Document Title	Cyber Security Policy
Document Reference	13.01
Version	1.0.0.5
Issue Date	1st January 2023
Document Author	John F Macleod
Document Approval	Douglas Leask
Applicability	All areas of operations within the company
Pages	6

1.0 Purpose

The purpose of this policy document is to detail Leask Marine Ltd's Information Technology (IT) infrastructure regarding Cyber security. The procedure encompasses hardware, software, network resources and services for the secure operation of the IT system.

2.0 Scope

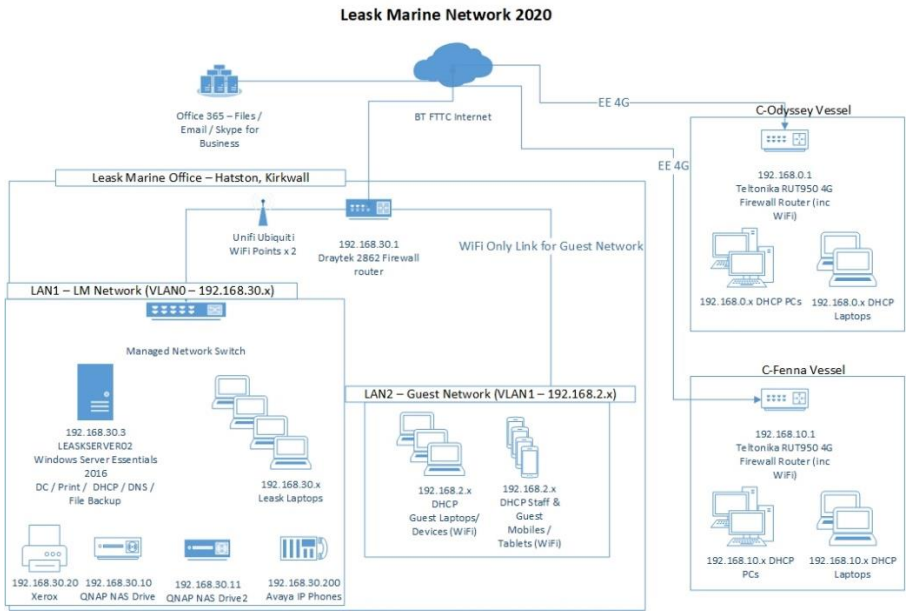
This document gives an overview of all aspects relating to Cyber Security of the Company's IT systems. The procedure will incorporate the following;

- Boundary Firewalls and Gateways
- Access Control & Administrative Privilege Management
- Internet Access Policy
- Patch Management
- Malware Protection

3.0 Responsibilities and Requirements

The Commercial Manager is the appointed Information security Manager responsible for ensuring that the suitable equipment and software is supplied and suitable for authorised use. The Company's IT systems are managed on a day-to-day basis by their sub-contractor RM Computing (Orkney) Limited. The appointed RM Computing appointed responsible person is Mr Robert Gray.

4.0 Business Network Layout



5.0 Policies

5.1 Boundary Firewalls and Internet Gateway

5.1.1 The primary business computer network (Leask Marine Office) is protected by a Draytek 2830 firewall router, which is situated at the edge of the business network. There are two secondary networks located on-board vessels which each have firewall routers located at the edge of each business network (C-Odyssey Vessel and C-Fenna Vessel).

5.1.2 On the primary network the firewall is configured with one administration level access login, and it can only be administered from internally of the network, or directly from our external IT Support provider's office (RM Computing (Orkney) Ltd).

On each of the secondary networks the firewall is configured with one administration level access login and can only be administered from internally on the network.

5.1.3 The firewall passwords are set as minimum of 12 characters and include a mixture of letters numbers and special characters. Leask Marine staff do not hold the router passwords, these are held by our external IT Support provider.

5.1.4 All open firewall ports inbound and outbound on the Firewall will be reviewed on quarterly to ensure all implemented policies are still valid with any policies removed as needed. The open ports are detailed in the **Firewall Port Settings** log and the reviews are logged in the **Cyber Security Review Log**.

5.1.5 The computer host-based firewalls will be installed on all workstations with this enforced by Active Directory Group Policy Object for all domain connected computers and using Local Computer Group Policy for all non-domain connected computers. Staff are not permitted to adjust firewall settings on workstations.

5.1.6 Changes to firewall rules need to be pre-approved by the Managing Director with changes retained as part of the **Cyber Security Change Log** and **Firewall Port Settings log**. Change requests for firewall rules should be submitted immediately for approval to the Managing Director with an indication of any required timescales outlined.

5.2 Access Control and Administrative Privilege Management

5.2.1 Logon - To log onto organisations devices, a user will require a username and a strong password that meets the policies defined here. At log on previous system users' names will be removed from the log on screen. This is enforced by Active Directory Group Policy Object for domain connected devices and manually for no domain connected devices.

5.2.2 User Accounts - A register of user accounts will be maintained at **Authorised Users & Internet Access** log with the **Managing Director** with these permissions reviewed quarterly with a log of the reviews maintained at **Cyber Security Review Log**.

5.2.3 Administrative Accounts **-** Only authorised users will be given administrative level permission with this logged and tracked on **Authorised Users & Internet Access** log with these permissions reviewed quarterly with a log of the reviews maintained at **Cyber Security Review** Log. Where administrative access is granted to a user, this must be approved by the Managing Director and logged in the **Authorised Users & Internet Access** log.

5.2.4 Old User Accounts **-** All user accounts will be deleted 3 months after the employee terminates employment with the company with any user which requiring approval from senior manager

if it is to be retained longer than this. A review of all user accounts will be carried out quarterly and maintained at **Cyber Security Review Log**.

5.2.5 Users Passwords - Every user who requires access the system must have a unique defined login and unique password. The user password will be set as complex password at system level and managed using Active Directory for domain connected computers and manually where they are not domain connected. The password rules must contain at least 1 of each of the following characters;

- Upper Letters A – Z
- Lowercase Letters a – z
- Numbers 0 – 9
- Special Characters, e.g. (!, $ #, %)

Password Minimum Characters	12
Meet Complexity	Yes
Password History	10
Account lockout threshold	10 attempts
Account lockout duration	10 minutes
Account lockout reset	5 minutes

Users should avoid choosing obvious passwords such as those based on easily discoverable information like pets, children, and place of birth. Passwords should ideally be based on multiple unrelated words rather than words from the English language.

5.2.6 Storing Passwords – Users can only store passwords in authorised password management systems. Approved password management software is listed in the Software Control Register. Where passwords are stored on paper these must be given to the Managing Director. These password storage policies should only be used where the password is used infrequently and would benefit from being stored.

5.2.7 Change Passwords - Users must change their passwords promptly if they suspect that their password has been compromised.

5.2.8 System / Administrator Passwords - Every administrator level user account password must meet the complexity defined above. System / Administrator passwords will be reset on each quarterly service visit.

5.2.9 **Data Location Register** – The Information Security Manager will maintain the Sensitive or Business Critical Data Register of locations where business critical or sensitive data is held. Access to the data will be restricted to approved users only with this reviewed and logged quarterly in the Cyber Security Review Log.

5.2.10 Wi-Fi - No employee shall be permitted to use the business Wi-Fi or the guest Wi-Fi connections without authority from the Managing Director. In the event of a guest requiring Internet access through the business network, the password for the guest Wi-Fi shall be the only password shared. The password for the business Wi-Fi will be changed every quarter as part of the scheduled maintenance to be carried out on the Wi-Fi equipment.

5.3 Internet Access

Internet Access will only be authorised to authorised users with the log of authorised users kept in the Authorised Users & Internet Access register. A Blacklist of unauthorised webpages and categories are in place, managed through the third-party web filtering service "Webroot DNS Protection". All users are required to limit their use of the Internet to sites and searches appropriate to their job. The company may monitor all Internet use by employees.

Users are expressly forbidden from accessing web pages or download files from the Internet that could in anyway be regarded as illegal, offensive, in bad taste or immoral. Users who are working on any computer console or using a remote login with administrative permissions, should not access the Internet directly. Files should be downloaded by a normal user account and saved to allow installation to be performed by an administration level user.

5.4 Software Control Measures

5.4.1 A **Software Control Register** will be maintained by the **Information Security Manager** for all installed software throughout the organisation and only software from this may be installed on computers by authorised users. Any software required or used on the network must be approved by a senior manager with the **Software Control Register** being updated when software is installed/removed from a computer system.

5.4.2 Software listed in the **Software Control Register** must be licensed, supported, and be set to automatically update, where available, and is reviewed quarterly to ensure that these criteria is met with software updated/removed as appropriate.

5.4.3 Build Process – All new computers will be built to comply with the **Computer Build Process Checklist**.

5.4.4 Auto-run - All computer system will have the Auto Run/Auto Play features turned off to prevent the accidental execution of code on computer systems. This policy is enforced through Active Directory Group Policy Objects for domain connected computers and manually for non-domain connected computers.

5.4.5 User Account Control - All computer system will have the User Account Control features turned on and configured to the maximum level to prevent the accidental execution of code on computer systems. This policy is enforced through Active Directory Group Policy Objects for domain connected computers and manually for non-domain connected computers.

5.4.6 Executable Code – Users are not permitted to run unauthorised executable; this includes program installation. Only authorised administrative users shall be permitted to install programs and updates.

5.4.7 Removable Media - Users are not permitted to use removable media for the import and export of information without authority with the devices to be configured with encryption.

5.5 Malware

Malware Protection - All computer devices will operate with the organisations approved security protection “Webroot Secure Anywhere” at all times with this installed and managed to ensure that all devices have receive regular product updates. The solution is configured to perform a full scan of the device daily with this managed by a central policy.

5.6 Patch Management

5.6.1 All Microsoft based operating systems and configured and controlled through Active Directory Group Policy Object if they are domain joined or manually if they are not domain joined to automatically download and install security updates.

5.6.2 All network devices and computers that are not running a Windows operating system are checked quarterly to see if there are any updates to be applied with them reviewed and installed in a timely manner.

5.7 Event Logs

All Windows based computers will be configured to retain a minimum of 7 days of system event logs with these controlled by Active Directory Group Policy Objects for domain connected computers and manually for all non-domain connected computers.

5.8 Data Backup

All critical computer systems are configured to carry out a data backup daily to meet the business requirements to protect critical business data and operates as defined below:

- An encrypted image backup is always used.
- The external drive is only connected when there is a backup scheduled
- Data backups are retained for a minimum of 3 months
- Data backups are tested from (various media) on a quarterly basis

5.9 Compliance

To ensure compliance a regular audit process has been established whereby the tracked computer systems will be audited quarterly to ensure no un-approved changes have taken place. The checklist (13.09 RM Quarterly Service Visit) includes the following areas;

- Software Audit
- Windows Updates
- Review Software Updates
- Review User Accounts
- Review Admin Accounts
- Review Password Policy
- Review Events Logs
- Review Port Status
- Review Firewall Updates

- Review Client Malware protection

6.0 Review and Monitoring

The Cyber Security Policy procedure will be reviewed annually in January by the company including support and input from third party service providers with recommendations made regarding

7.0 Records

1.02.1 Health & Safety Policy
1.02.2 Structure of Policies within the IMS
13.16 GDPR Procedures
13.18 Statement of Applicability procedures
13.18.1 Statement of Applicability Annex A
13.19 Information Classification & Handling Procedures

8.0 References

ISM Code BS EN ISO/IEC 27001:2017

This policy will be reviewed annually to ensure it reflects the businesses current priorities, plans and targets.

Signed: 

Name: Douglas Leask, Managing Director

Date: 1st January 2023