Technology Acceptable Use Policy

1.0 Overview

With advancements in new technology and practices, companies must ensure that deployment of these technologies does not expose the company to additional risks. These risks include: data compromise, network intrusion, virus outbreak, distribution of malicious software, distribution of intellectual property, etc.

2.0 Purpose & Scope

The purpose of this policy is to manage the introduction of devices and technology utilized by RevGen contractors. This policy applies to contractors, consultants, temporaries and other workers at RevGen, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by RevGen.

3.0 Policy

3.1 Policy Compliance

- It is the policy of RevGen that the use of its computers and software is for appropriate business use with limited use of personal activity. Installation of software must be approved by IT for licensing and security purposes. Further, this policy reaffirms that the Company's contractors have no reasonable expectation of privacy with respect to any computer hardware, software, electronic mail or other computer or electronic means of communication or storage. The Company reserves the right to monitor the use of its computer system. All users are expected to use computer resources responsibly, professionally and lawfully in furtherance of the Company business. Only authorized individuals are allowed access to our computer systems, and at no time should a personal computer be used at a client or to access client information. RevGen Partners reserves absolute access and control over our computer systems.

- The RevGen network, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail and web browsing are the property of RevGen. These systems shall be used for business purposes in serving the interests of the company or the interests of the company’s clients and customers in the course of normal operations.

- Effective security is a team effort involving the participation and support of every RevGen employee, contractor, and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

3.2 General Use and Ownership

- While RevGen desires to provide a reasonable level of privacy, users shall be advised that the data they create on the corporate systems remains the property of RevGen. Because of the need to protect RevGen's network, management cannot guarantee the confidentiality of information stored on any network device belonging to RevGen.

- Contractors shall be responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, contractors should consult their direct contact at RevGen.

- Any information considered sensitive or vulnerable must be encrypted. This includes passwords and client data at rest, in storage, and in transit.

- For security and network maintenance purposes, authorized individuals within RevGen may monitor equipment, systems and network traffic at any time. See the monitoring section at 3.5.

- RevGen reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

- Any lost or stolen devices, whether a company provided laptop or device, or a personal device that had access to company resources (i.e. email, SharePoint, OneDrive, etc.), must be reported to the IT department immediately.

- RevGen reserves the right to remove company data from personal mobile devices if the need arises, including, but not limited to, when the contractor no longer performs work for RevGen, a device is lost or stolen, etc. Personal data will not be removed from these devices by RevGen, unless specifically requested to by the contractor, such as in the case of a lost/stolen device.

3.3 Security and Proprietary Information

- The user interface for information contained on the RevGen network shall be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in the RevGen *Access Control Policy*. Examples of confidential information include, but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists and research data. Contractors shall take all necessary steps to prevent unauthorized access to this information.

- A list of all systems and/or devices authorized for use shall be established and maintained.

- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords shall be changed according to the *User ID and Password Policy*. If the contractor has reason to believe their password has become known, they must immediately notify the Help Desk, so a new password can be set and systems can be checked for unauthorized access.

- All workstations shall be secured with a password-protected screensaver with the automatic activation feature set according to the *User ID and Password Policy* or by logging-off when the workstation will be left unattended.

- All mobile devices accessing company resources must require an unlocking code to be entered before the device may be accessed.

- Because information contained on portable computers is especially vulnerable, special care shall be exercised to physically safeguard such devices.

- Postings to newsgroups by contractors from a RevGen email address shall contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of RevGen, unless posting is in the course of business duties.

- All workstations used by the contractor that are connected to the RevGen network, whether owned by the contractor or RevGen, shall be continually executing approved antivirus software with a current virus database unless overridden by departmental or group policy.

- All network connections, including connectivity to the RevGen network shall be implemented by the Network Administration Team and shall be subject to security review. Contractors are prohibited from connecting an unauthorized network access device such as a modem, wireless access point, or cellular broadband device to the RevGen network.

- Remote access technologies deployed by the network infrastructure team shall meet the following requirements.

    - Cell phones may only connect to the guest Wi-Fi network while in the REVGEN office.

- The handling of client data should be done so in accordance with MSAs and any other agreement that may be in place to safeguard information.

- Contractors shall use extreme caution when opening email attachments or using links received from unknown senders as they may contain malware. In the event a suspicious attachment or link is opened, the contractor must immediately notify the IT department so any necessary steps can be taken.

- The use of removable media should be used in accordance with client agreements and the data classification policy.

3.4 Unacceptable System and Network Activities

Note: The following activities are, in general, prohibited. Contractors may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., the Systems Administration Team may need to disable the network access of a host if that host is disrupting production services, etc.).

- Under no circumstances shall a contractor or associate of RevGen engage in any activity that is illegal under local, state, federal or international law while utilizing RevGen-owned resources.

- Contractors and associates shall not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by RevGen.

- Contractors and associates shall not make unauthorized copies of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which RevGen or the end user does not have an active license.

- Contractors and associates shall not export software, technical information, encryption software or technology, in violation of international or regional export control laws. Senior management should be consulted prior to export of any material that is in question.

- Contractors and associates shall not introduce malicious programs into the network or IT environment (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Contractors and associates shall not reveal account passwords to others or allow the use of company accounts by others. This includes family and other household members when work is being done at home.

- Contractors and associates shall not use a RevGen computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

- Contractors and associates shall not make fraudulent offers of products, items or services originating from any RevGen account.

- Contractors and associates shall not make statements about warranty, expressly or implied, unless it is a part of normal job duties.

- Contractors and associates shall not affect security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the contractor is not an intended recipient or logging into a server or account that the contractor is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Contractors and associates whose job function does not include information security shall not engage in port scanning or security scanning.

- Contractors and associates shall not execute any form of network monitoring which could intercept data not intended for the contractor's host unless this activity is a part of the contractor's normal job/duty.

- Contractors and associates shall not circumvent user authentication or security of any host, network or account.

- Contractors and associates shall not use any program, script or command or send messages of any kind with the intent to interfere with or disable a user's terminal session, via any means, locally or via the RevGen network.

- Contractors and associates shall not provide information about, or lists of, RevGen employees to parties outside of RevGen without authorization.

- Contractors and associates shall not connect to unsecure or public wifi, unless some security mechanism, such as VPN, to ensure the security of corporate and client information is used. Examples include coffee shops, restaurants, airports and other public wifi points.

3.4 Unacceptable Email and Communications Activities

- Contractors and associates shall not send unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

- Contractors and associates shall not engage in any form of harassment via email, telephone, texting or other electronic means, whether through language, frequency, or size of messages.

- Contractors and associates shall not send confidential information (i.e. customer data) through email without proper safeguards in place.

- Contractors and associates shall not set up automatic email forwarding rules.

- Contractors and associates shall not engage in unauthorized use or forging of email header information.

- Contractors and associates shall not engage in creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

- Contractors and associates shall not engage in the use of unsolicited email originating from within the RevGen network of or that of third party services providers on behalf of, or to advertise, any service hosted by RevGen or connected via the RevGen network.

3.5 Monitoring

RevGen reserves the right to:

- Block and/or monitor Internet access to sites
- Monitor user's electronic communications activity (email, IM, etc.)
- Monitor activity on other network-connected devices

3.6 Responsibilities

- RevGen Contractors shall abide by the acceptable use policies set forth in this document.

- The RevGen Security Officer shall:

    - Create, disseminate, and maintain technology acceptable use policies.
    - Maintain a list of acceptable technologies and their use.
    - Provide guidance and other policies related to information security and technology.

4.0 Guidelines

None.

5.0 Enforcement

Any contractor found to have violated this policy shall be subject to disciplinary action, up to and including termination of contractor agreement.

6.0 Revision History

The following table maintains the history of changes to this policy.

Rev	Date	Author	Description
1.0			Initial Content
1.1	12/5/18	Steven Martin	Updated email policy
1.2	6/24/19	Steven Martin	Contractor version