

## POLICY WITH REGARDS TO THE USE OF INFORMATION TECHNOLOGY

The use of the Company's information technology must be legal and consistent with the Company's reputation, standards, and rules of conduct that require regulations and productivity expectations. As such, all employees and other individuals who use the Company's information technology should:

- Prevent unauthorized access to the technology and its tools
- Lock work stations when absent
- Secure the following equipment at all times to avoid theft and information leakage: laptops, portable computers, and similar devices
- Use passwords that are hard to guess and comply with the conditions required to obtain a password
- Keep their passwords confidential. Under no circumstances reveal their passwords to a third party
- Change their passwords regularly
- Protect information that is considered confidential and reveal it only if approved by an authorized person
- Comply with confidentiality and information disclosure policies
- Not violate a third party's intellectual property, privacy or other rights
- Not use the Company's information technology to undertake any commercial or other activity that is not directly related to it
- Minimize the use of the Company's electronic equipment for personal reasons
- Avoid as much as possible downloading and transferring files unrelated to their job on-site or in the field
- Comply with the laws and regulations in effect and avoid using the Company's electronic equipment for illegal or inappropriate activities, such as hacking or sending junk mail
- Avoid deactivating the safeguards installed by the Company, such as firewalls or antivirus software

- Make sure all the software they install and use is legally licensed in Stornoway's name

### ▼ ELECTRONIC MESSAGES

All employees and other individuals who use the Company's email addresses should at all times write polite, precise and respectful messages. They should also:

- Identify themselves
- Make sure their personal opinions cannot be interpreted as belonging to the Company
- Refrain from using the Company logo in their signature when sending a personal email
- Refrain from sending offensive, slanderous or inappropriate emails
- Refrain from viewing, downloading, saving or sharing sites with pornographic, racist or inappropriate content
- Inform the IT department if they receive information from the Internet with content that goes against elementary rules of good taste, courtesy, and professionalism, and immediately cease all communication with the sender
- Immediately inform the Company's IT department of any virus present

### ▼ ELECTRONIC COMMUNICATIONS STANDARDS

- a) Avoid voicing an opinion in the Company's name or opinions that can be interpreted as belonging to the Company.
- b) Avoid revealing confidential information that can tarnish the Company's reputation.
- c) Avoid posting pictures of personnel, facilities, equipment, locations, routes, maps, and any other elements that can go against the Company's confidentiality policy.
- d) Avoid at all times the use of discriminating, hateful, and inappropriate language.

## POLICY WITH REGARDS TO THE USE OF INFORMATION TECHNOLOGY

### AUDITS AND SUPERVISION

The Company and its representatives reserve the right to monitor, record, access, use, and disclose information regarding an employee's use of the Company's technology if deemed necessary to ensure compliance with the Company's policies or for any other legitimate commercial reason, during or after the employee's term of employment or that of any person authorized to use the Company's information technology. The Company can access, save, and archive an employee's emails (including those sent and received with Web based systems like Hotmail) and voice messages, the documents they posted on the Company's systems as well as the list of Web sites they visited. The Company can also monitor the employee's use of the telephone, security card, photocopier, and Internet.