Scope

This Policy applies to Ship and Shore staff working at all levels as employed by the Company, Volunteers, Contractors, Business partners or other Third Parties with a material interest in the operations of Elbana di Navigazione and to whoever has permanent or temporary access to the systems and hardware owned, operated, or leased by Elbana di Navigazione or registered under Elbana di Navigazione.

Policy introduction and purpose

All staff, ashore and on board ships (the Employees), are 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 and the environment, as well as severely deteriorate the reputation of Elbana di Navigazione (The Company) and cause severe financial loss. If the Company systems are infected with malware, this could severely prevent the efficiency of the Company.

This company cyber security policy draws the guidelines and enforce provisions for protecting the Information and Operation Technology systems.

Nowadays we rely on technology to store and manage information and this makes us vulnerable to security breaches which may cause severe consequences. Human errors, hacker attacks and system malfunctions could cause damages to the human life, the environment and the property and finally causing severe financial loss and finally deteriorate our Company's reputation.

For this reason, the Company has developed and implemented a range of approved protective rules that everyone having access to Elbana di Navigazione technology and information assets must comply with.

The Company also prepared instructions that may help to mitigate cyber risks. We have outlined the provisions in this policy.

The main purpose of this Policy is to inform company users of their compulsory requirements for protecting the technology and information assets of the Company. The Cyber Security Policy holds Guidelines and Best Practice as drafted by the Company.

The Cyber Security Policy also draws the responsibilities of users. It clarifies legal use and rules governing the internet access. The Policy holds also procedures for responding to events that threaten the security computer systems and network.

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

Cyber Security Guidelines

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

Employees must use common sense and take an active role in security. If they see suspicious activity, they must report it to their Company Cyber Security Officer /IT administrator. If employees become aware of an error, even after it has happened, reporting it to Company Cyber Security Officer/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, ashore and on board, 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. 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.

Awareness

All employees should be aware 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. Awareness training for all the shore staff and crews is arranged by the Company.

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

Email

Different kinds of phishing emails and scams are described/presented to employees in order to be able 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.

Emails often host scams and worms. To avoid virus infection or stealing data, the employees are instructed to:

- Avoid opening attachments and clicking on links when the content is not clear or satisfactorily explained (e.g. "watch this, this is amazing.")
- Be suspicious of what appears as a bait (e.g. discounted prizes, important notice.)
- Check email and names of senders to ensure they are genuine.
- Look for inconsistencies or gift.

Password

Weak passwords are dangerous because they can allow unauthorized and malicious entry into our infrastructure and compromise it. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, the employees are instructed to:

- Minimum password requirement is a combination of lower case and upper case letters and numbers and avoid information that can be easily guessed (e.g. own name, birthdays.)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done. If necessary store passwords carefully (no post-it on your monitor!), when sharing passwords use the phone and avoid absolutely email.
- Give credentials only if absolutely necessary. When giving person-to-person is not possible, employees must use the phone and not email, and only if they personally recognize the person they are giving the credentials.
- Change their passwords every two months.

Leaving the desk

When employees ashore 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 and any paper, if any, kept close to the keyboard or any other unprotected place on or around the desk on which are noted passwords and/or any credential must be removed. Procedures for "locking the screen" after 5 min idle time should be enforced.

On board the ships the crew members must follow and implement strictly the provisions of the Ship Security Plan addressed to the visitors who will never left alone. Any maintenance performed by shore technicians (visitors) will be monitored closely and accurate checks will be carried out upon completion and prior the visitors leave the ship.

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.

Company Cyber Security Officer/IT department can take remote actions on devices.

Laptops must also be physically locked when not in use and any paper, if any, kept close to the keyboard or any other unprotected place on or around the desk, on which are noted passwords and/or any credential must be removed.
A domain policy, or local policy for PC not domain joined, must be enabled to enforce lock screen after 5 min idle time.

Confidential data

Confidential data are secret and valuable. All employees must protect these data:

- Financial information
- Data of charterers/brokers/partners/vendors
- Ship's data (administrative and technical)
- Data of crew members
- New technologies

Protection of personal and company devices

When employees use their digital devices to access Company emails or accounts, they introduce security risk to the Company data. All the employees must keep both their personal and Company-computer, tablet and cell phone secure doing the following:

- Making sure the antivirus software is kept up-grated.
- Keeping all devices protected by password renewed every two months.
- Following the IT instructions for security updates of browsers and systems.
- Logging into Company accounts and systems through secure networks only.
- Making sure not to leave any device exposed or unattended.

The employees are also instructed to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new employees receive Company-owned equipment they will receive instructions for:

- Disk encryption setup
- Password management
- Installation of antivirus/ anti-malware software

For any problem they must refer to the Company Cyber Security Officer/IT to whom address also any question.

Transferring data

Transferring data involves security risk. Employees must:

- Avoid transferring sensitive data to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed then the Company Cyber Security Officer/IT assistance must be requested.
- Share confidential data using the Company network/system and not over public Wi-Fi or private connection (hotel, airport etc).
- Make sure that the recipients of the data are properly authorized people or organizations.
- Report scams, privacy breaches and hacking attempts

Company Cyber Security Officer/IT needs to know about scams, breaches and malware so he can better protect our infrastructure. This is why the employees must report suspected attacks, suspicious emails or phishing attempts as soon as possible. The Company Cyber Security Officer/IT then must investigate immediately, resolve the issue and when necessary send an alert over the entire Company.

Company IT is responsible for training employees on how to detect scam emails. He will be ready to answer any question on the matter.

Additional measures

To reduce the likelihood of security breaches, the employees are also instructed to:

- Refrain from downloading suspicious, unauthorized or illegal software on their Company PC
- If/when a device is stolen change immediately the passwords of all the accounts.
- Report to the IT as soon as possible stolen or damaged equipment.
- Avoid accessing suspicious websites
- Report an observed threat or possible security weakness in Company systems.

Company Cyber Security Officer/IT **should:**

- Complying with this policy.
- Install firewalls, anti-malware software and access authentication systems.
- Issuing regularly information about new scam emails or viruses and ways to respond.
- Arrange for cyber security training to all employees as per DPA and CSO instructions.
- Being part of the team investigating cyber security breaches .

The Company overall effort is to protect its assets, the human life at sea and the environment.

Remote employees

Remote employees must follow this policy's instructions too. Since they will be accessing the Company's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

The Company encourages them to contact the Company Cyber Security Officer/IT for seeking advice from him.

Take security seriously

Everyone, from Company customers and partners to the employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Managing Director

Fabrizio Freschi