INSIGHT
INVESTMENT PARTNERS

Cyber Security Policy

Version	**1.0**
Last updated	**10.05.2022**

AIM OF THIS POLICY

This policy outlines the guidelines and provisions for preserving the security of data and technology infrastructure.

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 jeopardize our company'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.

APPLICATION OF THIS POLICY

This policy applies to all Representatives of Insight Investment Partners and their employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

YOU MUST:

- Keep all devices password protected.
- Ensure you do not leave devices exposed or unattended.
- Install complete antivirus software.
- Log into company accounts and systems through secure and private networks only
- Utilise the services of a password management tool which generates and stores passwords. Examples of such tools are iC2 Password Management, LastPass, Password Keeper, Practice Protect.
- Immediately report any security or privacy breach to your Compliance Manager

Protect personal and company devices

When using digital devices to access company emails or accounts, they introduce security risk. We advise all Representatives of Insight Investment Partners and their employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware 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.
- Install complete antivirus software.
- Ensure you do not leave devices exposed or unattended.
- Install security updates of browsers and systems monthly or as soon as updates are available.
- Log into company accounts and systems through secure and private networks only.
- We also advise you to avoid accessing internal systems and accounts from other people's devices or lending your devices to others.

Keeping emails safe
Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct all Representatives of Insight Investment Partners and their employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware 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 give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

Managing 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 advise 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.)
- Remember passwords instead of writing them down. Should you need to write a password, you are obliged to keep the paper or digital document confidential and destroy it you're your work is done.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the phone instead of email, and only if they personally recognise the person they are talking to.
- Utilise Two Factor Authentication (2FA) where available.

Remembering a large number of passwords can be daunting. It is highly recommended you utilise the services of a password management tool which generates and stores passwords. Examples of such tools are iC2 Password Management, LastPass, Password Keeper.

Employees are obliged to create a secure password for the tool itself, following the abovementioned advice.

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

- Avoid transferring sensitive data (e.g. client information) to other devices or accounts unless absolutely necessary.
- Share confidential data over the company network/ system and not over public Wi-Fi.
- Ensure that the recipients of the data are properly authorised people or organizations and have adequate security policies.
- Immediately report scams, privacy breaches and hacking attempts to your Compliance Manager.

Additional measures
To reduce the likelihood of security breaches, we also instruct all Representatives of Insight Investment Partners and their employees, contractors, volunteers and anyone who has permanent or temporary access to our systems to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to your Compliance Manager.
- Change all account passwords at once when a device is stolen.

- Report a perceived threat or possible security weakness in company systems to your Compliance Manager
- Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
- Avoid accessing suspicious websites.

Working From Home and Remote Employees or Contractors

When working from home or engaging remote employees or contractors, you must ensure you follow this policy's instructions. Since they will be accessing our systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Reporting Security & Privacy Breaches

You must immediately report any security or privacy breach to your Compliance Manager. You are able to raise a new breach using the Compliance Hub in the iC2 App. Alternatively, you are able to email your Compliance Manager directly.

Take security seriously

Everyone, from our clients and partners to 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.