IT Policies

IT policies which govern acceptable use practices within the organization.

- Systems & Securities Policy
- Password Policy
- Assigned Equipment
  - Equipment for Home
  - Office-Based Equipment
  - Hardware Replacement
- Restrictions
  - Device Restrictions
  - Application Restrictions
  - Email Restrictions

Systems & Securities Policy

Currently under review

Telephone & Email

- Email signatures must conform to our company standard signature. If in doubt, please speak with the office manager.
- If the Company subsidizes your cell phone contract and/or if you give out your cell phone number to business clients or contacts, please ensure that you record a professional greeting on your mobile voicemail. This does not need to include our firm's name, however, at a minimum, you should include your first and last name and when you expect to be able to return the call.
- When you are away from the office or not intending to answer work-related voicemails, record an appropriate out-of-office message and/or activate your automated 'out of office reply' stating the dates of your absence and appropriate contact information for clients during your absence.

System Security

General system security practices at George & Bell include the following:

- Be sure to validate the source of all email attachments prior to opening.
- If considering emailing confidential data (as an attachment), see Section 3 below. If considering transferring such confidential data to a work colleague internally by email, *the same procedures as "external" (below)* ***must*** *be followed*; alternatively (and preferably), you may send a file link to our server by email.
- Immediately report any concerns about computer or file server / network to IT Support and please copy your responsible partner.

Transferring / Receiving Data Between G&B & External Entities

George & Bell uses LiquidFiles to send and receive files that include confidential data[1] in a convenient and secure manner. This web-based application's primary purpose is to replace insecure methods (email, postage, etc.) of moving confidential information between George & Bell and its clients.

Features include:

- Send confidential files to a client using LiquidFiles' build-in mailer interface or by sharing a link.
- Request files from a client. The client sees a simple and easy-to-use interface for uploading the requested file. No signup is required on the client's part.
- Provide a permanent URL to clients who regularly need to upload confidential files.
- Store a collection of files accessible by any team member for easy distribution.

Each employee receives an email from LiquidFiles asking to complete the signup process. If you did not receive this message please email IT Support.

To access the LiquidFiles service, go to and bookmark: https://transfer.georgeandbell.com. For information on how to use LiquidFiles please see LiquidFiles' User Guide.

[1] Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Personal data of clients/partners/vendors/members (e.g., files including names, SINs, addresses, health information, etc.)
- Client lists (existing and prospective)

Working from Home & Security

To ensure the security of our client data and related information, work must only be performed on George & Bell-owned computers / laptops[1]. If you are not physically in the office, access client files through a secure VPN connection (from your George & Bell computer only).

Furthermore:

- Please ensure that when you leave the office, you either take your laptop with you or lock it in your desk or some other secure location. Similarly, when working from other locations, care should be taken as to the accessibility of your laptop by non-G&B employees.
- If working from the office, it is up to the employee as to whether you take your laptop home every night. We encourage employees to take their laptop home if:
  - There's a good chance that getting to the office the next day may be an issue;

    - It would be beneficial for their health/the health of the office to work from home the next day; or
    - There are other reasons why working from home would be beneficial to the employee/the office.

[1] If you need to conduct work and you do not have access to a George & Bell computer and VPN connection, you should contact your manager or a Partner to discuss how to proceed.

Physical Security

- Lock your screen when you temporarily leave your computer (hold windows button and hit "L" on keyboard).
    - The same considerations with respect to the security of your laptop, as described above, apply to any cellphone you use for work purposes, in particular if such cellphone includes work-related emails, messaging apps (e.g., Microsoft Teams), client files, etc.
    - "Locking screens" requires that a "strong" password must be used to regain access. [Note: a strong password on your cellphone is *not* four digits.]
- Ensure all doors to our office are always kept locked (including front, side, and patio doors).
- Do not lend your office key or building passes to any non-G&B employees.
- Should you notice suspicious persons loitering on our floor or near our office, contact Building Security immediately (778-838-8625).
- All office desks are to be cleaned at the end of each day and any physical files are to be locked in a drawer at the end of the day.
- Report stolen or damaged equipment to the office manager and our IT Consultant as soon as possible.
    - All account passwords should be changed at once when a device is stolen; contact our IT Consultant for further instructions.
- Review the COVID-19 Workplace Safety Policy for safety/security recommendations specific to the COVID-19 pandemic.

Archiving

- To remove and secure past email messages which may have contained sensitive and/or confidential information from Microsoft Office 365, please configure and enable the AutoArchive feature within Microsoft Outlook.

- Once enabled, all email messages older than 6 months will be removed from your Microsoft Office 365 account and stored locally within a PST file on your laptop. It will be accessible even if you are not connected via VPN and it will also be backed up (as it is stored within Documents which gets synchronized with the file server anytime the VPN is connected). Email messages stored within the archive will no longer be accessible via your mobile device or through a web browser; only via your Outlook client.

- Please refer to the Configuring AutoArchive guide to walk you through the set-up process.

Phishing

To further enhance the firm’s cyber defenses, increased attention should be paid to some very common types of cyber-attacks. “Phishing” is the most common type of attack that affects organizations. The goal of these attacks is getting you to share sensitive information such as login credentials, credit card information or other sensitive information. Listed below are a few tips to help you spot such attempts.

1. Do not click on any links or attachments from senders you do not recognize.
2. Do not provide sensitive personal information such as usernames, passwords, or credit card information over email/text/messaging apps.
3. Inspect URLs carefully to make sure they are legitimate.
4. Always check the sender’s email address to confirm that no alterations have been made such as additional numbers, letters, or a different domain.
5. Many phishing emails also contain a lot of spelling and grammar errors.
6. Do not try to open documents that you are not expecting to receive.
7. Rely on our message header (see below) that shows if the email is from an external sender. If the sender is purporting to be someone who works for George & Bell, their message will NOT have this header.
8. Written instructions/directions from fellow G&B team members will generally be sent to you via email or Microsoft Teams. It is *very* rare that you would be given instructions (particularly instructions to purchase goods/services or grant access to our server or confidential client information) through any other applications (like FB messenger, WhatsApp, Signal, etc.) If you do receive instructions via this medium, you should confirm by speaking to the sender in person before acting on any instructions.
9. If you are unsure about any instructions received by e-mail or Microsoft Teams from a G&B team member, call that person or ask your manager for help.
10. Let your instincts and common-sense help protect you.

All employees will be required to complete information security training upon hire. Furthermore, all employees will be subject to ongoing phishing testing on a regular basis and the results of the same will be reported to the partners for further action as necessary.

Please do not hesitate to contact IT Support if you have any concerns regarding an email or attachment.

Password Policy

The following policy outlines the password requirements employees must follow in order to ensure their accounts remain secure and uncompromised.

> Please see the section *Password Generation Recommendations* on how to easily generate a secure and memorable password.

> There will be no regular interval at which a password change will be required. However, should you suspect that your account has been compromised, in conjunction with discussions with our IT provider, you should reset your password.

Domain Credentials

Domain credentials are used to logon to the majority of George & Bell's services including:

- Laptop Logon
- Microsoft Office 365 account
- Office Wireless
- LiquidFiles
- FortiClient VPN

Password Requirements

- Must be a unique password not used on any other service or device.
- Minimum 20 characters in length.
- Does not require a mix of uppercase, lowercase and symbols.
- Spaces can be used.

1Password Master Password (Still to be released)

Your Master Password is used to logon to your 1Password account.

Password Requirements

- Must be a unique password not used on any other service or device.
- Minimum 20 characters in length.
- Does not require a mix of uppercase, lowercase and symbols.
- Spaces can be used.

Client/Other Service Provider Credentials

Client credentials include any services or account you use to access on behalf of a client. These services can include:

[list of common client services]

Password Requirements

- Must be a unique password not used on any other service or device.
- Minimum 20 characters in length or the maximum character length if 20 characters is not supported.
- Mix of uppercase and lowercase characters.
- Randomly generated via 1Passwords password generator.

Password Generation Recommendations

For your 1Password and domain credentials, its recommended that your passwords be either a grouping of easily memorable words or a short sentence. For example (but please don't use):

- flattered moneywise trade
- rebuff pulse richly
- banner antiquely postbox
- The thin blue mountains reflected off of the sunset.
- The green lizards jumped towards the passing flies.

All of the above are easily memorized but incredibly difficult to guess.

To generate a new memorable password, feel free to use a password generator such as https://www.useapassphrase.com On online password generator is an easy way to create difficult to guess passwords without having to put much thought into them.

If opting to come up with your own password, please avoid names, places or numbers that are associated with you, your family or the company. For example don't include any of the following:

- Personal or company address.
- Personal or company phone number.
- Company name.
- Children or pet names.
- Dates associated with a special occasion (wedding, birthday etc.).

Assigned Equipment

Outlines what equipment each employee can expect when employed with George & Bell Consulting and how equipment is handled through its lifecycle.

Equipment for Home

Every employee of George & Bell, upon employment is provided with a predefined set of equipment for use when working from home. Below outlines what equipment each employee's is entitled.

Fully Remote Employees

For employees who work 100% remotely and rarely come into one of George & Bell's offices.

- 1x Laptop
- 2x 24" Monitors
- 1x Docking Station
- 1x Keyboard/Mouse
- 1x Power Bar

Hybrid Employees

For employees who work both from home and out of an office on a defined schedule, two options are available. Employees may only select one option.

- 1x Laptop
- 2x 24" Monitors
- 1x Docking Station
- 1x Keyboard/Mouse
- 1x Power Bar

or

- 1x Laptop
- 1x 27" Monitor with built-in Docking Station
- 1x Keyboard/Mouse
- 1x Power Bar

Office-Based Equipment

Each desk at George & Bell is provided with a predefined set of equipment for use when working in the office. Below outlines what equipment each desk will be outfitted with.

- 2x 22" or 24" Monitors (1080p resolution)
- 1x Docking Station
- 1x Keyboard/Mouse
- 1x Power Bar or UPS

It is asked that employees do not remove or move equipment between desks as all desk equipment is tracked. If you find that a piece of equipment is damaged, please contact IT Support and let them know.

Assigned Equipment

Hardware Replacement

IT-based equipment at George & Bell Consulting is replaced per the schedule below or when deemed necessary by the IT department. Early replacement is allowed if the hardware is defective or damaged and approval has been given both by the partners and the IT department. Valid reasons for early replacement include:

- Flickering or heavily scratched screen.
- Worn out or defective keyboard/mouse.
- Incompatible docking station due to laptop change.
- Power bar which has been damaged or no longer provides surge protection.

Hardware	**Replacement Cycle**
Laptop	5 Years
Monitor	10 Years
Docking Station	As needed
Keyboard/Mouse	As needed
Power Bar	As needed

Requesting Hardware Replacement

If you have equipment that requires replacement, please reach out to IT Support outlining what equipment needs replacement and what issues you're experiencing with this equipment. Replacement are provided upon approval from the IT department and the partners.

Restrictions

Device Restrictions

Removeable Storage Media

To eliminate the possibility of having a laptop compromised via removable storage media such as a USB flash drive or an external hard drive, the following removable storage media is blocked if connected to a company laptop:

- USB Flash Drives
- External Hard drives
- Memory Cards
- Digital Cameras
- Smart Phones (charging is not affected)

Restrictions

Application Restrictions

Currently employees have full administrative access to their laptop, allowing for any application to be installed without approval. Due to the risk of infection leading to data breach or account compromise, its asked that employees only install applications which are relevant to their job.

The following types of applications are not permitted to be installed on laptops:

- Remote access software (TeamViewer, LogMeIn etc.)
- Games
- VPN clients (Nord VPN, SurfShark etc.)
- Applications used solely for personal use.
- Application from unknown developers (random applications from SourceForge for example).
- Applications which have not been digitally signed.

If you are unsure if an application you require is permitted or not, please contact IT Support for confirmation before installing.

Email Restrictions

Attachments

Any email message with the following attachment filetypes will be blocked upon being received by Microsoft 365. The sender will be notified via a NDR (non-deliverable report) indicating that the email was not delivered due to the email including a banned filetype.

.ace	.ani	.apk	.app	.appx	.arj	.bat	.cab
.cmd	.com	.deb	.dex	.dll	.docm	.elf	.exe
.hta	.img	.iso	.jar	.jnlp	.kext	.lha	.lib
.library	.lnk	.lzh	.macho	.msc	.msi	.msix	.msp
.mst	.pif	.ppa	.ppam	.reg	.rev	.scf	.scr
.sct	.sys	.uif	.vb	.vbe	.vbs	.vxd	.wsc
.wsf	.wsh	.xll	.xz	.z	.ppsm	.xlsm	

Receiving Blocked Files

If you require a file that would be blocked by the above restriction, and that file is coming from a trusted source, please ask that the individual provide you the file via the LiquidFiles service.