Acceptable Use of Information Assets Policy

The information systems, communications systems and/or information technology resources provided by Heritage Resource Limited Partnership ("Heritage Royalty" or the "Company") are property of the Company and are intended to be used in a manner consistent with the Company's business and Code of Ethics and Business Conduct. Users are responsible for the appropriate, ethical, and lawful use of the Company's Information Assets.

This policy defines the boundaries for acceptable use of the Company's Information Assets to minimize the Company's exposure to electronic security risks and ensure compliance with applicable laws and regulations.

The Company's Information Assets are business-critical items that must be protected from accidental or intentional damage and/or loss. The security and integrity of these Information Assets is largely dependent upon each User's use of the same in a manner consistent with this Policy, any related policies of the Company and the Company's Code of Ethics and Business Conduct.

Each User must ensure that their use of any information systems, communications systems and/or information technology resources is done in an appropriate, responsible and ethical manner. A glossary of specific terms is provided at the end of this document.

This Policy will be reviewed annually by the Company's Advisory Board and updated as required.

PURPOSE

Information Assets and Technologies are powerful tools for accessing and distributing information and knowledge. The purpose of this policy is to promote the ethical and responsible use of the Company's Information Assets to minimize potential privacy, security, and litigation risks to the Company resulting from the unacceptable use of these Assets and to make Users aware that they bear the primary responsibility for any unlawful or unacceptable use.

The key objectives of this policy are to:

- Define the principles and requirements of acceptable use and describe how these will be implemented across the Company;
- Ensure each User is aware of the Company's expectations and requirements for acceptable use of Information Assets and each User's role in protecting the security and integrity of the same;
- Create a level of awareness that Information Assets are critical items and that the security and integrity of the same are necessary for the Company's day to day business; and
- Create a framework and control environment where the Company, with each User's cooperation, can ensure protection of Information Assets, effectively manage the risks of misuse and protect the Company's reputation and public image.

This policy applies to all Users (including employees, volunteers, contractors, etc.) who create, access or use any of the Company's Information Assets, technologies and electronic environment(s). This policy also applies to any personally-owned devices that are connected to the Company's networks.

DEFINITIONS

For purposes of this Policy:

A. "**Communication Systems**" The systems for transmitting data between persons and equipment often over a distance in the form of sound, text, or video. Communication Systems consist of physical and virtual devices, data cable, fibre, voice devices, (phones, speakers), video streams and monitors, as well as the telecommunication system itself.

B. "**Information Systems**" The infrastructure, processes, and technologies used to store, generate, manipulate, and transmit information to support the Company, also referred to as information services or information technology.

C. "**Information Technology Resources**" or **"IT"** All IT hardware, software, facilities, applications, and networks that are owned by, in the custody of, and operated or managed by the Company.

D. "**User"** Employee, officer, director, contractor, or third party having been granted access to the Company's Computing Environment.

A full glossary of terms is included as an Appendix of this Policy.

RESPONSIBILITY

Access to IT Assets and Services

User access and use of the Information Assets must be primarily for the purpose of conducting work and services for the benefit of the Company. Reasonable personal, non-commercial use of the Computing Environment is permitted provided that such use:

- Is otherwise consistent with the Company's policies;
- Does not unduly interfere with the User's work and services for the benefit of the Company;
- Does not expose the Company to additional risk (reputational, legal, or otherwise) or material cost; and
- Does not make use of any information owned or licensed by the Company.

Unacceptable uses include but are not limited to:

- Using or accessing any Information Assets contrary to the User's permissions or authorizations;
- Revealing passwords to others or allowing use of the User's account by others;
- Acquiring and/or making use of another User's password;
- Using any Information Assets for any purposes or activities in poor taste or contrary to applicable law;
- Making offers of products, items, or services (fraudulent or otherwise) originating from any Company account;
- Causing or contributing to a security breach or disruption of network communication, including introducing a virus into the Company's network;
- Maliciously accessing or intercepting information for which the User is not an intended recipient;
- Except for IT staff, monitoring of data, electronic data traffic, or network communications by any means;
- Port scanning or security scanning of any kind;
- Circumventing User authentication or security controls;
- Using any program, script, command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means;

- The use of unauthorized computing devices in the Computing Environment; and
- Posting or distributing confidential, proprietary, or other sensitive Company information outside of the Company for non-business purposes.

Privacy and Personal Information

The privacy and content of Personal Information will be protected in accordance with the Company's policies and applicable legislation. Each User must exercise good judgment regarding the content and nature of personal information he/she introduces into the Computing Environment.

All personal information and messages introduced into the Computing Environment will be treated in a similar manner as business-related information and messages and their content and use must be consistent with Company policies. The Company reserves the right to examine personal electronic communications and information retained on Company Information Assets and networks in accordance with application laws.

Passwords

Each User will abide by the Company's Password Policy as outlined in the Company's IT Procedures and Practices and enforced by the Company's IT services provider when setting up accounts.

Third Party Intellectual Property

Only software approved by IT in advance may be introduced into the Computing Environment. Information, software, programs, and other electronic products or applications available to Users may be the intellectual property of a third party and such items may be subject to intellectual property rights and restrictions (e.g. copyrights, patents, trademarks, license agreements, etc.) that govern their access, distribution, or use.

The following activities are specifically prohibited:

- Violation of the intellectual property rights of any third party by any means, including, but not limited to, the use, installation, or distribution of pirated software or other products or applications that are not properly licensed for use;
- Unauthorized copying, representation, or use of copyrighted or trademarked material; and
- Use or modification of patented items, processes, or designs without the expressed permission of the patent holder.

The misuse of third party intellectual property may expose the User and the Company to legal action. Any questions concerning the access, distribution, or use of third party information, software, programs, and other electronic products or applications should be referred to IT or legal services prior to use.

Email

Each User must ensure that use of their Company email account is appropriate and otherwise consistent with this Policy. Unacceptable uses of email include, but not limited to:

- Opening unsolicited email attachments without prior scanning;
- Using personal email addresses for Company business purposes;
- Sending unsolicited email messages, including the sending of junk mail or other advertising material;
- Sending inappropriate email messages that feature adult, offensive, or other material in poor taste;

- Unauthorized use or forging of email header information;
- Any form of harassment via email including solicitation of email from any other email address, with the intent to harass or to collect replies;
- Sending email messages internally or externally that contain unencrypted, sensitive corporate information. If any doubt exists, Users should consult with their supervisor or IT; and
- Any activity associated with phishing or emails designed to collect personal information (name, account numbers, Usernames, passwords, etc.) under false pretense.

Voicemail

Unacceptable uses of voicemail shall be prevented including, but not limited to:

- Sharing of voicemail boxes without proper IT authorization;
- Creating voicemail boxes without password protection; and
- Voicemail greetings or messages with inappropriate content or language.

Instant Communication

Only Instant Messaging (IM) tools that have been made available or approved in advance by IT may be used to conduct Company business and/or loaded on Company Information Assets. Any such IM tool must have appropriate security.

Internet and Social Media

Any online social media activities (including but not limited to newsgroups, online forums, bulletin boards, and social networking sites like Facebook, LinkedIn, etc.) using the Company's hardware or network must be consistent with this policy as well as the Code of Ethics and Business Conduct and related policies.

Unacceptable online social media activities include but are not limited to:

- Disseminating, viewing, downloading, storing, or forwarding adult, pornographic, obscene, offensive, or other material in poor taste;
- Harassment or any form of discrimination;
- Discussion or disclosure of confidential, proprietary, or other sensitive Company information;
- Discussion or disclosure of any internal Company matter that could be damaging to the Company or beneficial to the Company's competitors; and
- Use of the Company logo, brand, or trademarks or posting non-Company sponsored videos, media clips or images that reference the Company.

Cloud Storage and Services

In respect of any Company Information, any use or access to cloud or personal network storage/backup (e.g. Dropbox, Microsoft OneDrive, Google Drive, Apple iCloud, etc.) must be with the prior expressed permission of IT.

File Sharing

In respect of any Company information, any use or access to file sharing platforms (e.g. Virtual Data Rooms, etc.) must be with the prior express permission of IT.

Removable Media

In respect of the storage or transmittal of any Company information, any use of Removable Media

must be approved by a company supervisor and the approach/media must be approved with prior express permission by IT.

Remote Access

Remote access to the Company's Computing Environment will be provided by IT only to authorized Users. Users must utilize an IT approved connection (VPN, Citrix, etc.) when accessing the Computing Environment from offsite locations. Users must take reasonable precautions to safeguard access to the Company's information and network while using remote access.

Business Applications and Software

All use of business applications and software must be consistent with this policy and any specific rules defined by the business. All business applications and software must:

- Have a clear business purpose;
- Have been approved for use by IT consistent with the Company's computing environment;
- Have been scanned for viruses;
- Be compatible with the Company's technology and security infrastructure; and
- Be properly licensed and issued in accordance with the distributor's software license (which itself has been approved by IT in advance).

Information stored within the business application is considered and will be treated as proprietary Company information.

Mobile Devices

Each User must employ reasonable security measures to protect the security and integrity of his/her Mobile Device where such device contains Company information or could be used to access the Company's network or information. Such measures include but are not limited to password protection, encryption and physical control in accordance with the company policies.

Personal Mobile Devices

Users may use Personal Mobile Devices for Company business purposes provided that prior express approval from IT is obtained before any such device is used to access the Company's Computing Environment. IT will maintain a list of approved Personal Mobile Devices and related software applications and utilities. Users must read and acknowledge the Company's Bring Your Own Device Agreement before connecting their personal devices to any Company network.

Lost, Stolen or Damaged Devices

In respect of a Corporate Mobile Device or Personal Mobile Device where such device contains Company information or could be used to access the Company's network or information, Users must immediately report to their supervisor and IT:

- The loss or theft of such device or the device's access password or PIN;
- Any incident (real or suspected) to hack or otherwise gain control of such device or access information; and
- Any significant damage to or malfunction of such device.

As determined by IT, appropriate measures will be taken to erase all Company data from any lost, stolen, or compromised Mobile Device and lock the device to prevent access by anyone other than IT. In many circumstances, personal and Company information may be indistinguishable or such

measures may otherwise result in the loss of personal information, files, pictures, etc. from the affected device. As such, Users are encouraged to remove or back up such personal information regularly.

User Accountability

Any real or perceived security breach or misuse in relation to Information Assets contrary to this policy will be reviewed or investigated and the User may be subject to disciplinary action (up to and including termination of employment or contract) and/or legal action. It is important for each User to understand and accept their personal responsibility to ensure the security and integrity of the Company's Information Assets and the potential severe consequences of misuse, loss and breach of security and confidentiality.

Each User will be required to review and acknowledge this Policy prior to using or gaining access to the Company's Information Assets and Computing Environment and periodically thereafter as determined by the Company.

GOVERNANCE

It is essential that all representatives understand and be responsible for abiding by and implementing this Policy.

Users, upon logon to any of the Company's information systems, communications systems, and/or information technology resources, agree to abide by this Policy.

The Company has the right to monitor, record, and audit the use of the Company's Information Assets including any information systems, communications systems and/or information technology resources. If there is probable or reasonable cause to suspect illegal or unacceptable conduct, the Company may undertake monitoring, recording, and auditing of the suspected User's information systems, communications systems, and/or information technology resources.

Any violation of this Policy will result in discipline by the Company. If any representative misuses Information Assets, it will be considered a serious offence for which appropriate disciplinary action may be taken, up to and including termination of employment or service agreement, or court action. This Policy includes examples but is not intended to be restricted in its application to such examples, therefore where the word "including" is used, it shall mean "including without limitation".

Approved by the Advisory Board of Directors, December 2019. Effective January 2020.

APPENDIX 1: GLOSSARY OF TERMS

Company	Heritage Resource Limited Partnership and its affiliates and subsidiaries from time to time.
Computing Environment	Company's interconnected IT assets including but not limited to hardware (computing devices, Mobile Devices, etc.), databases, operating systems, servers, networks and applications capable of processing, storing and sharing information.
Employee	A director, officer, employee, contractor or consultant providing work, advice or service for the benefit of the Company.
Encryption	The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
Information Asset	Company owned, controlled or licensed information, software, network, system or hardware.
IT	Information Technology Services group within the Company.
Mobile Device	Any mobile hardware device (and related software) capable of storing data and connecting to a Company network including but not limited to: Smartphones; Other mobile/cellular phones; Tablet computers; and Portable media devices.
Password	A unique, User-defined string of characters used to validate a User's identity in order to gain access to the applicable program, system, network…etc.
Pirated	Software which has been duplicated and/or distributed illegally without proper permission from the owner.
Port Scanning	Surveillance of computer ports (often by hackers with malicious intent) to locate weaknesses within specific computer ports.
Removable Media	Any type of storage device capable of storing and transporting electronic information between computers. Examples include but are not limited to: Portable Universal Serial Bus-based ("USB") memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives; Memory cards in secure digital ("SD"), CompactFlash, Memory Stick, or any related flash-based supplemental storage media; External hard drives; USB card readers that allow connectivity to a personal computer; Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support a data storage function; Personal digital assistant ("PDAs"), cell phone handsets, and smartphones with internal flash or hard drive-based memory that support a data storage function; Removable memory-based media, such as rewritable DVDs and CDs; and Any hardware that provides connectivity to USB devices through wireless ((Wi-Fi,

	WiMAX, IrDA, Bluetooth…etc.) or wired network access.
Security Breach	A successful attempt by a malicious party to access or control the Computing Environment.
Spam	Unauthorized and/or unsolicited electronic mailings.
User	Employee, officer, director, contractor, or third party having been granted access to the Computing Environment.
Virus	A malicious software program capable of reproducing itself and which may cause harm to files or other programs on the same computer or network and includes but is not limited to viruses, worms, Trojan horses, phishing programs and email bombs.
VPN	Virtual Private Network. A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.