POLICY

POLICY: **A-7**
SUBJECT: **COMPUTER USE**
EFFECTIVE: **JANUARY 1, 2022**
SUPERCEDES: **APRIL 7, 2014**

POLICY

This policy outlines the acceptable use of company information and information technology and is intended to protect the Company's information technology resources against illegal and/or damaging actions by system users, either knowingly or unknowingly. This policy applies to all information owned or possessed by the Company, all information technology owned or leased by the Company, and all crew members of the Company.

The Company's information technology resources must be used ethically, respectfully, and lawfully, in accordance with the Company's policies and applicable federal and provincial laws.

Crew members utilizing company workstations, including network, wireless and remote access, are responsible for their actions and activities. Personal use of such company information technology resources must be appropriate, lawful and in keeping with the intent of this policy. The Company reserves the right to change, limit, suspend or prohibit access to these information technology resources where necessary.

1.0 OWNERSHIP

1.1 Access to the Company's information technology resources is conditional upon user agreement to abide by this policy and acknowledge responsibility for the material created, accessed, displayed, stored, printed, sent, or made available to others.

1.2 Company information technology, including but not limited to computer equipment, software, operating systems, storage media and network accounts, are intended for business use.

1.3 All information, including but not limited to personal information and email messages created or stored on company information technology resources, including back-ups, are company property.

2.0 CONFIDENTIALITY AND PRIVACY

2.1 The Company's computers, networks, internet services and other electronic devices remain under the control, custody, and supervision of the company at all times and the company reserves the right to monitor all computer and Internet activity by crew members and other system users. Crew members and other system users should maintain no expectation of privacy in their use of company information technology resources, including email messages, stored files, and the internet.

2.2 The Company monitors information technology usage, including intercepting and reviewing personal and business communications for the following purposes:

- Troubleshooting hardware and software problems
- Preventing unauthorized access and system misuse
- Retrieving business-related information
- Investigating possible violation of company policy, local/provincial/federal law
- Complying with legal/regulatory requirements
- Re-routing or disposing of undeliverable mail
- Performing information technology administration
- Providing information for crew member conduct reviews

3.0 ACCOUNT, PASSWORD AND WORKSTATION SECURITY

3.1 Crew members are responsible for keeping the confidentiality of their accounts and passwords, and for all activities performed with/on their accounts. All passwords must be promptly changed if they are suspected of being disclosed or known to have been disclosed.

3.2 Company computer workstations must never be left unattended while users are logged in. Users must log out, lock the workstation or invoke password protected screen saver before leaving a workstation unattended. Gaining access to, intercepting, interrupting or using, for any reason, any company

information technology resource or account for which a crew member has not been authorized is strictly prohibited.

3.3 Crew members must take reasonable precautions to protect and secure laptops, notebooks, tablets, smartphones, removable storage media and other portable computer equipment, especially those containing confidential or restricted information.

4.0 E-MAIL, INTERNET AND SOCIAL NETWORKING

4.1 When using company information technology resources, examples of unacceptable/prohibited uses/actions include, but are not limited to, the following:

- Posting, transmitting or distributing information that constitutes or encourages a criminal offense or civil liability
- Using company information technology to restrict or inhibit any other authorized user from using the information technology, in whole or in part
- Posting or transmitting messages constituting "spam", including unsolicited email messages, mail bombing or any other abuse of email
- Posting or transmitting any information or software containing a virus, "Trojan horse", "worm" or other harmful or disruptive component
- Creating, using, possessing or providing access to software or other material that is: (i) confidential or is protected by copyright or other intellectual property rights, without prior authorization from the rights holder(s); (ii) defamatory, obscene, sexually explicit, pornographic, hate literature or otherwise illegal; or (iii) an invasion of privacy, appropriation of personality or unauthorized linking or framing. The company reserves the right to refuse or to remove any such information, software or material from its information technology resources
- Private business activities, amusement or entertainment purposes, or to distribute hoaxes, chain letters or personal or private advertisements.
- Email messages concerning non-company business must not be sent, forwarded or replied to using excessively large email distribution lists
- Using information technology resources in such a way to be considered harassment, or which may contribute to a hostile work environment, as defined by company policy A-4

- Misrepresenting, obscuring, suppressing or replacing one's identity in/on email communications
- Misrepresenting oneself as a representative of the company while participating in discussion groups, chat rooms, social networking and/or other public internet forums, unless such communications are done for the express purpose of discharging job requirements and are authorized by a director or above
- Use of streaming audio/video sites for non-business-related activities

4.2 Incidental personal use of company information technology resources is permissible if it:

- Occurs outside a crew member's work schedule
- Does not consume more than a trivial amount of time and/or resources
- Does not interfere with a crew member's productivity or with work being performed by another crew member
- Does not pre-empt any business activity
- Is not for pay or profit
- Does not violate software licensing agreements
- Does not expose company information technology resources to security risks
- Complies with the restricted use provisions of this policy

5.0 VIRUS PROTECTION

5.1 Crew members must minimize the risk of damage from virus programs and their propagation through attention to anti-virus warnings and ensure that all external storage devices and email are from a trusted source. If a crew member becomes aware of a virus program on a workstation, the crew member should not attempt to delete the virus or continue to use the affected workstation. Contact the Director of IT immediately.

5.2 If a crew member becomes aware of a virus warning or if a virus warning is mailed to the crew member, forward the warning to the Director of IT immediately.

6.0 SOFTWARE

6.1 Only crew members who are authorized by the nature of their job functions in software maintenance and support, software research and evaluation are permitted to add, change, remove or copy software from company information technology resources. Loading of unauthorized or unlicensed software onto company information technology resources is otherwise prohibited.

6.2 Shareware, freeware or any public domain programs are prohibited on company information technology resources unless authorized in advance by IT.

7.0 CONSEQUENCES FOR VIOLATION OF POLICY AND RULES

7.1 Failure to comply with this policy and/or other procedures or rules governing company information and information technology resources may result in progressive discipline, up to and including employment separation. Crew members using company information technology resources for illegal, defamatory or fraudulent purposes are also subject to criminal and/or civil liability.

Further interpretation of this policy is the responsibility of the Vice President, Employee & Guest Experience. The Company reserves the right to make, modify, revoke, suspend, terminate, or change any policy or procedure, in whole or in part, at any time.