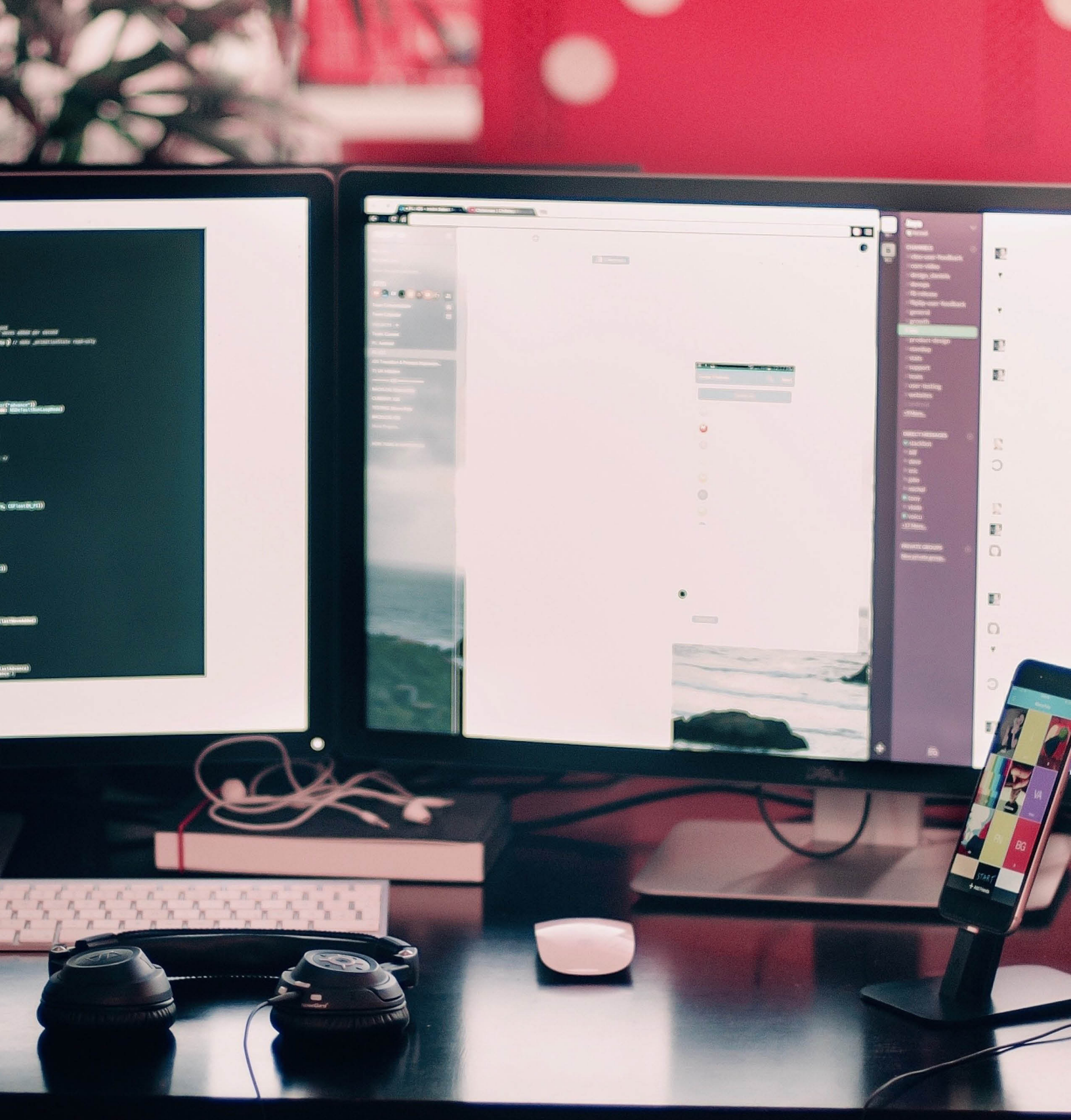

BURGHERGRAY

IT POLICY

I. SCOPE

This Information Technology and Data Security Policy ("Policy") outlines BurgherGray LLP's (the "Firm") information security practices and related business requirements. Users are expected to read, understand, and follow this Policy. However, no single policy can cover all the possible information security issues Users may face, and Users are required to seek guidance from the Firm's leadership if Users have any questions or concerns regarding this Policy or the Firm's technology or data. The Firm may treat any failure to seek and follow such guidance from the Firm's leadership as a violation of this Policy.

This Policy is confidential and proprietary to the Firm. Do not share this Policy outside the Firm unless authorized by a member of the Executive Committee.

This Policy applies to the Firm and our information technology ("IT") hardware (including laptops and other mobile devices), software (including mobile applications), systems, platforms, servers, drives, devices, wireless, Internet or email systems, telephony (including VOIP-related) systems, printers and related systems, or Firm services (collectively, without limitation, "System Resources").

Central to the Firm's IT security, data protection, privacy, disaster recovery and business continuity policies, procedures, requirements, protocols and protections, the Firm employs certain third-party, cloud service providers, to house, secure (including, when applicable, encrypt), manage and maintain much of the Firm's System Resources and Information. Collectively, these secured, third-party environments are the "Work Environment."

This Policy applies to the access, use, handling and protection of any information, data, files or emails owned by, pertaining to, or otherwise in the custody or control of, the Firm (collectively, "Information"), including, without limitation, Firm, client or other third-party information, and the use of any System Resources related to the access to such Information, including, without limitation, any process or method to access, hold, secure, store, copy, transmit, communicate or destroy such Information.

The Firm's System Resources and Information are managed by an IT administrator ("IT Administrator") as designated by and reporting into the Firm's executive committee ("Executive Committee"). The Work Environment is managed by designated third-party, system administrators ("System Administrator(s)"). System Administrators are third-party contractors who are directly managed by their employer's management, and indirectly by the Firm's IT Administrator.

All persons and entities that have access to the Firm's Information, Work Environment, or other System Resources, whether as a partner, employee, independent contractor, of counsel, associate, temporary or contract staff, secondee, consultant, vendor, agent, advisor, counsel, auditor, insurer, government, self-regulatory organization or judicial representative, client or otherwise (collectively, a "User," or "Users") are required to adhere to this Policy.

This Policy applies to the Firm's Information, Work Environment, and any other Firm System Resources, whether managed and/or generated, directly or indirectly, by the Firm, its Users, its third-party service providers or others. This Policy applies to any other form of technology or System Resource that was not deployed or Information that was not generated as of the last update of this Policy, but has been since. All Users must follow this Policy and all other relevant Firm policies while accessing the Firm's Information or Systems Resources.

The Firm's Information, Work Environment, including any other System Resources, as between the User and the Firm, are Firm property and are to be used for Firm business only. Failure to comply may result in immediate termination of User's access to the Firm's Information, Work Environment, and any other System Resources, and/or relationship with the Firm, and any other remedies the Firm may have under law or equity.

This Policy is determined by the Firm's Executive Committee and IT Administrator, and administered by the IT Administrator. The Firm reviews and/or updates this Policy as needed (including as may be required to comply with laws, rule and regulations), and at least once annually. The Firm reserves the right to change this Policy at any time without prior notice.

This Policy is generally communicated by the Firm in four (4) ways: (i) in our employee handbook and new-hire materials, (ii) as a supplement to client and third-party agreements, as required or requested, (iii) in periodic written policy supplements and updates, and (iv) as a part of routine personnel training programs. Alerts and reminders may also be communicated verbally via internal Firm meetings either prior to or after written communication.

II. USER ACCOUNTS AND PASSWORDS; TRAINING

Each User will have a user name and password that is unique to such User. Users are responsible for all actions performed under their user account. Users are responsible for properly safeguarding of their passwords.

All User passwords, regardless of title or system access level, must be changed every thirty (30) days. Users will be reminded of upcoming password expirations via email and task bar notification five (5) days prior (and everyday thereafter) to the expiration time. A User's password must meet the following requirements:

Must be at least 8 characters including a capital letter and number

Must contain characters from the following four categories:

English uppercase characters (A through Z)

English lowercase characters (a through z)

Base 10 digits (0 through 9)

Non-alphabetic characters (e.g., !, $, *, %)

Cannot contain a User's name or parts of a User's full name that exceeds two consecutive characters.

Previous 10 passwords cannot be reused within 180 days.

Users must never share their password with anyone. If a User requires a resetting of his/her password such User must contact the applicable System Administrator for assistance. Password reset requests cannot be made on another user's behalf and must be requested promptly after any access failure. If a User is concerned that his/her user name and/or password have been compromised, breached or misused a User must contact the IT Administrator, or his/her designee, immediately.

Multi-Factor Authentication.

All Users are required to use the Firm's multi-factor authentication system to log on to the Work Environment and certain other System Resources. The first factor is a User's username and password and the second factor preferably is via a security application on a User's mobile phone. Each User must disclose to the Firm a mobile number and the operating system of their mobile Device (as defined below) to enable multi-factor authentication. Any User who does not have access to a personal mobile device may be granted an authentication key fob upon request, or can be authenticated in the office only via the User's Firm desktop phone line.

User Accounts.

Access to the Firm's Work Environment is restricted to authorized Users only. Users who are granted a valid user name and password by a System Administrator, under the instruction of the Executive Committee and/or the IT Administrator, are deemed to be authorized by the Firm to log onto the Work Environment.

Unless authorized by personnel with the authority to grant such authorization, any attempt to gain access to another user's account.

Termination of User Accounts.

User accounts shall be promptly terminated upon either a User's terminated relationship with the Firm or the request of the Executive Committee.

Third-Party Access.

Under no circumstance are clients or other third parties to be given access to the Firm's Information, Work Environment, or any other System Resources unless the Firm's Executive Committee or Managing Partner grants prior written approval.

User Training.

All personnel shall receive training on, and show satisfactory comprehension of, all applicable System Resources and the proper management of Information during their onboarding to the Firm, and at least once a year thereafter.

III. THE WORK ENVIRONMENT.

The Work Environment is hosted by certain third-party service providers, allowing Users to connect via remote protocols using 256-bit AES encryption. Users are capable of connecting using any remote protocol capable device. Saving of system passwords on any personal or Firm issued computer is strictly prohibited with the exception of email passwords on mobile phones and tablets. Users must enter his/her password upon every login attempt.

Access to the Work Environment is granted during the creation of a User's login account. The System Resources and Information to which access is granted will depend on a User's role and access rights. All User access rights are reviewed on an ongoing basis by the Firm's IT Administrator and at least quarterly by System Administrators.

Standard Firm applications included in the Work Environment, without limitation are: Microsoft Office (i.e., Word, Excel, PowerPoint, OneNote), Microsoft Office 365 Outlook (i.e., email, Teams and Skype),

document management (i.e., Worldox and Workshare), Adobe Acrobat, Westlaw, Internet access, time entry (i.e., Sage Timeslips) and client relationship management (i.e., Lexicata) systems. Authorized users are also granted access to a personal storage area on the network. Firm electronic storage area may only be used for storing Firm-related materials.

If a User requires access to non-standard network resources, such User should seek approval and access starting with the IT Administrator, who will arrange the relevant access if appropriate and pre-approved, in writing, by the Executive Committee and/or Managing Partner. All client-related Information is to be saved strictly within the Work Environment, without exception.

Users are prohibited from altering the Firm's Work Environment, or any other System Resources or Information, including attempting to customize the User's desktop. In particular, Users are prohibited from unauthorized installing commercial software, adding non-standard hardware or removing any computer component rendering or potentially rendering the system or systems unstable or otherwise at risk. Only Firm-supplied or approved software, hardware, and information systems may be installed in the Firm's environment or connected to the Firm's network.

IV. ILLEGAL AND PROHIBITED ACTIVITIES.

Use of System Resources or Information for any activities unrelated to Firm business, or to unlawful or unethical activities, is strictly prohibited. Unpermitted activities include, without limitation, tampering, vandalizing, destroying and/or unauthorized access of the Firm's Systems Resources or Information. The Firm specifically prohibits the use of System Resources and Information that are disruptive, offensive to others or harmful to morale, including sexually explicit messages, images and cartoons, ethnic slurs, racial comments, off-color jokes or anything that could be construed as harassment or shows disrespect for others, defames or slanders others, or otherwise harms another person or business. A User's failure to adhere to this Policy may be cause for immediate termination of User's relationship with the Firm, as well as, other remedies allowed the Firm by law and equity.

V. INFORMATION SECURITY.

Physical Security.

The Firm's Work Environment is stored in a secure facility using the following security measures:

All servers that are relevant to the Firm's platform are housed in locked cabinets. Cabinet keys are located within a secure environment with appropriate access and physical controls in place.

Documented procedures are enforced to ensure that physical access to the Work Environment is limited to authorized individuals.

All entrance and exit points into the areas housing the Work Environment are monitored via alarms and CCTV. All activities and CCTV recordings are kept for a minimum of 90 days.

Access control and intrusion detection alarm monitoring systems recording door opening, door closing, and all access attempts are in place and active at all times. Records of such activity are kept for a minimum of 12 months.

Alarm systems transmit alerts directly to facility security as well at the local police.

All staff and visitors within the data facility prominently wear identification credentials.

All authorized data center guests/visitors are required to sign in and out of the access logbook and be escorted at all times.

All Firm related media sent outside the data facility is logged, authorized by management and sent via secured courier or other delivery method that can be tracked.

Digital/Virtual Security.

Saving information from the Firm's Work Environment to any local device whether personal or Firm issued is strictly prohibited. All Firm and client-related Information is to remain inside the Work Environment.

User access to all System Resources and Information is actively reviewed and monitored and is subject to audit at any time without prior notice.

Data Encryption, Backup & Exportation.

All data in the Firm's Work Environment is encrypted whether it is at rest, in transit or actively in use. Any Information exported from the Firm's Work Environment (for the sake of clarification, this includes, without limitation, email, the document management system, a User's desktop and personal folders, or any network shares) must be (i) authorized by the Executive Committee or Managing Partner, and then (ii) decrypted by the IT Administrator or his/her designee, before it can be used elsewhere. If data to be exported is owned by a client, such client must provide a written request to the Firm to have its Information exported from the Firm's System Resources/Work Environment.

The Firm uses TLS encryption for email communication and is able at any time, to establish TLS trust with any external domain.

The Work Environment, including email, is backed up on a daily basis at 7 PM and 12 midnight. In order to retrieve a lost a file or a version of a file, contact the System Administrator to have the file restored. Files created and deleted before daily backup commences will be permanently deleted and unable to restore or obtain. Information in the Work Environment is backed-up for ninety (90) days.

Viruses/Malicious Code/Malware.

Users must not intentionally or inadvertently spread computer viruses, malicious code, malware or ransomware. A computer virus is a software program capable of reproducing itself and usually is capable of causing harm to files or other programs on the same computer or network. Malware, short for malicious (or malevolent) software, is a general term used to refer to a variety of forms of hostile or intrusive software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts and other software. Ransomware is software used or created by attackers to encrypt files on a computer or network. Attackers then demand payment or ransom in order to obtain a key to decrypt such files. The issuance of a decryption key is not guaranteed regardless of payment or other compliance with the attackers' demands. Ransomware can appear in the form of code, scripts and other software.

VI. INCIDENT REPORTING.

How to Respond to an Incident.

If a data breach is suspected or has occurred (either being an "Incident"), such Incident must be immediately reported directly to the IT Administrator, or in his/her absence to a Systems Administrator, the Managing Partner, a member of the Executive Committee or the Firm's Director of Operations, in each case, who will in turn alert the IT Administrator. The IT Administrator is charged with making an initial assessment of the severity based on a number of predetermined, industry standard, criteria designed to assess Firm and other risks. Depending on the result of the initial risk assessment, the incident is reported to the other members of our Crisis Response Team (which is comprised of the IT Administrator, the Managing Partner, at least one Member of the Executive Committee and the Director of Operations). The Crisis Response Team will evaluate various response options and determine the appropriate response based on the Firm's legal, contractual, ethical and fiduciary obligations.

Immediately notify the IT Administrator if Users discover a security incident or suspect a breach in the Firm's information security controls. The Firm maintains various forms of monitoring and surveillance to detect security incidents, but Users may be the first to become aware of a problem. Early detection and response can mitigate damages and minimize further risk to the Firm. Treat any information regarding security incidents as highly confidential Information and do not share it, either internally or externally, without specific authorization.

Security Incident Examples.

Security incidents vary widely and include physical and technical issues. Some examples of security incidents that Users should report include, but are not limited to:

loss or suspected compromise of user credentials or physical access devices (including passwords, tokens, keys, badges, smart cards, or other means of identification and authentication);

suspected malware infections, including viruses, Trojans, spyware, worms, or any anomalous reports or messages from anti-virus software or personal firewalls;

loss or theft of any Device that contains Firm Information, including computers, laptops, tablet computers, smartphones, USB drives, disks, or other storage media;

suspected entry into the Firm's System Resources by unauthorized persons;

any breach or suspected breach of Firm Information;

any attempt by any person to obtain passwords or other Firm Information in person or by phone, email, or other means (sometimes called social engineering, or in the case of email, phishing); and

any other any situation that appears to violate this Policy or otherwise create undue risks to the Firm's Information or System Resources.

Compromised Devices.

If Users become aware of a compromised computer or other Device:

immediately deactivate (unplug) any network connections, but do not power down the equipment as valuable information regarding the incident may be lost if the Device is turned off; and

immediately notify the IT Administrator, an Executive Committee member or the Director of Operations.

Event Management.

Report all suspected incidents, as described in this Policy, and then defer to the incident response process. Do not impede the incident response process or conduct an independent investigation unless the IT Administrator specifically requests or authorizes it. The IT Administrator will serve as Firm's ongoing single point of contact for purposes of addressing issues with respect to the use and security of the Firm's System Resources and Information. The IT Administrator, or his/her designee, shall be accessible to answer questions and address issues on a 24X7 basis, with the ability to obtain relevant information specific to any incidents within 48 hours. The IT Administrator, or his/her designee, shall have access to, or direct knowledge of, the Firm's System Resources and Information network architecture and information technology systems.

Breach Notification.

The law may require the Firm to report security incidents that result in the exposure or loss of certain kinds of information or that affect certain services or infrastructure to various authorities, affected individuals or organizations whose data was compromised, or both. All external notifications will be made under the Managing Partner's direction. No User should act on his/her own or make any external notifications without prior guidance and authorization from the Managing Partner.

Client Notification.

In the event of a data security breach, the Firm shall fully cooperate with its clients to provide all related information in a timely manner and issue any notifications required by applicable law. The Firm will fully cooperate with its clients to identify a root cause and remediate any data security breach discovered.

VI. CLIENT INFORMATION PROTECTION.

All documents relating to client work must be saved in the Firm's Work Environment, namely its document management system (i.e., Worldox). Illegal duplication of Information, software or violation of copyright and other intellectual property laws by the unauthorized duplication or sharing of Information or software, or the unauthorized distribution of copyrighted material, is strictly forbidden. Also, a User should not use a password, access or retrieve stored Information that is not normally accessible to that User.

Any client-provided Information must be treated as confidential Information and held in compliance with this Policy and the Firm's Standard Operating Procedures. All Users must protect all client Information the Firm creates or receives in accordance with this Policy and the Firm's Standard Operating Procedures, in addition to any specific client-identified requirements.

Retention and Return of Client Information.

The Firm retains client Information only for as long as specified by such client or as otherwise necessary to satisfy the purposes for which it was provided to the Firm, except to the extent that longer retention is required by applicable Firm business requirements, legal hold demands, law, regulations or professional ethical rules.

In the event that a client requests their data to be returned and or destroyed, the Managing Partner, or his designee, may contact the client in writing confirming the return and or destruction.

Proper Destruction of Client Information.

In the event that digital information needs to be permanently destroyed, files should be given to the IT Administrator or Director of Operations (who will coordinate with the IT Administrator) for proper destruction.

Paper documents containing privileged or confidential information are to be shredded and under no circumstance be placed in trash receptacles for disposal in an un-shredded state. This includes destruction of pages by hand.

Any non-routine destruction of digital information requires prior approval from the Managing Partner or a member of the Executive Committee.

VII. E-MAIL ACCESS CONTROLS & USE.

The Firm's e-mail services and other System Resources are provided for Firm-related use only. E-mail can expose the Firm to certain risks and offenses. The misuse of e-mail and other System Resources can also cause problems for individual employees. The guidelines below apply equally to internal and external email communications. All e-mail systems and traffic is monitored, encrypted and audited. There should be no expectation of privacy. All emails sent, received and drafted under the "burghergray.com" domain are property of the Firm. Inappropriate or unauthorized use of the Firm's e-mail system, including for non-work related matters, is strictly prohibited. Without limiting the generality of the foregoing, the Firm's e-mail system and other System Resources should not be used to transmit information which:

promotes religious or political causes;

is defamatory or illegally discriminatory (whether on the grounds of sex, race, disability or otherwise);

infringes copyright and other intellectual property laws;

constitutes bullying or harassment or may be construed as harassment or disparagement of others based on race, color, religious creed, sex, national origin, ancestry, citizenship status, pregnancy, childbirth, physical disability, mental/intellectual disability, age, military status or status as a Vietnam-era or special disabled veteran, marital status, registered domestic partner or civil union status, gender (including sex stereotyping and gender identity or expression), medical condition (including, but not limited to, cancer related or HIV/AIDS related), genetic information or sexual orientation;

if so transmitted would result in breach of the Firm's confidentiality obligations owing to our clients or any other third-party;

contains files to be used for hacking or other computer misuse;

contains viruses and other malicious code;

if so transmitted would result in the breach of any data protection law, rule or regulation to which the firm (or any relevant client) is subject;

includes forwarded chain messages;

contains sexually explicit images or images of a pornographic or otherwise inappropriate nature;

may cause offence or harm to another employee or other person;

may reflect poorly on the Firm's name or reputation or any of its clients; and

promotes illegal activity or is illegal to so transmit.

Transmission of Firm and client related emails are to be sent and received with a User's Firm email account only. Use of personal email accounts to conduct firm business is strictly prohibited.

E-mails transmitted using the Firm's System Resources from either have the Firm's name and/or the "burghergray.com" domain address in or otherwise associated with them, whether the e-mail is for official Firm business or for private purposes. Both types can bind the Firm. Users should make every effort to avoid entering into either personal commitments or commitments on behalf of the Firm over the Internet using System Resources unless you are expressly authorized to do so.

E-mail Attacks.

E-mail exposes the Firm to certain forms of cyber-attack. Before opening any attachment or following a link, the User should consider whether:

the e-mail was expected

the e-mail was sent from a known, reputable source

the attachment or link is expected from that source

the wording of the e-mail matches others from that source.

If a User has any doubt about the safety of an email, please do not be opened and but instead report to the IT Administrator immediately. If a User has followed a link or opened an attachment and then become suspicious, please report it immediately to the IT Administrator.

Sending and Receiving Emailed Confidential Information.

All emails for business purposes should conform to Firm standards with confidentiality protected at all times. A User must ensure that emails are sent to the intended recipient and be mindful of the use of the "auto-fill" or "reply to all" functions. If a User has inadvertently misdirected an email, the User should contact the IT Administrator or an Executive Committee member immediately on becoming aware of such mistake.

Access to External Personal E-Mail Accounts.

Access to personal online e-mail accounts (e.g., Gmail) is available through use of System Resources, however, such personal e-mail accounts are not secure and therefore must not be used to transmit client information or otherwise for work purposes, except in cases of emergency when authorized by a partner of the Firm.

VIII. INTERNET ACCESS CONTROLS & USE.

Access to and Use of the Internet.

Employees may not access the Internet to log onto any websites that contain any such material, including any gambling or pornographic websites, or any website that contains any discriminatory message, or disparages any group. Employees may not use computers or the e-mail system for commercial messages of any kind or for messages of a religious or political nature, chain letters, solicitations, gambling or other inappropriate usage. E-mail and Internet access should be used in such a way that all transmissions, whether internal or external, are accurate, appropriate, ethical and lawful.

Many Firm System Resources have access to the Internet. Internet access is intended for official Firm business. Use of the Internet for non-business purposes should generally take place before or after work or during a lunch break and should not interfere with a User's official duties, and in any event should not be excessive. All use of the Internet must be in accordance with this Policy. All Internet activity is monitored.

Prohibited Browsing.

The Internet must not be used for inappropriate or otherwise unauthorized purposes, including, without limitation, the following purposes, any of which may result in disciplinary action:

Activities of a sexual nature

Activities of an inflammatory nature

Activities of an offensive nature

Activities of a racist nature

Bullying

Infringement of copyright laws

Breaches of confidentiality

Hacking - computer misuse

Dissemination of business secrets and confidential information

Introduction of viruses and malicious code

Downloading and or installing unauthorized software

Posting confidential information about other employees, Firm or its clients or suppliers

Gambling/game/entertainment sites

Video streaming via YouTube, Netflix, etc.

Please note that when visiting sites on the Internet, that the owners of such sites and the Work Environment will record a User's activities, including time and date of visit. Accessing inappropriate sites may therefore be damaging to the Firm's image and/or reputation.

IX. PROTECTING YOUR WORKSTATION/WORK SESSION.

The Firm uses physical safeguards to avoid theft, intrusions, unauthorized use, or other abuses of its information assets. Users must comply with the Firm's and our building's current physical security policies and procedures. In addition, Users must:

position computer screens where information on the screens cannot be seen by unauthorized parties;

not display Information on a computer screen where unauthorized individuals can view it;

log off or shut down his/her workstation when leaving for an extended time period or at the end of User's work day. Also, if a User is away from his/her desk for any significant length of time (e.g., lunchtime or breaks) it is good practice to lock one's desktop session to prevent others from accessing Information, including User-generated documents, e-mails or other work product; and

upon logging off the Work Environment, physically clear desks and workstations of all client Information, including, any User notes and drafts.

X. PERSONAL DEVICE MANAGEMENT.

Use of personal computing devices, such as laptops, mobile phones or tablets (collectively, "Devices") by Users for Firm-related purposes may consists of three different mobile Device management methods ("Methods"), namely, Bring Your Own Device ("BYOD"), Choose Your Own Device ("CYOD"), and Corporate Owned Personally Enabled ("COPE") (individually, a "Device Policy"). The purpose of this section is to define appropriate use procedures for personally owned computing Devices used by Users for Firm-related purposes and to lay out the appropriate procedures for the storage of any Information on such Devices. The Firm will determine which Device Policy will apply to each User's Device needs and usage. At any given time a User can fall into one or more Device Policies.

"Bring Your Own Device" (BYOD).

Under the BYOD Device Policy, Users will be allowed to use their own Devices for work either while at the office, or during non-working hours. Users use own their personal Devices must abide by this Policy. The Firm is not responsible for any purchases or costs associated with the use of these personally owned Devices. All Firm Information contained on a BYOD Device shall belong to the Firm.

"Choose Your Own Device" (CYOD).

Under a CYOD Device Policy, Users may choose either a preferred personal computing Device from a Firm-approved list of Devices. This User-chosen Device will either be paid for and owned by the User, or the Firm. If paid for by the Firm, the CYOD Device will be submitted to the Firm upon the User's termination or resignation. Under CYOD, the Firm shall be responsible for certain Device hardware repair and replacement costs. The Firm owns all Information and non-Firm information contained on the CYOD Device.

"Corporate Owned Personally Enabled" (COPE).

Under a COPE Device Policy, the Firm will choose, purchase, and fully own all COPE Devices and all Information and non-Firm information such Device may contain. Here the Firm will cover all Device repair and replacement costs and shall retain the Device following the termination or resignation of such User.

General Device Management.

Unless stated otherwise, the following applies all Device Policies to work performed on a Device on Firm's behalf during working hours and non-working hours, on and off of Firm's premises. In addition, each User is responsible for using his or her Device in a sensible, productive, ethical, and lawful manner. Without limiting the foregoing, Users are expected to know and follow all local and state laws related to using communication devices while driving and are responsible for all traffic violations and consequences resulting from the use of communication devices while driving.

Device Privacy.

All material, data, communications and information, including but not limited to e-mail (sent and received), telephone conversations and voice mail recordings, instant messages, ad internet and social media postings and content created on, transmitted to, received for printed from or stored or recorded on the Device for Firm's behalf is the property of Firm, regardless of who owns the Device.

The Firm reserves the right to monitor, intercept, review and or erase (in the case of BYOD Devices, Firm Information only), without further notice all content created on, transmitted to, received or printed from, or stored or recorded on the Device for Firm's business on behalf of Firm.

In the case of all Devices, use of a Device for Firm business or on behalf of Firm is at the User's own risk and Firm will not be responsible for any personal lost on a wiped, copied, edited, or erased Device.

Users should have no expectation of privacy whatsoever in any content created on, transmitted to, received or printed from, or stored or recorded on any Device, whether personally owned, or otherwise used for Firm business.

Device Security Requirements.

All Devices must be registered with the IT Administrator, or his/her designee, and in registering each Device, the User must provide

The name of his/her Device

The software currently installed on it

The Device's serial number

If applicable: the username associated with the Device

To protect Firm's Information from being lost or becoming public, a User must immediately report any Device that is lost, stolen, or has been accessed by unauthorized persons.

A User must promptly provide Firm with access to the Device when requested or required for Firm's legitimate business purposes, including in the event of any security incident or investigation.

The use of all Devices for Firm business must comply with this Policy and all other applicable Firm policies, procedures and requirements.

All Devices used for Firm business must have:

A strong password that complies with Firm's password policy; and

All appropriate software installed.

All Devices used for Firm business must not without authorization:

Download or transfer work product or sensitive business content, for example e-mail attachments (all information inadvertently downloaded must be immediately deleted).

Back up to cloud- based storage or services without Firm's prior consent.

Create a mobile Device hotspot without prior clearance from the IT Administrator, or his/her designee.

Transmit any Firm Information over an unsecure Wi-Fi network

Be accessed by anyone not authorized by Firm, including fellow business associates.

At all times Users must use their best efforts to physically secure a Device against physical loss, theft, or use by persons who have not been authorized to access the Device by Firm. Furthermore,

New Users who are using their own Devices under this policy must erase all information related to any previous employers before using their Devices for Firm business

Firm reserves the right to conduct periodical downloads of information stored on each Device

Any Users who disconnect use of their devise under this policy or leave Firm's employ must allow Firm to remove any relevant work product or sensitive business content from their Devices.

Device Technological Support.

For Users Operating under the BYOD Policy:

The Firm does not provide any technological support for physical or internal hardware damage to User-owned Devices. The User alone is responsible for any repairs, maintenance or replacement costs and services.

The Firm will only provide technical support involving Firm network authentication issues, login issues, and issues related to the Firm's multi-factor authentication process.

For Users Operating under the CYOD Policy:

The Firm will provide technical support for any wide spread manufacture, company, or distributor acknowledged external and or internal personal computing Device damages, faults, or malfunctions that lead to a recall and or discontinuation of that specific Device.

Other than the support previously mentioned, the Firm does not provide any technological support for physical or internal hardware damage to CYOD Devices. The User alone is responsible for any such out-of-coverage repairs, maintenance or replacement costs and services.

The Firm will only provide technical support involving Firm network authentication issues, login issues, and issues related to the Firm's multi-factor authentication process.

For Users Operating under the COPE Policy:

The Firm will provide technological support for all external and internal personal computing Device damages except the following:

Cosmetic scratches or wearing

Damages caused by operating the Device outside this Policy or its published guidelines

Damages caused by unwarranted external modifications and internal software modifications such as "jailbreaking".

Device Risks, Liabilities, Disclaimers.

The Firm will not be liable for the loss, theft, or damage of a Device. This includes, but is not limited to, when the Device is being used for Firm business, or during business travel.

The Firm reserves the right to implement technology such as Device management to enable the removal of Firm owned Information.

The Firm reserves the right to conduct the Device inspections previously mentioned in this policy on Users who are on any form of paid or unpaid leave.

XI. MONITORING.

In order to enforce this Policy, System Resource and Information usage may be monitored by the Firm, including retrieving and reading e-mail messages and other computer files, and monitoring of Internet traffic. Even though a User may be issued a private password or other private access code to log in to System Resources, including the Work Environment, a User should not have any expectation of privacy with regard to his/her use of the Firm's Information or System Resources.

The Firm reserves the right (but is under no obligation) to:

Access, review, audit and disclose the contents of all e-mail folders

Block harmful and offensive outgoing and incoming e-mail messages

Track Internet use and any other use of System Resources for the purpose of monitoring compliance with these policies or otherwise

Track Internet use and any other use of System Resources for the purpose of preventing the disclosure of sensitive or confidential information.

XII. USER COMPLIANCE AND BREACH.

Users should immediately notify either the IT Administrator, the Managing Partner, or other Executive Committee member(s) or his/her immediate supervisor regarding any violations (or suspected violations) of this Policy. Users who violate this Policy will be subject to disciplinary action, up to and including termination of employment, including any rights or remedies the Firm may have in law and equity.

The Firm may treat any attempt to bypass or circumvent security controls as a violation of this Policy. The Firm may deem failure to participate in required training a violation of this Policy. The Firm will retain attendance records and copies of security training materials delivered.

All Users should be aware that breaches of this Policy may in some cases also constitute a criminal or tortious act and result in the User being subject to criminal or civil liability charges or liability.

Suspected violations of this policy will be handled by Executive Committee and/or their designee, and will result in disciplinary action taken against the responsible Firm User. All requirements stated in this Policy apply to Users on any type of paid or unpaid leave. Users who are exiting the Firm or their relationship with the Firm, for any reason, must comply with the Firm's exit and data collection procedures stated in this Policy and all other relevant Firm policies.

XIII. RELEVANT CONTACTS.

IT Administrator: Gopal M. Burgher

Email: gburgher@burghergray.com

Telephone: (646) 513-3231, ext 102

System Administrator: Legal Workspace

24/7 Help Desk: (877) 713-8302, option 2

Email: helpdesk@legal-workspace.com

Executive Committee:

Gopal M. Burgher, Managing Partner

Sandra Honegan-Pounder, Partner

Director of Operations: Marcia Nieves

USER ACKNOWLEDGEMENT

I have read and been informed about the content, requirements, and expectations of the BurgherGray LLP (the "Firm") Information Technology and Data Security Policy & Procedures, dated [_____] (the "Policy") for Users of the Firm's System Resources, Work Environment and Information. All defined terms used in this Acknowledgment are as defined in the Policy.

I have received a copy of the Policy. As a User or potential User of the Firm's System Resources, Work Environment and Information, I understand that it is my responsibility to be familiar with the terms of the Policy and agree to abide by the Policy as a condition of my continuing employment, engagement or partnership with Burgher Gray Jaffe LLP. I understand that the Policy is intended to protect the Firm, its clients and other Users, when I access and use the Firm's System Resources, Work Environment and Information.

This Policy is not promissory and does not set terms or conditions of employment, engagement a continued relationship or creates an employment contract. I understand that the Firm may change, modify, suspend, interpret or cancel, in whole or part, the Policy, with or without notice to me, at its sole discretion, without giving cause or justification to any User, including myself. Such a revised Policy may supersede, modify or eliminate existing Firm policies. The Firm's Executive Committee shall have sole authority to add, delete or adopt revisions to this Policy.

I have read this Policy carefully, and, if directed by the Firm, participated in Firm-sanctioned IT security training, to ensure that I understand it before signing this document. I understand that if I have questions, at any time, regarding this Policy or my training, I will consult with my immediate supervisor, the office manager or a human resources staff member.

User's Signature: _____

Printed Name: _____

Date: _____