UNITED SHIP CHANDLERS LTD
Quality policy statement

Company USCL(United Ship Chandlers Ltd) was established in 1997 to provide chandlery services to the oil/marine industry. We are based in Trinidad Port of Spain and employ 16 persons.

Quality is important to our business because we value our customers. We strive to provide our customers with products and services which meet and even exceed their expectations.

We are committed to continuous improvement and have established a Quality Management System which provides a framework for measuring the quality of our products/goods.

We have the following systems and procedures in place to support us in our aim of total customer satisfaction and continuous improvement throughout our business:

1. Regular gathering and monitoring of customer feedback
2. A customer complaints procedure
3. Selection and performance monitoring of suppliers against set criteria
4. Training and development for our employees
5. Regular audit of our internal processes
6. Measurable quality objectives which reflect our business aims
7. Management reviews of audit results, customer feedback and complaints
8. Ensure all employees are wearing disposable gloves when handling provisions.
9. Ensure cold Storages & Chillers are set to -1**0° F** and **35° to 45°F respectively.**
10. Ensure all items are stored in separate areas taken into consideration the nature of the goods(eg chemicals and dry goods stored separately)

Our internal procedures are reviewed regularly and are held in a Quality Manual which is made available to all employees

This policy is posted on the Company Notice Board and can also be found in the staff handbook.

The essentially qualitative feature of USCL is the "punctual and full realization of the agreed customer requirements", taking into account the relevant environmental aspects. By accepting this challenge and following it in the daily work procedures we offer our customers a maximum delivery capacity, an attractive service portfolio and an interesting range of products of reliable high quality.

All persons of the company are informed about the content of this Q&U-Politics and are motivated to follow it strictly. In order to realize this important part of the company strategy it is necessary to have the unconditional support of all employees - from the warehouse worker, driver, clerk and all kinds of management levels to the managers and owner.

Although the Managing Director has ultimate responsibility for Quality, all employees have a responsibility within their own areas of work to help ensure that Quality is embedded within the whole of the company.

The policy review date is 21 September, 2018

Signed:.....(Director) PAUL ABRAHAM

Date:.....19/3/19.....

Health,Safety & Environmental policy

UNITED SHIP CHANDLERS LTD is committed to providing and maintaining a safe and healthy workplace for all workers (including contractors and volunteers) as well as clients, visitors and members of the public. Hazards and risks to health and safety will be eliminated or minimised, as far as is reasonably practicable.

The responsibility for managing health and safety ultimately rests with the person in control of the business or undertaking (PCBU), directors and management. Workers also have important responsibilities for health and safety in the workplace.

We are committed to complying with the *Work Health and Safety Act of Trinidad & Tobago*, the Work Health and Safety Regulation , codes of practice and other safety guidance material.

Management will:

- Ensure the business complies with all legislation relating to health and safety
- Eliminate or minimise all workplace hazards and risks as far as is reasonably practicable
- Provide information, instruction and training to enable all workers to work safely
- Supervise workers to ensure work activities are performed safely
- Consult with and involve workers on matters relating to health, safety and wellbeing
- Provide appropriate safety equipment and personal protective equipment
- Provide a suitable injury management and return to work program

Workers will:

- Take reasonable care for their own health and safety
- Follow safe work procedures, instructions and rules
- Participate in safety training
- Report health and safety hazards
- Report all injuries and incidents
- Use safety equipment and personal protective equipment as instructed

Our goal is to provide a safe and healthy work environment that is free from workplace injury and illness. This will only be achieved through the participation, co-operation and commitment of everyone in the workplace.

Name: Parry Abraham Position: Director

Signature: Date: 1/1/2019

Review date: 1/1/19

United Ship Chandlers Ltd Security Protocols

Data management

- Backups of data are taken on a daily basis. .

Risk assessments

United Ship Chandlers Ltd security team perform quarterly risk assessments including security auditing, penetration testing, vulnerabilities assessment, and account auditing. Based on the assessment, security recommendations are made to the relevant organizational departments, and security patches and software upgrades are performed. If vulnerabilities are discovered, security updates and/software updates are performed immediately, and do not wait for the scheduled security assessment period. An investigation into any resulting breaches is immediately performed as per the Breach Policy below.

Firewalls & Security Software

- Security groups and secure management ports are enabled on all of our instances.
- All staff and contractor devices have up to date anti-virus and anti-malware software.

Accounts

United Ship Chandlers conducts a quarterly review of all the privileged accounts in the technology stack. In coordination with the HR and Operations Departments, terminated users and/or staff accounts are disabled and privileges are revoked immediately upon departure or end of contract.

Login Security

All account changes are monitored and logged, and alerts are sent to notify users in case of changes in their account access credentials. United Ship Chandlers encourages all staff to change all their login credentials bi-annually.

Security Awareness

- We provide in-house training to all staff about data security and protection, and all privacy policies and procedures are presented to incoming staff.
- All staff who have access to user data must sign a Non-Disclosure Agreement.
- IT staff are additionally trained on complying with the organization's security standards and making users aware of policies and procedures regarding appropriate use of networks, systems, and applications.

United Ship Chandlers Data Breach Policy

Risk Assessment and Incident Prevention

Preventing incidents is less costly than reacting to them after they occur. Thus, in addition to automated detection capabilities, as part of the organization's incident prevention policy, the security team will conduct quarterly risk assessments under the direction of the IT Director.

The assessment will include a review of baseline activity logs and the security of all data repositories, ports, anti-virus products, application activity, usage data, email security, and intrusion detection.

Based on the outcome of the risk assessment, the organization will determine the presence of incident precursors and the need for security enhancements.

If indicators of a breach are discovered, the risk assessment and the supporting documentation shall be fact specific and address:

- Assess the accuracy of the indicators discovered and the presence of a breach
- Consideration of who impermissibly used or to whom the information was impermissibly disclosed;
- The type and amount of data involved;
- The cause of the breach, and the entity responsible for the breach.

Discovery of Breach

A breach shall be treated as "discovered" as of the first day on which such a breach is known to United, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the organization's users, partners, or subcontractors). United shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or partner of the organization.

For an acquisition, access, use or disclosure of data to constitute a breach, it must constitute a violation of the data privacy policy. A use or disclosure of data that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper procedures would not be a violation of the Privacy Policy and would not qualify as a potential breach. The organization has the burden of proof for demonstrating that all notifications to appropriate users or that the use or disclosure did not constitute a breach.

Breach Investigation and Containment

Following the discovery of a potential breach, including unauthorized access to user data or unauthorized access to the technology stack, the organization shall:

- Apply containment measures immediately
- In conjunction, launch an investigation and risk assessment
- Begin the process to notify each user affected by the breach.
- Determine what external notifications are required or should be made.

The Incident Response Team, constituted by the IT Director shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others within or outside the organization as appropriate to contain, eradicate, and recover from the breach. They will identify other staff and departments within the organization who may need to participate in the investigation or its resulting response, including relationship managers and communication managers. They will also assess whether outside consultation with specialized expertise is required to complete the investigation, assess the breach, or provide the necessary security measures.

Incident prioritization is done by the IT Director. Prioritization is done on the basis of safety and security of users, confidentiality and integrity of user data, and impact on organizational function.

Timeliness of Notification

Upon discovery of a breach, notice shall be made to the affected United users no later than 72 hours after the discovery of the breach. Incidents will also be reported to relevant stakeholders, board members and to the relevant authorities.

Content of the Notice

The notice shall be written in plain language and must contain the following information:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- A description of the types of protected information that were involved in the breach, if known;
- Any steps the user should take to protect user data from potential harm resulting from the breach.
- A brief description of what we are doing to investigate the breach, to mitigate harm to individuals and users, and to protect against further breaches..

Methods of Notification

United Ship Chandlers users will be notified via email within the timeframe for reporting breaches as outlined above.

Maintenance of Breach Information Log

If any organizational or user data is compromised, the following information will be collected and logged for each breach:

- The current status of the incident
- A summary of the incident
- Indicators related to the incident
- Other incidents related to this incident
- Actions taken by all incident handlers on this incident
- Impact assessments related to the incident
- Contact information for other involved parties (e.g., system owners, system administrators)
- A list of evidence gathered during the incident investigation
- Comments from incident handlers
- Next steps to be taken

Recovery

The security team will determine the best course of action for recovery. These include restoring systems to normal operation, confirming that the systems are functioning normally, and remediating vulnerabilities to prevent similar incidents. Recovery may involve restoring systems from clean windows backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, or tightening network perimeter security

Post-Incident Activity

A thorough analysis of each breach incident and handling process will be conducted by the security team in conjunction with our leadership. Lessons learned will be shared with relevant staff and organizational departments, and used to build more robust security systems.