Information Security Risk Policy

1. PURPOSE

This document sets forth The Real Brokerage Inc.'s ("Company") Information Security Risk Policy ("Policy"), designed to ensure that an effective Information Security Program ("Program") is in place to monitor and manage risks impacting the Company's information assets.

The purpose of the Policy is to establish the appropriate guidelines to ensure users and networks within an organization meet the Company's Information Technology ("IT") security and data protection security requirements. The Policy will define the guidelines for:

- Acceptable use of information systems at the Company
- The Company's information security usage and access standards to protect the Company and its employees

The Policy provides general principles to guide the Program's processes; documenting the Company's acceptable processes for avoiding and effectively mitigating information security risk.

2. OBJECTIVES

The Policy formalizes the Company's objectives to measure, monitor, and manage information security risk within the Company's IT processes. The primary objectives of the Policy are to:

- Document information security measures
- Protect information from unauthorized access and misuse
- Protect information from unauthorized alteration
- Ensure timely and uninterrupted access to the Company's information assets and systems

The Program will be managed to:

- Prevent and detect information security incidents
- Comply with legal and regulatory requirements related to information security
- Limit access to key information technology assets and information generated

3. SCOPE

The Policy is applicable to all workers, employees, contractors, consultants, and temporary employees at the Company and subsidiaries owned or controlled by the Company, including:

- Real Technology Broker Ltd.
- Real Pipe LLC
- Real Broker MA, LLC
- Real Broker NY, LLC

- Real Broker CT, LLC
- Real Broker, LLC
- Real Brokerage Technologies Inc.
- Real Broker Commercial, LLC
- Real Title, LLC
- Real Broker AB LTD
- Real Broker Ontario, LTD
- Real Broker BC LTD
- Real Broker AZ, LLC
- Real Broker LFRO, LLC

This policy applies to all information equipment and assets that are owned or leased by the Company and other information equipment that may be used to access the Company systems.

Supplemental guidelines may be created for specific systems that require users to comply with rules beyond those contained in this document. System owners must document any additional system-specific guidelines.

This Policy applies to local, network, and remote use of Company information (in both electronic and physical forms) and information systems by any individual.

3.1 Risk Appetite

The Company will accept low information security risk exposure. The Company's risk tolerance will be conservative in the support of achieving organizational objectives and adhere to the guidelines identified within this Policy.

The Company is a technology powered real estate brokerage firm exposed to information security and data risk, among others addressed in the Company's other policies and procedures. The Company has developed and implemented control procedures and objectives to mitigate the inherent risk exposure relevant to the Company's business model, to an acceptable residual risk level. The Company will continuously monitor information security risk exposure against current risk level tolerances to ensure the Company has not exceeded its conservative risk appetite.

4. PROTECTION AND SECURITY

4.1 Electronic Communication

Users are to use electronic communications systems primarily for business-related purposes and authorized access to Company systems and data.

The Policy applies to electronic communication resources, including, but not limited to the Company's network, computers, workstations, software, hardware, Internet/Intranet,

electronic messaging systems (e-mail), fax machines, tablets devices, voice mail, telephones, pagers, and cellular phones.

4.1.1 Right to Access/Privacy

Electronic information resources, telephonic communication systems, and all data residing therein belong to Company and may be viewed or accessed at any time without consent or knowledge of the sender or receiver.

Limited non-business use of Company's electronic information resources and telephonic communication systems is permitted and explained in the Company's Information Systems and Assets Acceptable Use Policy .

The Company reserves the right to monitor, access, and review any aspects of its electronic information resources and telephonic communication systems. The Company has installed mobile device management software on all Company issued laptops to facilitate data monitoring and security.

4.1.2 Access to Internet and E-mail

Each user of Company electronic communications systems is personally responsible for taking reasonable steps to use the resources responsibly and securely, and prevent unauthorized use of their Internet and Company e-mail accounts.

Each user of Company's electronic communications systems must:

- Access the Internet in a way that protects the Company from any legal, regulatory, operational, or reputational risk
- Not share access to their Internet account
- Not access websites or objects with inappropriate or illegal content
- Be aware that their Internet use is subject to logging and may be monitored consistent with requirements of applicable laws and regulations

4.1.3 Downloads/Software/Outside Files and Disks/USB Devices

Suspicious e-mail attachments are to be reported before clicking on the attachment.

Users should limit the download of files from the Internet, e-mail attachments from outside sources, or use disks/external storage devices from non-Company sources. The Company does not approve the use of USB devices on Company laptops and desktops.

Suspected malware introduced to the Company's network should be reported immediately to CTO.

4.1.4 Retention and Litigation

User communications can be retained on the system, and, even if no longer retained on the user's machine, they may be retained by the recipients or forwarded to others whom the user never intended to receive.

Electronic communications are discoverable and subject to subpoena by outside persons and entities in arbitration/litigation and regulatory proceedings.

4.2 E-mail

The Company prohibits the unauthorized or inadvertent disclosure of sensitive Company information via e-mail and also prohibits unacceptable and inappropriate use of electronic mail, which is defined below.

This policy covers appropriate use of any e-mail sent from a Company e-mail address and applies to all employees, vendors, as well as external consultants, temporary staff, agents and third-party contractors, operating on behalf of the Company.

Any e-mail that contains information regarding the business of the Company falls in the scope of the E-mail policy.

4.2.1 E-mail Use and Retention

The Company e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages and to send PII or other confidential/sensitive information to unauthorized recipients.

The Company may monitor messages without prior notice. The Company is not obliged to monitor e-mail messages.

The Company shall tag e-mails from external networks to differentiate between Company recipients e-mails from the internal network vs. external sources to assist in preventing phishing scams.

Emails are retained for 5 years and purged automatically.

Mass marketing mailings from the Company shall be approved by the Company's Chief Marketing Officer ("CMO") before sending.

Users will not store or transfer Company-related e-mail on non-work-related computers or devices, except as necessary or appropriate for Company purposes.

4.3 Clean Desk and Clear Screen

Laptops, disk, tapes, CDs/DVDs, Thumb drives, and paper shall be placed in secured locations/cabinets depending on their security classification.

All desktops and laptops should have a password-protected screensaver that will automatically be activated within five to fifteen minutes of inactivity.

Incoming and outgoing mail collection points should be protected or supervised so that letters cannot be stolen or lost, and faxes should be protected when not in use.

Desk and filing cabinets are to be locked whenever employees are away from them for a prolonged period and when leaving the office.

Workspaces are to be cleared of personally identifiable information (PII) and other confidential information before leaving for the end of the business day and whenever the employee will be absent from the office for extended periods of time.

4.4 Mobile Devices

Employees granted corporate mobile devices are responsible for its safekeeping and any information it may contain. Approved encryption software will be used on all corporate mobile devices. Corporate mobile devices are provided for official use by authorized employees, they are not to be loaned or used by unauthorized individuals.

Mobile devices are not to be left unattended; users are to shut down, log off, or activate a password-protected screensaver before walking away from the machine. The user is expected to update the corporate mobile device when new operating systems and security patches become available to maintain the security of the device.

If an employee is terminated or resigns, the user's access will be immediately cut and will not have access to email.

4.5 Physical Security

Only authorized personnel are allowed entry into designated work areas. All visitors must check in with reception or security upon entering Company offices and are required to be escorted by authorized personnel at all times.

Physical keys or keycards are issued for access to designated work areas. It is each employee's responsibility to provide appropriate protection of their physical keys to prevent unauthorized use. Managers authorize the issuance of physical keys or keycards for employees through appropriate requests. The Company will maintain an inventory of physical keys or keycards issued and returned.

4.6 Access

Access control to information assets will be enforced via one-time password authentication or public/private keys with strong passphrases.

All users must have their identity verified with a user ID and a secret password, or by other means that provide equal or greater security, prior to being permitted to use Company's information resources.

Inactive logon credentials may be suspended after 30 days. Removal will occur at the discretion of Company management and IT. IT will inform managers of inactive accounts at regular intervals.

The number of consecutive attempts to enter an incorrect password will be limited, following three consecutive failed attempts, the user ID will be suspended until reset by an authorized user, such as a system administrator, the IT help desk, or other IT security professional.

4.6.1 Third-Party Access

Contractor access

Encryption or password protection must be used when available to protect Company information. If unable to encrypt, contractors should consider alternatives to e-mail.

Each contractor is responsible for safeguarding his or her password, user ID, and protecting them from unauthorized use. Any unauthorized attempt to discover the password of another user or to access Company information or systems using another person's password or user ID is prohibited.

Contractors are accountable for any incident arising from improperly protected personal user IDs and passwords. Compromised passwords and/or user IDs must be brought to the notice of IT for immediate action.

Vendor access

Vendor access must be uniquely identifiable and password management must comply with the password standard practice referenced in section 4.7.

Upon termination of contract or at the request of the Company, the vendor must surrender Company data, equipment and supplies as reasonably able.

All software used by the vendor in providing service must be properly inventoried and licensed.

4.6.2 Third-Party Connection Requests and Approvals

All third-party connection requests must have an authorized signature for approval and all third parties requesting a network connection must complete and sign a Company Non-Disclosure Agreement.

4.7 Passwords

All production system-level passwords must be managed in a secure fashion (such as a password management database). User-level passwords (e.g., e-mail, web, desktop computer):

- Must be changed at least every 90 days
- Must lock out after 3-5 failed password attempts
- Must conform to the password guidelines referenced in section 4.7.1

4.7.1 Password Guidelines

User passwords should contain a combination of 3 of 4 criteria:

- Upper-case character
- Lower-case character
- Number
- Special characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc.)
- User passwords must be at least 8 characters in length.

4.7.2 Password Protection Standards

- Users are to use different passwords for Company accounts from other non-Company access
- Users will not share Company passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Company information
- Passwords should never be written down or stored on-line without encryption
- Users will not reveal a password in e-mail, chat, or other electronic communication
- Users will not speak about a password in front of others
- Users will not reveal a password on questionnaires or security forms

4.8 Antivirus

This section applies to all computers that are connected to the network via a standard network connection, wireless connection, modem connection, or virtual private network connection. The definition of computers includes desktop workstations, laptop/tablet computers, handheld computing devices, and servers.

All computers attached to the Company's network are installed with and supported anti-virus software powered by MalwareBytes. Malwarebytes, an EDR (End-point Detection & Response) software, finds and removes malware from devices, including malware, virus, and ransomware attacks. This software monitors all Company laptops, hardware, and applications 24/7 with the ability to lock down a device at any moment.

The Company's ERD system includes 72 hour ransomware rollback which allows the Company to wind back the clock and rapidly get back to a healthy state. If an attack impacts end user files, the ERD system rolls back these changes to restore files that were encrypted, deleted, or modified in a ransomware attack allowing the Company up to 72 hours to undo any damage.

Activities with the intention to create and/or distribute malicious programs onto the network (e.g. viruses, worms, Trojan horses, e-mail bombs) are strictly prohibited.

If an employee receives what they believe to be a virus or suspects that a computer is infected with a virus, it must be reported to IT support. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from IT support. Any virus-infected computer will be removed from the network until it is verified as virus-free.

4.9 Cyber and Data Security

This section applies to the guidelines for protecting the integrity of data and technology infrastructure. To ensure the security of Company devices and information, employees are required to:

- Ensure Company-issued devices (including tablets, computers, and mobile devices) are password protected
- Obtain authorization before removing Company devices from Company premises
- Regularly update devices with the latest security software and operating system updates

Personal devices may be used to access Company systems, applications and information and must request approval of the use of personal devices; employees must:

- Ensure personal devices used are password protected
- Install applicable antivirus software and update regularly

Intrusion Risk Mitigation

All Company owned devices must have mobile device management software (MDM) installed enabling the CTO or their designee the ability to permit or deny access to the Company's networks, applications or systems.

A firewall to permit or deny network transmissions based upon a set of rules as specified by the user/owner will be maintained to protect the Company's networks from unauthorized access while permitting legitimate communications.

All Company owned devices must have commercially supported malware protection installed.

Vulnerability Scanning and Penetration Testing

An annual penetration testing and vulnerability assessment will be performed, including tests and intrusion simulations to assess the strength of the Company's network security measures and reveal potential security weaknesses. Findings will be identified in an assessment report and reviewed by the CTO or their desinee.

Confidential Data and Network Security

Only authorized users should have access to the Company's confidential data and Company network; the IT staff must grant authorized users access to the systems, applications, network, or data in accordance with the security levels authorized by the CTO or their designee.

4.10 Breach Response and Breach Notification

This section applies to the procedures for data security breaches of protected or sensitive data.

4.10.1 Incident Reporting

Suspected exposure, theft, or breach of protected or sensitive data must be reported immediately to the CTO.

All reported incidents will be investigated immediately to confirm the suspected exposure, theft, or breach of protected or sensitive data. If a breach incident is confirmed to have occurred, the appropriate procedures in place will be followed and the severity of the data breach will be assessed.

An incident report must be filed that includes the full details of the incident, including the data impacted and individual reporting the incident.

In the event of a data breach, to limit the exposure, the Company will:

- Disconnect the impacted systems or networks from the Internet
- Contact the appropriate personnel to notify them of the breach
- Document the date and time of the breach, files, systems or applications impacted, and actions taken to secure the data
- If possible, reimage the system and restore from backup files

4.10.2 Incident Response

All data breach incidents must be investigated immediately and an incident report must be completed. The investigation should be documented and shared with the affected parties and relevant stakeholders. The investigations should:

- *Determine if the incident is classified as a breach*: classify the breach type and data impacted
- *Assess the severity of the breach*: determine the scope, confidentiality of data compromised, systems and applications affected, and extent of the breach
- *Identify the cause of the breach and whether it has been contained to mitigate further data loss or theft*: investigate the current status of the compromised data, applications, and systems
- *Determine depth of loss and exposure:* identify and document the data impacted, and vendors or individuals affected
- If appropriate, notify authorities

- *Ensure actions and decisions are appropriately documented:* Notify those impacted by the breach, determine internal communication and public messaging, and perform post-incident analysis

4.11 Document Retention and Destruction

This section applies to the procedures for disposing of electronic and paper documents and records, and to identify documents and records that need to be retained permanently or for some period of time for legal and/or operational reasons.

4.11.1 Retention

Electronic and paper documents will be retained in the same manner. A retention period of "current year plus 1 year" is adequate for most documents and records. Longer retention periods are based upon legal, audit, brokerage operations or management requirements.

A "legal requirement":

- Specific federal or state law requiring document or record retention
- Important property rights which the Company has a legal obligation to protect are involved
- The Company is aware of specific, impending legal action

An "audit requirement" refers to state and federal tax audits. Documents and records needed for audit are retained for the current year plus 7 years, a period long enough to cover each tax audit requirement.

A "brokerage operations requirement" refers to documents and records collected and stored in the Company's transactional management systems. Documents and records collected for each closed real estate transaction are retained for the current year plus seven (7) years, a period long enough to cover each state commission audit requirement.

A "management requirement" refers to the needs of Company department records of proprietary, technical or economic value to current or future operations of the Company.

If a user has sufficient reason to retain an e-mail or attachment, it should be moved to an archived file folder.

4.11.2 Disposal

Departments are responsible for the maintenance and destruction of their records. Once the appropriate retention period has elapsed, paper documents will be placed in secure bins for disposal or shredded.

Annually, each department conducts a formal record disposal review, in which a year's collection of records for those in which the record retention requirement has expired, should be properly disposed of.

E-mails and electronic documents and records in which the appropriate retention period has elapsed will be permanently deleted. Backup and archived copies of these files will be deleted. Users must ensure that their personal hard disks, storage media, and servers are purged of the documents and records.

Hardware will be disposed of in the following manner:

- All data will be deleted from the hard-drive
- Hard-drives will be removed from the equipment
- If equipment is kept, the hard-drive should be reimaged
- If equipment is disposed of, hard-drives should be wiped and/or physically destroyed

5. POLICY EXCEPTIONS

Adherence to established Policy guidelines is the responsibility of each employee of the Company**.**

While exceptions may occur within the ordinary course of business, Management must ensure that appropriate action is taken depending on the level and severity of Policy exceptions.

The Policy cannot account for every possible situation. Therefore, where the Policy does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.

6. ENFORCEMENT

Any employee found to have violated the Policy may be subject to disciplinary action up to and including termination. No provision of this Policy will alter the nature of the employment relationship at the Company.

7. GOVERNANACE

Changes to Real's Information Security Risk policy must first be approved by CTO. Thereafter the updated policy is presented to the Audit Committee for approval. Upon approval from the Audit Committee, the updated policy is presented to the Board of Directors for review and approval.

All changes to the policy are documented and are available to all employees.

At least on an annual basis, the CTO/CISO presents to the Audit Committee and the Board of Directors with a report on the state of Information Security at Real.

APPENDIX A Definitions

- **Access controls** – Methods used to prevent unauthorized access to Company's corporate network such as passwords, user ids, digital certificates, etc.
- **Access** – Any connection to Company's corporate network through a Company controlled network, device, or medium
- **Electronic communications system** – Voice mail, electronic mail, intranet, or Internet access system owned, leased, operated, maintained or managed by the Company

- **Information assets** – any data, device, or other component of the IT environment that supports information management related activities
- **Information security risk** – risk to the Company's operations, assets, and individuals due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems
- **Physical security** – Measures that are designed to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building facility, resource, or stored information.
- **Remote access** – Any access to Company's corporate network through a non-Company controlled network, device, or medium
- **Risk exposure** – The measure of possible future loss which may result from an activity or event
- **Risk tolerance** – The acceptable variation from the risk appetite
- **Sensitive data** – Personal data that contains information on the data subject's race or ethnic origin, religious beliefs or other beliefs of a similar nature, political opinions, physical or mental health or condition, sexual history or orientation, trade union membership and commission or alleged commission of any offense, and any related court proceedings
- **User ID** – User name or other identifier used when an associate logs into the corporate network
- **User** – Employee authorized to have access to certain designated information or system.
- **Virtual Private Network (VPN)** – Encryption and tunneling technology used to connect users or branch offices securely over a public network, usually the Internet; typically, a VPN will be configured to allow an authorized user to obtain remote desktop control of his or her office system. In the absence of a user-controlled system on the Company network, permissions will be configured only for remote access to the systems for which the user has prior authorized access.