"GCL International Bulgaria" Ltd. ("the Company") is committed to establish the acceptable usage guidelines for all technology resources. These resources can include, but are not limited to, the following equipment:

- Computers (Laptops, Desktop Computers, Mobile Devices, Servers, etc.)
- Network Equipment (Routers, Wireless Devices, Fiber Optic Lines, VoIP Phones, etc.)
- Audio/Video Equipment (Cameras, Projectors, Security Cameras, Digital Cameras and

Camcorders, Scanners, Printers, Copiers, Fax Machines, etc.)

- Software (Operating Systems, Application Software, etc.)
- Resources (Drive File Storage, Website File Storage, Email Accounts, Social Networking Accounts, etc.)

This policy applies to all employees, contracted employees, contractors, sub-contractors, at The Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by The Company.

While the Company desires to provide a reasonable level of freedom and privacy, users should be aware that all equipment, network infrastructure, and software applications are the property of the Company and therefore are to be used for official use only. Also, all data should be treated as such, and protected from unauthorized access.

The following activities provide a general guideline to use the Company resources in an acceptable manner:

- All passwords used to access the Company systems must be kept secure and protected from unauthorized use.
- No user account can be shared between individuals. Authorized users are responsible for the security of their own passwords and accounts.
- Do not transfer personally identifiable information on equipment, cloud drives and storage devices.
- All computers residing on the Company network, whether owned by the employee or the Company, shall be approved with virus-scanning software with a current, up-to-date virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders.

- All electronic works should be completed or transferred via the Company email accounts so that no data is transferred off-
- All workstations should be kept secure. Users should lock the workstation when not attended to protect unauthorized users from accessing secure files.
- Social media and chat apps shall not be used for business processes.

Under no circumstance shall an employee of the Company be authorized to engage in any activity that is illegal under local or international law while utilizing The Company resources. The lists below are to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, 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.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, and the installation of any copyrighted software.
- Exporting software, technical information, encryption software or technology, in violation of international or local export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server environments.
- Revealing the 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.
- Using any machine to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any The Company account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Executing any form of network monitoring which will intercept data, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.

- Sending unsolicited email messages, including the sending of “junk mail" or other advertising material to individuals who did not specifically request such material.
- Any form of harassment via email, telephone.
- Unauthorized use, or forging, of email header information.
- Use of unsolicited email originating from within the Company’ networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by The Company.

Passwords

When setting password users, the strength is normally determined within the settings of the system. However, user should:

- Avoid choosing obvious passwords (such as those based on easily discoverable information).
- Not to choose common passwords (use of technical means, using a password blacklist recommended).
- Should not re-use password.
- Shall not record passwords to store and retrieve them securely.
- Shall use only authorised password management software (available via the IT manager).
- All passwords must be memorised and not recorded anywhere.
- Must be unique for each application.