Security Policy

The Port of Stephenville firmly believes that implementing strong physical and cyber security measures is a pillar of our Management System and critical for the protection of people, environment, asset, and electronic data.

Physical Security

Top Management is committed to protecting physical security by:

- Collaborating with specialists to determine the risks associated with the areas we operate in and determining controls to minimize risk.
- Training our staff in their specific security-related duties including dedicated Marine Facility Officers.
- Conducting drills and exercises with seafarers to improve in competencies and readiness to respond to security-related events.
- Ensuring security is equipped with the required security equipment to proactively monitor and manage security risks.
- Developing and implementing internal vulnerability Transport Canada and reviewed at least annually.
- Establishing competent Marine Facility Officers to oversee security for the Port.

Cyber Security

Top Management is committed to protecting cyber security by:

- Conducting cyber-security risk assessments including:
  - Identifying critical infrastructures and the potential access points.
  - Determining the potential threat groups.
  - Identifying impacts if a breach shall occur.
  - Determining controls and protections.
  - Identifying measures to detect cyber-events and methods to respond and recover.
- Developing and implementing an IT and Cyber Security Plan. Ensure these documents are reviewed at least annually.
- Providing training to our employees and seafarers on expectations and requirements for cyber security.
- Conducting period drills and exercises to test competencies.

Personal Information and Electronic Documents

Top Management is commitment to protecting personal information and electronic documents by:

- Allocating a Privacy Officer to implement and maintain procedures and training. Developing privacy agreements, contracts, and reporting breaches.
- Informing personnel as to why personal information is being collected and obtaining appropriate consent.
- Ensuring information is accurate and is only being used as per the consent provided.
- Removing and destroying information once the retention period has expired.
- Safeguarding and limiting access to information to only authorized personnel who have a legitimate need to access the information.
- Allowing individuals access to their personal information, and to make corrections as appropriate.

Lonita Judge — July 1, 2023

Signature — Date

Rev 1

This policy shall be communicated and understood by all personnel including subcontractors, visitors, and stakeholders.