Scope:

This Policy applies to Ship and Shore staff working at all levels into Company, Contractors, Business partners or other Third Parties with a material interest in the operations of Elbana di Navigazione.

This Policy applies to IT equipment that is owned, operated, or leased by Elbana di Navigazione or registered under a Elbana di Navigazione owned internal network domain.

Purpose:

The purpose of this policy is to establish standards for the base security of internal server equipment, computers and networks that is owned and/or operated by Elbana di Navigazione.

Effective implementation of this policy will minimize unauthorized access to Elbana di Navigazione proprietary information and technology.

Overview:

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

Cyber Security Guidelines:

For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic.

All staff should be informed, why cyber security is important and what the potential risks are. If any data is lost or stolen, this could badly affect individuals involved, as well as severely jeopardize the Company. If the company systems are infected with malware, this could severely hamper the efficiency of the Company.

Minimum password requirement is a combination of lower case and upper case letters and numbers, store passwords carefully (no post-it on your monitor!), when sharing passwords use the phone instead of email.

Different kinds of phishing emails and scams should be described / presented to employees in order how to spot something 'fishy'. If employees receive an email that looks out of the ordinary, even if it looks like an internal email sent by another employee, they must check with the sender first before opening attachments. When in doubt, go to the company website instead of clicking on a link in an email. Scams can also be perpetrated over the phone, employees should be warned about people calling and asking for confidential company information.

All employees should be informed to update anti-malware programs, web browsers and other programs regularly and do full malware scans at least once a week.

When employees leave their desks, they must lock their screens or log out to prevent any unauthorized access. Laptops must also be physically locked when not in use.

When using portable devices such as mobile phones and laptops, passwords must be set to limit access. When bringing in portable media such as USB drives and DVDs, it is important to scan these for malware when connecting to the network.

All employees should be advised that stolen devices can be an entry point for attackers to gain access to confidential data and that employees must immediately report lost or stolen devices. IT department can take remote actions on devices.

Employees must use common sense and take an active role in security. If they see suspicious activity, they must report it to their IT administrator. If employees become aware of an error, even after it has happened, reporting it to IT means something can still be done to minimize the damage. Cyber security is

a matter that concerns everyone in the company, and each employee needs to take an active role in contributing to the Company's security.

For all employees, it is highly recommended to apply maximum privacy settings on their social media accounts such as Facebook, Twitter and Google+. They should make sure that only their contacts can see their personal information such as birth date, location, etc. By limiting the amount of personal information that is available online, the vulnerability to spear phishing attacks as well as identity theft can be reduced.

Monitoring:

Security-related events must be reported to IT department, who will review logs and report incidents to 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 data

Exceptions:

Any exception to the policy must be approved by IT team and Management in advance.

Non-Compliance:

An employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

Managing Director

Fabrizio Freschi