Stuart Jary
28 October 2019

Insolvency Practitioners Association

Data and Information Security Policy

1. Introduction

i. This IT security policy helps us:

- Reduce the risk of IT problems
- Plan for problems and deal with them when they happen
- Keep working if something does go wrong
- Protect company, client and employee data
- Keep valuable company information, such as plans and designs secret
- Meet our legal obligations under the General data protection regulation and other laws
- Meet our professional obligations towards our clients and customers
- Provide the ability to receive, store & disseminate intelligence and confidential information

ii. IT security problems can be expensive and time-consuming to resolve. Prevention is much better than cure

2. Responsibility

i. All staff have the responsibility of ensuring that they are adhering to the rules and regulations within this policy and taking appropriate actions when necessary.

ii. Sarah Munroe has day-to-day operation responsibility for implementing this policy. Whilst Sarah is on maternity leave, her replacement Donna Cullen will hold the day-to-day operational responsibility

iii. Any issues on confidential information as they apply to Money Laundering disclosures remain the responsibility of Andrew Kerr as the IPA Single Point of Contact ('SPOC'), David Holland as the IPA MLRO and Saira Mirza and Stuart Jary as the Deputy SPOCs for the IPA. Money Laundering in relation to this policy is at part 14 below.

iv. Server Consultancy and Progmatec is the IT organisation's that we use to help with our planning and support

v. Sarah Munroe is the data protection officer to advise on data protection and best practices.

vi. Sarah Munroe is the director with overall responsibility for IT security strategy.

3. Review Process

i. The IPA will review this policy annually

ii. In the meantime, if you have any questions, suggestions or feedback, please contact Sarah Munroe on 020 7397 6407 or by e-mail; sarahm@ipa.uk.com

4. Information Classification

i. We will only classify information which is necessary for the completion of our duties. We will also limit access to personal data to only those that need it for processing. We classify information into different categories so that we can ensure that it is protected properly and that we allocate security resources appropriately:

- **Unclassified**: This is information that can be made public without an implications for the company, such as information that is already in the public domain
- **Employee Confidential**: This include information such as medical reports, pay and so on
- **Company Confidential**: Such as contracts, business plans, passwords for critical IT systems, client contact records, accounts etc
- **Client Confidential**: This includes personal identifiable information such as name or address, passwords to client systems, market sensitive information etc

5. Access Controls

i. Internally, as far as possible, we operate on a ‘need to share’ rather than a ‘need to know’ basis with respect to company confidential information. This means that our bias and intention is to share information to help people do their jobs rather than raise barriers to access needlessly.

ii. As for client information, we operate in compliance with the GDPR 'Right to Access. This is the right of date subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose. Further, we shall provide, upon request, a copy of their personal data, free of charge in an electronic format.

6. Security software

i. To protect our data, systems, users and customers we use the following systems and processes:

- **Laptop and desktop anti-malware, Server anti-malware, intrusion detection and prevention, desktop firewall** – This is protected by Symantec.cloud Endpoint Protection Small Business Edition which is installed on every employee's laptop. This is renewed and reviewed on an annual basis.

- **Cloud-hosted email spam, malware and content filtering** as well as **email archiving and continuity** is protected by office 365 which is renewed and reviewed on an annual basis.

- **Data protection and Encryption** – All staff have had GDPR training provided through a company called Harlequin which emphasised the need for data protection and password encryption on all files containing sensitive data.

- The IPA also has an **in-house firewall** which has **Intrusion Prevention System** (IPS) enabled. Its WatchGuard firewall (red colour box) is currently placed in the server cabinet.

7. Employees joining and leaving

i. When a new employee joins the company, we will add them to the following systems:

- CRM
- Microsoft Office
- Sharepoint
- Website – Membership team only
- Social media – Membership team only
- Sage - Finance team only
- Bank systems – Finance team only

ii. The IPA will provide training to new staff and support for existing staff to implement this policy.

iii. This includes:

- An initial introduction to IT security, covering the risks, basic security measures, company policies and where to get help.
- Training on how to use company systems and security software properly
- On request, a security health check on their computer, tablet or phone

iv. When people leave a project or leave the company, we will promptly revoke their access privileges to company systems.

8. Staff responsibilities

i. Effective security is a team effort requiring the participation and support of every employee and associate. It is your responsibility to know and follows these guidelines.

ii. You are personally responsible for the secure handling of confidential information that is entrusted to you. You may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of your duties. Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to Sarah Munroe.

9. Staff own device(s)

i. It is also your responsibility to use your devices (computer, phone, tablet etc) in a secure way. However, we will provide training and support to enable you to do so (see below).

At a minimum:

- Remove software that you do not use or need from your computer
- Update your operating system and applications regularly
- Keep your computer firewall switched on and any other virus applications
- Store files in official company storage locations so that it is backed up properly and available in an emergency
- Understand the privacy and security settings on your phone and social media accounts
- Keep your work computer separate from any family or shared computers
- If you have access to an administrator account, do not use this on your computer for everyday use
- Make sure your computer and phone logs out automatically after 15 minutes and requires a password to log back in

10. Password Guidelines

- Change default passwords and PINs on computers, phones and all network devices – This should be done when on indication or suspicion of compromise.
- Don’t share your passwords with other people or disclose them to anyone else
- Don’t write down PINs and passwords next to computers and phones
- Use strong passwords which as a rule should consist of a mixture of letters (upper and lower case), numbers and symbols.
- Don’t use the same password for multiple critical systems
- Factory setting passwords should always be changed to something else which falls within the strong password bullet point.
- Passwords should never be written down therefore if you are struggling to remember various passwords, save them all into one document which is password protected.

11. Be alert to other security risks

i. While technology can prevent many security incidents, your actions and habits are also important.

ii. With this in mind:

- Take time to learn about IT security and keep yourself informed. Get safe online is a good source for general awareness *https://www.getsafeonline.org/*
- Use extreme caution when opening email attachments from unknown senders or unexpected attachments from any sender
- Be on guard against social engineering, such as attempts by outsiders to persuade you to disclose confidential information including employee, client or company confidential information. Fraudsters and hackers can be extremely persuasive and manipulative
- Be wary of fake websites and phishing emails. Don't click on links in emails or social media if you are not certain of its origin. Don't disclose passwords and other confidential information unless you are sure you are on a legitimate website
- Use social media in a professional and responsible way without violating company policies or disclosing confidential information
- Take particular care of your computer and mobile devices when you are away from home or out of the office
- If you leave the company, you will return any company property, transfer any company work-related files back to the company and delete all confidential information from your systems as soon as is practicable
- Where confidential information is stored on paper, it should be kept in a secure place where unauthorised people cannot see it and destroyed in confidential bins when no longer required

iii. The following things (amongst others) are, in general, prohibited on company systems and while carrying out your duties for the company may result in disciplinary action:

- Anything that contradicts the company policies
- Bypassing user authentication or security of any system, network or account
- Downloading or installing pirated software
- Disclosure of confidential information at any time

12. Information on external stakeholders

i. Any reports whether produced internally or externally which contain information regarding external stakeholders should be stored on the IPA's CRM system or the relevant folder in the share point system. The person who is involved in overseeing the particular report is responsible for ensuring that this is stored correctly.

ii. The IPA is utilising up to date secure cloud technology with enhanced security features. Any information relating to an external stakeholder should only be stored on record for a maximum of 6 years.

iii. If it is to be found that this type of information has not been handled correctly, then please report this matter to Sarah Munroe.

13. Backup, disaster recovery and continuity

i. There is a disaster recovery plan in place that covers backup and continuity which has been e-mailed to all staff and has also been saved in the 'housekeeping' file.

ii. Under GDPR, where a data breach is likely to result in a 'risk for the rights and freedoms of individuals' we must notify the customers and data controllers 'without undue delay'. We will ensure we inform them within 72 hours.

14. AML (Anti-money laundering)

i. Definition – Processes by which proceeds of crime are controlled and disguised, so that money can be spent freely without arrest

ii. Examples of AML in which staff need to be vigilant about are:

a) Identifying someone who is opening accounts at lots of different banks, depositing little cash at a time.

b) Identifying someone who is getting associates to deposit money and then transferring to criminals

c) Identifying someone who is using businesses to deposit cash at the bank along with normal takings

d) Identifying someone who is agreeing on purchase of investment and then concocting an explanation for needing to pay in cash

iii. Staff Responsibilities – We as members of staff at the IPA need to question cash deposits and how assets are bought in the first place. As a regulatory body, the IPA need to ensure firms we supervise operate policies and procedures in compliance with legislation.

iv. Staff are responsible for following AML procedures and reporting suspicions by adhering to the IPA AML Policy circulated and the Suspicious Activity Internal Reporting ('SARS') policy also circulated to all staff.

v. Staff are also reminded to ensure that they review the IPA Whistleblowing policy which provides details of how to make a disclosure that will be dealt with anonymously and confirms that information on the dedicated e-mail for whistleblowing is only able to be reviewed by the MLRO, SPOC and Deputy SPOCs.

vi. Information provided in respect of AML – either via a SAR, intelligence or a whistleblowing disclosure is held by the MLRO on a secure database and access to that database is restricted to the MLRO

vii. The IPA has also signed up the SIS system for AML intelligence and access to this database is held by the MLRO and Deputy SPOCs only. The information to be disseminated will be disciplinary sanctions and warnings issued to members and any intelligence on members that is in the public domain

viii. The obligations of the IPA members of staff with regards to AML are as follows:

- **Client Due Diligence (CDD) -** Under AML regulations, before the IPA can take on any new clients the following processes need to be adhered to and documented. This will allow the IPA to decide what level of due diligence needs to be applied from the outset

  - ✓ Assess risk of taking on new client by verifying ID and carrying out company searches on the business.

- ✓ Verify ID - For example passport or driving licence. It is the IPA's duty of care to ensure that the documents have not been tampered with and that the appearance is consistent with the person's date of birth.
- ✓ Know clients business – By carrying out a company search and verify identification of directors and significant shareholders. Obtain a certified copy of trust deed and extracts from it and verify identification of settlors, trustees and beneficiaries.
- ✓ Monitor – Visits are carried out by the inspection team once every two years which will allow the monitoring of AML regulations to be carried out.

- **Keeping records –** Under GDPR rules, the type of documents which are required to be checked to carry out the above works are legally allowed to be kept on files. Other documents that the IPA can keep on file are client instructions and financial instructions with dates, amounts, payers and/or payees

- **Reporting suspicions** – Any suspicions should be reported to the Money Laundering Reporting Officer (MLRO), David Holland using the IPA's secure systems as the information transported will be extremely confidential.

15. Sensitive personal information

i. The law requires that extra care should be taken when handling any of the following information. As the IPA do not have a procedure on this, then the below information should not be recorded in any circumstance:

- Racial/ethnic background
- Religious beliefs/affiliations
- Political views or trade union membership
- Physical/mental health and medical history
- Sexual orientation or activity
- Genetic/biometric data
- Criminal offences – convicted or alleged

ii. If you have any questions regarding AML, please contact the IPA money laundering reporting officer (MLRO).

16. AML Policies

i. For all staff that carry out activity on AML should refer to the IPA AML polices when carrying out this type of work, for example whistleblowing process, criminal reporting responsibilities (also contained within this policy) and escalation polices. These can be found on the IPA website where a specific page has been set up for AML. The page will be reviewed to ensure that it is kept up to date with current rules and regulations.

17. Data Security

i. As an IPA employee, before keeping any information relating to external stakeholders you should questions yourself on the following:

- ✓ Is the information needed?
- ✓ It is accurate?
- ✓ It is suitable for people to see?
- ✓ It is secure?

ii. To eliminate data security risks as specified under GDPR the IPA has procedures in place to ensure that we are correctly adhering:

- **Make sure data is backed up in case of system failure** – Now that all documents are saved in the cloud service means that risk is eliminated in case of a system failure and any documents going forward should always be saved on the shared drive. In exceptional circumstances where certain systems are still being saved on to the drive i.e. Sage, a backup of this is taken twice a day by the IPA IT maintenance company, Server Consultancy.
- **Ensure data is destroyed if no longer needed** – The IPA has secure bins in the office for confidential waste and for home workers the employee is responsible for secure disposal.
- **Keep personal data safe from people who are not allowed to see it** – Printers are regularly monitored and if papers are found, they are immediately destroyed. There are also locked cabinets, pedestals and a safe available for confidential documents to be stored.
- **Any memory sticks should be locked in drawers** Memory sticks and data discs can easily get lost, please ensure that these are cleared when the data is no longer required and locking them away when not in use.
- **Sensitive data files being sent in the post to the wrong person** –This is a risk and therefore postage of these type of documents should only be on a last resort basis and should in every instance possible be e-mailed securely. Any type of document that is e-mailed containing sensitive data must be encrypted with a password and two factor authentications. The password relating to the document must then be sent in a separate e-mail to the original document e-mail.
- **Laptop left in public place** – This is also a major risk and therefore all laptops are encrypted with passwords and two factor authentication enabled so that if this situation does arise then it will be very difficult for someone to gain access.

Server Consultancy should also be notified as soon as the situation arises so that can take the necessary action.

- **Only hold information about someone for legitimate business purposes** – all staff have been given training on data security which is to be updated on an annual basis. If you have any questions relating to this, please contact Sarah Munroe for guidance and refer the notes in this document.

18. Sending personal data to another person

i. Before sending anything that includes personal or confidential training, you need to consider both the means by which you send it, and whether you should be sending it at all.

- **Communicating to other parties** – Never provide personal information to another party, whether inside or outside of the IPA organisation without first checking that they are authorised to receive it.
- **Sending personal data outside the EU** – GDPR prohibits the sending of personal data to countries that don't have equivalent standards so if you need to send outside of the EU, so if you need to send data outside the EU, you must first check the correct procedure to follow.
- **Sending securely** – To ensure that your documents are being sent securely, all documents should be encrypted with a password and the password being sent in a separate document to the original e-mail (please refer to point 16ii in this document). The IPA also has access to Dropbox which is a secure method of transferring files between parties or giving permissions for external parties' access to particular share point files.

19. Data Storage

i. Staff carrying out inspector, complaints and other areas of work may well have access to personal data; and or financial data that could breach GDPR, and lead to loss of livelihood or have other consequences. It is vital therefore that you store only what is required for the IPA to carry out its functions, only shares in accordance with those functions, and does so securely, and destroys information (physically and electronically) as soon as it is no longer required.

ii. All staff are responsible for ensuring that any data that we hold that exceeds a period of six years should be destroyed using the confidential bins in the office or

if working from home, the individual should find their own way of ensuring that documents are destroyed securely.