Healthcare Systems.

The MIS Team must be notified immediately upon detection of a security incident, especially when a mobile device may have been lost or stolen.

The MIS Team is responsible for the mobile device policy at Halcyon Marine Healthcare Systems and shall conduct a risk analysis to document the safeguards of each media type to be used on network or on equipment owned by Halcyon Marine Healthcare Systems.

The MIS Team is responsible for developing procedures for implementing this policy. The MIS Team will also maintain a list of approved mobile computing and storage devices.