Insolvency Practitioners Association

Data and Information Security Policy

Guidance

1. Introduction

i. An IT security policy will help you to:

- 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 your legal obligations under the General Data Protection Regulations (GDPR) and other laws
- Meet your professional obligations towards our clients and customers

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 the IT policy and taking appropriate actions when necessary.

ii. Appoint a specific senior member of staff to have day-to-day operation responsibility for implementing the IT policy

iii. Appoint specialist IT organisations to help with your planning and support

iv. Appoint a specific senior member of staff as the Data Protection Officer to advise on data protection and best practices.

v. Appoint a specific director or senior member of staff to take overall responsibility for IT security strategy.

3. Review Process

i. Review the IT policy at least annually

4. Information Classification

i. Only classify information which is necessary for the completion of your duties. Have policies in place to limit access to personal data to only those that need it for processing. Classify information into different categories so that you can ensure that it is protected properly and that you allocate security resources appropriately:

- **Unclassified:** This is information that can be made public without any implications for the company, such as information that is already in the public domain
- **Employee Confidential:** This includes 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, operate on a 'need to share' rather than a 'need to know' basis with respect to company confidential information. This means that your bias and intention is to share information to help people do their jobs rather than needlessly raise barriers to access.

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

6. Security software

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

- **Laptop and desktop anti-malware, Server anti-malware, intrusion detection and prevention, desktop firewall** – Use recognised software which is installed on every employee's laptop. This should be renewed and reviewed on at least an annual basis.
- **Cloud-hosted email spam, malware and content filtering** as well as **email archiving and continuity** is protected by only using recognised software such as Office 365 which is renewed and reviewed on an annual basis.

- **Data protection and Encryption** – Ensure all staff have had GDPR training which emphasises the need for data protection and password encryption on all files containing sensitive data.
- Consider using an **in-house firewall** which has **Intrusion Prevention System** (IPS) enabled.

7. Employees joining and leaving

i. When a new employee joins the company, only add them to the systems to which they need access to perform their roles:

ii. 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, 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. Staff are personally responsible for the secure handling of confidential information that is entrusted to them. Staff may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of their duties. Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to the Data Protection Officer.

9. Staff own device(s)

i. It is also staf members' responsibility to use their own devices (computer, phone, tablet etc) in a secure way. However, the company should provide training and support to enable them to do so (see below).

At a minimum staff should:

- Remove software that they do not use or need from their computers
- Update the operating system and applications on their devices regularly
- Keep their computer firewall and any other virus applications switched on
- 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 their phone and social media accounts
- Keep their work computer separate from any family or shared computers
- If they have access to an administrator account, do not use it on their own computer for everyday use
- Make sure their 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 staff should:

- Take time to learn about IT security and keep themselves 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 their computer and mobile devices when they are away from home or out of the office
- If a members of staff leaves the company, they will return any company property, transfer any company work-related files back to the company and delete all confidential information from their 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 company's system. The person who is involved in overseeing the particular report is responsible for ensuring that this is stored correctly.

ii. The company should consider 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 the matter to the Data Protection Officer.

13. Backup, disaster recovery and continuity

i. Ensure 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' notify the customers and data controllers 'without undue delay'. Ensure they are informed 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 about which staff need to be vigilant 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 –Members of staff need to question cash deposits and how assets are bought in the first place.

iv. Staff are responsible for following AML procedures and reporting suspicions

v. The obligations of members of staff with regards to AML are as follows:

- **Client Due Diligence (CDD)** - Under AML regulations, before the company can take on any new clients the following processes need to be adhered to and documented. This will allow the company 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 company'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 verifying the 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.

- **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 company 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), using the company'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. Unless the company has a procedure on this, then the following 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 staff have any questions regarding AML, please contact the company's money laundering reporting officer (MLRO).

16. AML Policies

i. For all staff that carry out activity on AML should refer to the company AML polices when carrying out this type of work, for example whistleblowing process, criminal reporting responsibilities (also contained within this policy) and escalation polices.

17. Data Security

i. Company employees, before keeping any information relating to external stakeholders should question themselves 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**
- **Ensure data is destroyed if no longer needed**
- **Keep personal data safe from people who are not allowed to see it**
- **Any memory sticks should be locked in drawers** Memory sticks and data discs can easily get lost, ensure that these are cleared when the data is no longer required and locked away when not in use. Memory sticks should be password protected.
- **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 should be 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.

- **Only hold information about someone for legitimate business purposes** – all staff should be given training on data security which is to be updated on an annual basis.

18. Sending personal data to another person

i. Before sending anything that includes personal or confidential information, 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 company 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, 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 from the original e-mail (please refer to point 16ii in this document).

19. Data Storage

i. Staff carrying out certain 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 staff store only what is required for the company to carry out its functions, only share information in accordance with those functions, and do so securely, and destroy information (physically and electronically) as soon as it is no longer required.

ii. All staff are responsible for ensuring that any data that the company holds that exceeds a period of six years should be destroyed securely unless there is a specific and documented reason for retaining it for a longer period. In such circumstances the reasons for continuing to hold should be reviewed at least annually.