ACCEPTABLE USE POLICY

October 2022

Scope

This Acceptable Use Policy governs the use of Gravyty resources, its subsidiaries, affiliates and personnel including employees and contractors.

Policy

Any employee who uses any Gravyty resource consents to all of the provisions of this policy and agrees to comply with all of the terms and conditions set forth. Violations of this policy or any other Gravyty policy may be subject to revocation or limitation of computer and network privileges as well as other disciplinary actions or may be referred to appropriate external authorities. All entities covered under the policy Scope must follow the below:

- Comply with all applicable local, state and federal laws.
- Comply with all Gravyty policies, regulations, procedures and rules.
- Respect the intellectual property rights of others. Making unauthorized copies of licensed software or copyrighted material is prohibited.
- Removal of Company assets outside of the country requires approval of the TOC via a Help Desk ticket at toc@gravyty.com.
- Refrain from sharing passwords or accounts with anyone, including trusted friends or family members. Users will be held responsible for any actions performed using their accounts.
- Only access files or data with an authorized business need to do so.
- Circumvention of any security measure of Gravyty is prohibited.
- Operating a business, usurping business opportunities, organized political activity or conducting activity for personal gain is prohibited.
- All documents of a sensitive or confidential nature are to be shredded when no longer required.

Electronic Communications and Internet Acceptable Use

Business Use

Electronic communications are necessary to relay business information both internally and externally; however, such use must be in compliance with this policy and not violate confidentiality or privacy requirements. Employees may use the Internet to fulfill work responsibilities, increase their professional knowledge, and access topics that have relevance to their professional duties.

We reserve the right to monitor employees' use of the Internet (including Email) at any time, to ensure compliance with this policy. Employees should not expect that use of the Internet or electronic communications - including but not limited to the sites visited, the amount of time spent online, and the correspondence sent or received - will be private.

Upon termination, employees' Email and other electronic communications may be accessible to the department manager for business continuity purposes.

Provisions for Non-Business Related Use

Employees may use the Email system for non-business related correspondence, provided such use is brief and occasional. However, the employee must understand that all messages are stored on the Email server and become the property of Gravyty.

Incidental and occasional non-business related use of the Internet is permitted. Acceptable examples include: briefly checking personal web-based Email accounts, online news, travel schedules, and weather reports.

Personal use of the Email system and Internet is prohibited if it interferes with productivity or work performance, or if it adversely affects other employees or the efficient operation of any component of Gravyty's computer network.

Personal Networks Security Settings Recommendations

Prohibited Activities

The following activities are specifically prohibited:

- Using the Email system or Internet to upload/download/send copyrighted or proprietary information belonging to Gravyty or any third party (including commercial software), unless specifically directed to do so per Senior Management.
- Individual employees should not use the Email system or Internet to upload/send PII/PHI externally (outside the Gravyty network). The only persons within Gravyty who may transmit PII/PHI electronically outside the Gravyty network are those with appropriate permissions within the Customer Success and Data Implementation teams (only using secure methods such as encryption and secure file transfer protocol).
- Sending Email using another person's identity, an assumed name, or anonymously, except when necessary for newsletters and other business purposes.
- Intentionally deleting Emails upon termination that could result in a negative business impact. Employees' Email must remain intact upon departure.
- Permitting another person (employee or non-employee) to access the Email system and/or the Internet under one's logon user identification.
- Using personal Email to conduct Gravyty business.
- Using a personal computer to connect directly to Gravyty's network without obtaining a Policy Exception from the TOC.
- Storing Regulatory Confidential data on removable media without obtaining a Policy Exception from the TOC.
- Accessing, retrieving, or printing anything that exceeds the limits of generally accepted standards of good taste and ethics. Offensive or disruptive messages include those that contain sexual content/connotations, racial slurs, gender-specific comments, or any other subject material that offensively addresses someone's age, gender, sexual orientation, religious or political beliefs. Email and the Internet may not be utilized in such a way that is offensive, disruptive, harmful, or that may be construed as harassment. Creating, displaying, or sending offensive or derogatory images, messages, or cartoons can be construed as harassment and are thus

prohibited. If offensive or disruptive Internet sites are accessed inadvertently, this should be reported to the TOC.

- Engaging in any unlawful activities.
- Engaging in personal commercial activities, including offering services or merchandise for sale or ordering services or merchandise. Making occasional online purchases for personal reasons is acceptable as long as it does not interfere with productivity or work performance.
- Conducting solicitations for commercial ventures, religious, charitable or political causes, or any other solicitations not related to professional duties without explicit permission from the CEO.
- Downloading and storing files on the Gravyty computer network that do not serve business functions.
- Attempting to bypass Gravyty router/firewall restrictions on Internet access, intentionally interfering with the normal operation of the network, or avoiding Gravyty anti-malware policy and procedures.

Gravyty Blogging and Social Networking Policy

Gravyty respects the right of employees to use blogs, websites and social networking sites as a medium of self-expression and public conversation and does not discriminate against employees who use these mediums for personal interests and affiliations or other lawful purposes. Employees are expected to follow the guidelines and policies set forth to provide a clear line between each employee as an individual and as an employee of Gravyty.

Gravyty hosts a blog that includes information about company events and other topics of interest to its employees. There are also pictures taken of employees participating in company sponsored events or meetings. Every effort is made to ensure that individuals have granted permission for their picture to be displayed on the company blog. A limited number of individuals at the company are authorized to post to the blog and it is their responsibility to ensure that the appropriate permissions have been obtained. If an employee wishes to refrain from having their picture available for public viewing, they can contact the human resources department and it will be removed within 24 hours.

Employees are personally responsible for their commentary. Employees posting information on the Internet using any medium can be held personally liable for commentary that is considered defamatory, obscene, proprietary or libelous by Gravyty or any other offended. Employees must never post commentary on the Internet using any medium that directly or indirectly defames Gravyty. Employees must adhere to the Confidentiality Agreement and avoid posting any information about Gravyty business that is confidential or proprietary. Employees should refrain from posting pictures of any Gravyty personnel or related functions on any website which can be viewed publicly. Gravyty reserves the right, without any explanation or reason, to direct its employees to remove any commentary in a timely manner after Gravyty's request.

All employees have a duty to avoid affiliation, indirect, or direct involvement with organizations or relationships which conflict with the business objectives and interests of the Company, which may detract from one's loyalty to Gravyty, or which detract from providing sufficient attention to an employee's employment responsibilities to the Company. Employees cannot use blogs or social networking sites to harass, threaten, discriminate or disparage against employees or anyone associated with or doing business with Gravyty. If an employee chooses to identify themselves as an employee of Gravyty, they may be viewed by some readers as a spokesperson for Gravyty. Because of this possibility,

employees must state that views expressed in a personal blog or social networking site are their own and not those of the company, or of any person or organization affiliated or doing business with the Company.

Employees cannot post on personal blogs any advertisements of Gravyty services nor sell Company services without prior consent from Marketing.
If an employee is contacted by the media or press about any posts that may relate to Gravyty's business, employees are required to first notify and speak with Marketing before responding to any such inquiry. This policy is meant to include (but is not limited to) any blogs in the public domain, personal websites, as well as social networking sites like Facebook, Twitter and other websites, as applicable.

If an employee does not follow the policy regarding websites, blogs and social networking sites and/or violates our Company Confidentiality Agreement, disciplinary action may be taken, up to and including termination of employment for cause.
All questions relating to this policy or personal blogs may be addressed with Human Resources.

Inspection
Gravyty reserves the right to monitor and record all Email, Network, and Internet usage and transmitted content for management review. Gravyty also reserves the right to inspect any and all files stored in private areas of the Gravyty Network to ensure compliance with this policy.

Employee Considerations
Care should be taken when creating any Email message. Email is a medium for professional correspondence. Always check messages for correct address, accuracy, tone, and appropriate language. Electronic communication should be sent using care and good judgment. In particular, employees should realize that they represent Gravyty when using their agency domain address (Gravyty.com).
Employees must either lock their computers or log off when they are not physically present at their workstations. Employees must not share passwords with other employees or anyone outside Gravyty.
Employees must ask permission from TOC prior to downloading files from the Internet or accessing sites if they have any doubts about the source or file's network safety.
Email is not intended to replace employee responsibilities for communicating directly (or via Zoom) with their coworkers. Email is designed to address short, uncomplicated issues. It is not an appropriate medium for conveying information that may evoke a strong emotional response or for explaining complex topics.

Internal Communication and PII/PHI
As much as possible, Gravyty employees should refrain from including PII/PHI within internal electronic messages (either within the message itself, or as an attachment), or within Gravyty's ticketing system (e.g. Jira). If a Gravyty employee needs to electronically communicate PII/PHI to another Gravyty employee through the secure company network, below is the preferred method of doing so:

- Use Gravyty Donor ID or Import ID (e.g. CRM ID) for donors instead of PII/PHI when possible.
- Use Gravyty User ID for fundraisers instead of PII/PHI when possible.

- Use HubSpot Contact ID for employees, general business contacts, and current and former customers instead of PII/PHI when possible.
- Use ChurnZero Contact ID for current and former client contacts instead of PII/PHI when possible.
- Internal communications between Sales and Marketing will anonymize emails by removing PII/PHI when customer language needs to be shared.
- When PII/PHI needs to be included for troubleshooting purposes, upload the information to the Troubleshooting Documents subfolder contained within the specific Customer folder within the CS Shared Drive on Google Drive and include the link when escalating.

In cases where the preferred option is not feasible, the employee may transmit internal Email messages containing PII/PHI to a coworker or coworkers who need the information for a legitimate business reason. However, the employee will restrict the content of such messages to the minimum amount of PII/PHI necessary to accomplish the purpose. Email messages containing PII/PHI may not be transmitted to any source outside the network. Employees are routinely educated to be cognizant of this, as well as to carefully double check Emails for the correct internal recipient(s) address prior to sending.

External Communication and PII/PHI
Employees may not use the Email system, electronic communications or the Internet as a mechanism for collecting, displaying, transmitting, or disclosing PII/PHI from or to persons/places outside the Gravyty computer network. The Customer Success and Data Implementation teams have the exclusive right to electronically transmit files outside the Gravyty computer network. These teams do this by using encryption and secure file transfer protocols. Never include or attach PII/PHI to external electronic messages. If an employee has PII/PHI that needs to be sent outside Gravyty, the managers of Customer Success and Data Implementation will coordinate the transmission of PII/PHI.
If an employee receives PII/PHI in an electronic message from an outside source, the following should occur immediately:

- Not open any attachments, with the exception of communications with clients regarding adding/amending/deactivating user accounts (including but not limited to Advancement Team spreadsheets).
- Exception: Gravyty-generated messages (e.g. First Draft, Guide, Go Reports) that are forwarded back from a client or user.
- Submit a Help Desk ticket at toc@gravyty.com.

Violations of the Internet Acceptable Use Policy
Any employee who fails to adhere to the conditions for use of Email, electronic communications and Internet systems will be subject to disciplinary action up to and including termination of employment. Illegal activities may also be reported to the appropriate authorities. By logging on and using the Email electronic communications and Internet Systems, the user acknowledges and agrees with the above stated conditions.

Remote Access to Gravyty's Network
Only Gravyty-issued computers may connect directly to Gravyty network resources. Proper approval and instructions will be granted for those with a business need. Remote access users have the following responsibilities:

- If possible, remote access users should utilize a Gravyty provided system for remote access.

- Users should be aware of the specific risks, threats, vulnerabilities and the proper use of a secured remote access system.
- Users working from home must conduct business in an area separate from other activities in the home to minimize inadvertent exposure to sensitive information.
- Users should notify the TOC should they see or witness suspicious activity, or activity that violates this policy.

Special Considerations for Using Personally Owned Systems
Users accessing Gravyty network resources with their personally owned computer have the following responsibilities:

- Utilize Antivirus software that is current with up-to-date definitions.
- Utilize spyware detection/removal tools.
- Utilize a personal firewall.
- Utilize a manufacturer supported operating system (e.g. not a system that is no longer supported and has no security updates being developed).
- Secure the operating system, with all manufacturer security updates applied.
- Turn off the system when not in use.

Use of Public Computers
Kiosks and other publicly available computers must never be used to access Gravyty network resources.

Cell Phone Policy
Only devices (i.e. smart phones, cell phones, PDAs, etc) that support password enabled screen lock and remote wipe capability are permitted to establish a connection with Gravyty's WorkSpace. Should a user with a personal device meeting this criteria opt to configure Gravyty Email to his/her device, the user understands and agrees with the following terms:

- Remote wipe will occur upon termination of employment.

- Remote wipe may occur (during active employment) without the user's prior knowledge. Users are responsible for reporting misuse, loss, theft or any other breach that could potentially compromise the integrity of Gravyty confidential information or PII/PHI.
- Users are required to activate MFA for all Gravyty accounts.

Cell Phone Use While Driving Policy
Employees must adhere to all federal, state or local rules and regulations regarding the use of cell phones and its applications while driving. Accordingly, employees must not use cell phones if such conduct is prohibited by law, regulation or other ordinance. If you are not sure whether the use of a cell phone while driving is prohibited in a particular area, please check with the Human Resources department.
Should an employee need to make a business call while driving, he/she must locate a lawfully designated area to park and make the call or use a hands-free speaking device such as a speakerphone or earpiece. The use of cell phones or other handheld devices to access the internet, Email or text while driving is strictly prohibited.

Collaborative Computing Devices and Tools
Some Gravyty departments may use collaborative computing tools, and the list of approved tools is outlined below:

- Adobe Creative Suite
- Cisco Webex
- Descript
- DocuSign
- Figma
- Google Suite
- Grammarly
- Hootsuite
- HubSpot
- Loop & Tie
- Microsoft Teams
- Rev
- Slack
- Spotify
- Thnks
- Zoom (including mmhmm plugin)

Any other use of hardware or software needed to facilitate collaborative computing must be approved by the TOC and a helpdesk ticket must be submitted for security review, approval and tracking. Remote activation of collaborative computing devices is prohibited.

Return of Assets
Employees and contractors (users) are responsible for exercising good judgment regarding appropriate use of Gravyty assets in accordance with Gravyty policies, standards, and guidelines. Gravyty assets may not be used for any unlawful or prohibited purpose. Assets issued are to be used for conducting Gravyty business exclusively while employed at Gravyty and shall be returned under the direction of Management or upon termination of employment. In an effort to protect PII/PHI and to prevent financial loss, Gravyty has developed a procedure to help retrieve assets from terminated users.
Both Corporate IT and Human Resources will maintain detailed procedures in Google Drive for managing the process associated with collecting Gravyty owned equipment.

Responsibilities
IT/DevOps should:
- Control the dissemination of Gravyty assets by justifying the need of assets and tracking location of assets through proper documentation.
- Educate employees, contractors and partners about the appropriate use and restrictions associated with Gravyty assets.

Human Resources should:
- Notify the TOC whenever a termination is made so that proper asset reports may be provided to them in advance of an exit interview.
- Notify the TOC if the conditions of a termination or transfer are unfriendly.

Employees and contractors should:
- Respect all assets provided by Gravyty.
- Abide by all guidelines set forth to protect Gravyty's assets.
- Return any assets provided by Gravyty upon termination of employment.

Ownership, Location, History and Approval Statement

The TOC is the owner of this document and is responsible for ensuring that this procedure is reviewed in accordance with the Data Security Policy.

Issue	*Date*	*Description of Change:*
1	08/30/2021	Initial Release
2	12/16/2021	Reviewed and approved by TOC
3	07/21/2022	Minor updates approved by TOC
4	10/27/2022	Updated logo to reflect rebranding