GAI Cyber Security Policy

March 2021

Introduction
The Guild's information is an important asset. It must be protected from the consequences of breaches of confidentiality, failures of data integrity and interruptions to its availability. The Guild must therefore take appropriate organisational and technical measures to protect its information.

Purpose
Our company cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.
The policy aims to minimise potential damage to the Guild by reducing the number and impact of information security incidents. The measures set out in this policy, including training requirements, are mandatory.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human errors, hacker attacks and system malfunctions could cause great financial damage and may jeopardise the Guild's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope
This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Elements

Confidential data
Confidential data is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/members
- Examination results/questions
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protect personal and company devices
When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise GAI employees to keep both their personal and company-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all devices password protected.
- Choose and upgrade a complete antivirus software (we provide this for company devices).
- Ensure they do not leave their devices exposed or unattended.
- Install security updates of browsers and systems weekly or as soon as updates are available.

- Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new employees receive company-issued equipment they will receive instructions for password management. They should follow instructions to protect their devices and refer to our IT service providers if they have any questions. If using your own devices to access the GAI's networks, ensure that your device is kept up to date, is secure, and does not access any sensitive or confidential information held on our networks.

Keep emails safe
Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing")
- Be suspicious of clickbait titles (e.g. offering prizes, advice)
- Check email and names of people they received a message from to ensure they are legitimate
- Look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks)

If an employee isn't sure that an email they received is safe, they can refer to our IT service provider.

Manage passwords properly
Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advice our employees to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays, names of family members/pets)
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Change their passwords every two-three months.

Transfer data securely
Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our IT service provider for help.
- Share confidential data over the company network/ system and not over public Wi-Fi – use a VPN or company phone if travelling
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies
- Report scams, privacy breaches and hacking attempts

Our IT service provider needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT service provider must investigate promptly, resolve the issue and send a companywide alert when necessary.

Our IT service provider are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

Additional measures
To reduce the likelihood of security breaches, we also instruct our employees to:

- Turn off their screens and lock their devices when leaving their desks
- Report stolen or damaged equipment as soon as possible to your line manager
- Change all account passwords at once when a device is stolen
- Report a perceived threat or possible security weakness in company systems
- Refrain from downloading suspicious, unauthorised or illegal software on their company equipment
- Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy. All employees have a responsibility not to compromise the company for example by sending defamatory or harassing electronic mail, or by making unauthorised purchases, and must also be aware that the confidentiality and integrity of information transmitted by email and other means may not be guaranteed.
Our IT service provider has installed firewalls, anti-malware software and access authentication systems, and informs employees of any new scam emails or viruses and how to combat them.
GAI has all physical and digital shields to protect information.

Remote employees
Remote employees (working from home or 'on the road') must follow this policy's instructions too. Since they will be accessing GAI's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage them to seek advice from our IT service provider if unsure.

Disciplinary action
We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and re-train the employee on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination. We will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face disciplinary action, even if their behaviour hasn't resulted in a security breach.

Take security seriously
Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

STAFF TRAINING: 10 Cybersecurity Best Practices
Cybersecurity best practices encompass some general best practices — like being cautious when engaging in online activities, abiding by company rules, and reaching out for help when you encounter something suspicious. Here's a deeper dive into the 10 cybersecurity best practices for businesses that every employee should know and follow.

1. Protect your data

In your daily life, you probably avoid sharing personally identifiable information like your Social Security number or credit card number when answering an unsolicited email, phone call, text message, or instant message. It's important to exercise the same caution at work. Keep in mind that cybercriminals can create email addresses and websites that look legitimate. Scammers can fake caller ID information. Hackers can even take over company social media accounts and send

Companies may also require multi-factor authentication when you try to access sensitive network areas. This adds an additional layer of protection by asking you to take at least one extra step — such as providing a temporary code that is sent to your smartphone — to log in. Two factor Authentication should be set up on Guild accounts for social media and key systems.

computer screen in the background, you could accidentally reveal information someone outside the company shouldn't see.

By the same token, be careful to respect the intellectual property of other companies. Even if it's accidental, sharing or using the IP or trade secrets of other companies could get both you and your company into trouble.

The Guild aims to protects its employees, customers, and data. Destroy data thoroughly – shred paper, delete files and wipe USB drives. Ensure you report suspicious emails or ransomware to our IT support company.

2. Avoid pop-ups, unknown emails, and links

Beware of phishing. Phishers try to trick you into clicking on a link that may result in a security breach.

Phishers prey on employees in hopes they will open pop-up windows or other malicious links that could have viruses and malware embedded in them. That's why it's important to be cautious of links and attachments in emails from senders you don't recognize. With just one click, you could enable hackers to infiltrate your organization's computer network.

Here's a rule to follow: Never enter personal or company information in response to an email, pop-up webpage, or any other form of communication you didn't initiate. Phishing can lead to identity theft. It's also the way most ransomware attacks occur.

The Guild uses email authentication technology that blocks these suspicious emails. You'll usually be notified that the email has been sent to a quarantine folder, where you can check to see if it's legitimate or not.

Be cautious. If you're unsure about the legitimacy of an email or other communication, always contact the IT provider.

3. Use strong password protection and authentication

Strong, complex passwords can help stop cyberthieves from accessing company information. Simple passwords can make access easy. If a cybercriminal figures out your password, it could give them access to the company's network. Creating unique, complex passwords is essential.

A strong password contains at least 10 characters and includes numbers, symbols, and capital and lowercase letters. You should also change your passwords on a regular basis. Changing and remembering all of your passwords may be challenging - a password manager can help.

Companies may also require multi-factor authentication when you try to access sensitive network areas. This adds an additional layer of protection by asking you to take at least one extra step — such as providing a temporary code that is sent to your smartphone — to log in. Two factor Authentication should be set up on Guild accounts for social media and key systems.

4. Connect to secure Wi-Fi
The Guilds office Wi-Fi network is secure and encrypted. If you're working remotely, you can help protect data by using a virtual private network such as provided by a 'mi-fi' router, or your work smartphone. A VPN is essential when doing work outside of the office or on a business trip. Public Wi-Fi networks can be risky and make your data vulnerable to being intercepted.

5. Enable firewall protection at work and at home
GAI employs a firewall for the company network, but your home network is a first line of defence in helping protect data against cyberattacks. Firewalls prevent unauthorised users from accessing websites, mail services, and other sources of information that can be accessed from the web.

6. Invest in security systems
The Guild has invested in protections such as strong antivirus and malware detection, external hard drives that back up data, and running regular system checks.
All of the devices you use at work and at home should have the protection of strong security software such as eSet. Alert our IT provider if you see anything suspicious that might indicate a security issue. There may be a flaw in the system that needs to be patched or fixed. The quicker you report an issue, the better.

7. Install security software updates and back up your files
Following IT security best practices means keeping your security software, web browsers, and operating systems updated with the latest protections. Antivirus and anti-malware protections are frequently revised to target and respond to new cyberthreats, so make sure your computer and work smart phone is set to update automatically.

If your company sends out instructions for security updates, install them right away. This also applies to personal devices you use at work. Installing updates promptly helps defend against the latest cyberthreats.

Cyberthreats often take aim at your data. That's why it's a best practice to secure and back up files in case of a data breach or a malware attack. The Guild backs up important files offline on an external hard drive and in the cloud.

8. Talk to your IT department
Your IT department is your friend. Reach out to our IT support team about information security if you have concerns.

It's also smart to report security warnings from your internet security software to IT. They might not be aware of all threats that occur.

It's also important to stay in touch when traveling. Let our IT support team know before you go abroad, especially if you're forced to use public Wi-Fi. Have a great trip — but don't forget your VPN.

Remember to make sure IT is, well, IT. Beware of tech support scams. You might receive a phishing email from someone claiming to be from IT. The goal is to trick you into installing malware on your computer or mobile device, or providing sensitive data. What to do? Don't provide any information. Instead, contact our IT provider right away.

9. Employ third-party controls
Here's a fact that might be surprising. It's common for data breaches to begin from within companies. That's why organisations need to consider and limit employee access to customer and client information.

You might be an employee in charge of accessing and using the confidential information of customers, members, and other employees. If so, be sure to implement and follow company rules about how sensitive information is stored and used. If you're in charge of protecting hard or soft copies, you're the defender of this data from unauthorised third parties. You may also have to monitor third parties, such as consultants or former employees, who have temporary access to the organisation's computer network. It's important to restrict third-party access to certain areas and remember to deactivate access when they finish the job.

10. Embrace education and training
We want you to be aware of how to keep our data safe. Your responsibility includes knowing your company's cybersecurity policies and what's expected of you. That includes following them. If you're unsure about a policy, ask.

Here's an example. Maybe you wear a smart watch at work. It's important to protect personal devices with the most up-to-date security. You'll also want to know and follow your company's Acceptable Electronic Use (AEU) policy. When you Bring Your Own Device — also known as BYOD — ask your IT department if your device is allowed to access corporate data before you upload anything to it. Always be sure to use authorized applications to access sensitive documents.

A little technical savvy helps, too. Learning the process for allowing IT to connect to your devices, along with basic computer hardware terms, is helpful. That knowledge can save time when you contact support and they need quick access and information to resolve an issue.

Undertake some training – see **Stay Safe Online Top Tips for Staff (ncsc.gov.uk)** for a video
If you want to back up data to the cloud, be sure to talk to your IT department first for a list of acceptable cloud services – we use Microsoft OneDrive and Sharepoint. Do not store work data elsewhere unless specifically authorised to do so. Violation of this policy might be a cause for dismissal.

You can prevent a data breach
Having the right knowledge - like the cybersecurity best practices that every employee should know - helps strengthen the Guild against the possibility of attack. Remember, just one click on a corrupt link or a failure to update your system could let in a hacker or leave us vulnerable to cyberattack.

It's part of your job to engage in safe online behaviour and to reach out to your IT department when you encounter anything suspicious or need help.
Staying on top of these cybersecurity practices could be the difference between a secure company and one that a hacker might target.