CRAGGY RANGE
VINEYARDS LTD

Policy Name:	Information Systems Acceptable Use Policy		Department:	Human Resources	
Policy Owner:	Human Resources		Approved By:	Chief Executive Officer	
Creation Date:	August 2016	Review Date:	August 2018	Version Number:	1

1. Purpose

1.1. The purpose of this policy is to outline the acceptable use of Craggy Range systems. These rules are in place to protect the employee and Craggy Range.

1.2. Inappropriate use exposes Craggy Range to risks including virus attacks, compromised network systems and services, and legal issues.

2. Scope

2.1 This policy applies to employees, licensees, contractors, consultants, temporaries, and other employees at Craggy Range, including all personnel affiliated with third parties. This policy applies to all Craggy Range supplied or supported devices that are owned, leased or operated by Craggy Range and other equipment that is granted access to Craggy Range systems.

3. Definitions

LAN	Local Area Network (LAN) is a network that connects computers and other devices in a relatively small area, typically a single building or a group of buildings. Most LAN's connect workstations and personal computers and enable users to access data and devices (e.g. printers and modems) anywhere on the network.
WAN	Wide Area Network (WAN) is a telecommunications network or computer network that extends over a large geographical distance. Wide area networks are often established with leased communication circuits.
Internet	A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardised communication protocols.
Intranet	A local or restricted communications network, especially a private network created using World Wide Web software.
Extranet	An intranet that can be partially access by authorised outside users, enabling businesses to exchange information over the Internet in a secure way.
Device	A thing made or adapted for a particular purpose, especially a piece of mechanical or electronic equipment.

4. Policy

4.1 General Use and Ownership

4.11 While Craggy Range 's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on company systems remains the property of Craggy Range. Because of the need to protect Craggy Range 's network, management cannot guarantee the confidentiality of information stored on any device belonging to Craggy Range.

Policy Name:	Information Systems Acceptable Use Policy		Department:	Human Resources	
Policy Owner:	Human Resources		Approved By:	Chief Executive Officer	
Creation Date:	August 2016	Review Date:	August 2018	Version Number:	1

4.12 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of any other policies or any uncertainty, employees should consult their supervisor or manager.

4.13 For security and network maintenance purposes, authorised individuals within Craggy Range may monitor devices, systems, network traffic, data usage and types of calls, messaging, websites, application and data at any time.

4.14 Craggy Range reserves the right to audit networks and systems on a periodic basis to ensure compliance.

4.2 Security and Proprietary Information

4.2.1 Employees should take all necessary steps to prevent unauthorised access to company confidential information.

4.2.2 Keep passwords secure and do not share user accounts. Authorised users are responsible for the security of their passwords and user accounts. User level passwords may be changed every 60 days.

4.2.3 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the device is left unattended.

4.2.4 Because information contained on portable devices is especially vulnerable, special care should be exercised. Power-on passwords should be applied to all portable devices.

4.2.5 All devices, including laptops, desktops, servers and mobile devices used by the employee that are connected to the Craggy Range LAN/WAN/Intranet/Extranet, whether owned by the employee or Craggy Range, shall be continually executing approved virus-scanning software with a current virus definitions.

4.2.6 Employees must use extreme caution when opening email attachments or following links embedded within email received from unknown senders, as these may pose serious security threats to company systems.

4.3 Internet

4.3.1 Software for browsing the Internet is provided to authorised users for business and research use only.

4.3.2 All software used to access the Internet must be part of the Craggy Range standard software suite or approved by Craggy Range management. This software must incorporate all vendor provided security patches.

4.3.3 All files downloaded from the Internet must be scanned for viruses using the approved Craggy Range virus detection software.

4.3.4 Incidental use:

- Incidental personal use of Internet access is restricted to Craggy Range approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to Craggy Range.
- Where direct costs are incurred as a result of incidental use, the employee issued with the device will be expected to reimburse these amounts.

Policy Name:	Information Systems Acceptable Use Policy		Department:	Human Resources	
Policy Owner:	Human Resources		Approved By:	Chief Executive Officer	
Creation Date:	August 2016	Review Date:	August 2018	Version Number:	1

- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to Craggy Range.
- All files and documents – including personal files and documents – are owned by Craggy Range, may be subject to open records requests, and may be accessed in accordance with this policy. Incidental use must not result in performance degradation of the Craggy Range network(s).

4.4 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Craggy Range authorised to engage in any activity that is illegal under New Zealand or international law while utilising Craggy Range's systems.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4.1 Hardware Care and Maintenance

The equipment provided by Craggy Range to employees at all times remains the property of Craggy Range. This equipment must not be misused or damaged through negligence.

Where evidence of gross negligence is found, in some circumstances the employee responsible for the equipment may be asked to contribute towards the cost of repair or replacement.

4.4.2 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Craggy Range.
2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Craggy Range or the end user does not have an active license is strictly prohibited.
3. Introduction of malicious programs onto the network (e.g. viruses, worms, Trojan horses, email bombs, etc.).

4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using a Craggy Range computing asset to actively engage in procuring or transmitting material that is sexually explicit in nature.
6. Accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access.
7. Port scanning or security scanning.
8. Executing any form of network monitoring which will intercept data not intended for the employee, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network or account.
10. Providing information about, or lists of, Craggy Range employees to parties outside Craggy Range.

4.4.3 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Downloading, saving and transmission of explicit and/or implied pornographic video clips, text or still pictures, and any other similar matter.
3. Excessive transmission/receipt of personal emails.
4. Sending messages in the name of a co-worker and/or from the personal computer of a co-worker without that person's knowledge or permission.
5. Messages that are unethical or may cause offense, breach any law including human rights, criminal or privacy legislation and break of any confidentiality obligations or the Code of Conduct.
6. Any form of harassment via email, telephone, the Internet, or electronic messaging, whether through language, frequency, or size of messages.
7. Unauthorised use, or forging, of email header information.
8. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
9. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
10. Use of unsolicited email originating from within Craggy Range's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Craggy Range or connected via Craggy Range's network.

4.4.4 Application

Any employee found to have breached this policy may be subject to disciplinary action, up to and including termination of employment.