Information Security Policy

Metadata Training

CONTENTS

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

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

2. Responsibilities

- Lori Toader is the director with overall responsibility for IT security strategy.

3. Review process

- We will review this policy every year.

- In the meantime, if you have any questions, suggestions or feedback, please contact Lori Toader, lori.toader@metadatatraining.co.uk, 020 7272 3726.

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 any implications for the company, such as information that is already in the public domain.
- Employee confidential. This includes information such as medical records, pay and so on.
- Company confidential. Such as contracts, source code, business plans, passwords for critical IT systems, client contact records, accounts etc.
- Client confidential. This includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market sensitive information etc.

I. Please also check the Privacy Policy.

II. We have categorised the information we keep as follows:

Type of information	Systems involved	Classification level
Customer Details	ZohoCreator, Active Campaign, Moodle e-learning, WordPress website	Client confidential
Customer's Booking and Exam Results	Zoho Creator	Client confidential
Credit Card Details	Sage Pay	Client confidential
Financial information	Accounting Package	Company confidential
HR Information	Payroll package	Employee confidential
Business records	Google Mail, Google Drive	Company confidential
Customer emails and correspondence	Google Mail, Live chat, Active Campaign	Client confidential

I. The deliberate or accidental disclosure of any confidential information has the potential to harm the business. This policy is designed to minimise that risk.

II. We do not protectively mark documents and systems. Therefore, you should assume information is confidential unless you are sure it is not and act accordingly.

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 data 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.

III. However, in general, to protect confidential information we implement the following access controls:

- Company confidential - restrictive permissions and sharing of important information.
- Client confidential - we put in place restrictive permissions, the admin user has control and access to sensitive information, two-factor authentication has been implemented and notification of strange system activity is in place; administrators have been trained on how to protect customer data.
- Employee confidential - restrictive permission to information.
- In addition, admin privileges to company systems will be restricted to specific, authorised individuals for the proper performance of their duties.

6. Security software

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

- Laptop and desktop anti-malware - Windows 10 Defender Antivirus
- Website malware and vulnerability scanning - Anti-Malware from GOTMLS.NET, 4.18.69, Sucuri WP Plugin v1.8.21
- Desktop firewall - Windows 10 Defender Antivirus

7. Employees joining and leaving

I. We will provide training to new staff and support for existing staff to implement this policy.

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.

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

8. Your 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 follow 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 Lori Toader at lori.toader@metadatatraining.co.uk.

9. Protecting your own device(s)

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.
- For Windows users, make sure you install anti-malware software (or use the built-in Windows Defender) and keep it up to date. For Mac users, consider getting anti-malware software.
- Store files in official company storage locations (Google Drive) so that it is backed up properly and available in an emergency.
- Switch on whole disk encryption.
- Understand the privacy and security settings on your phone and social media accounts
- Have separate user accounts for other people, including other family members, if they use your computer. Ideally, keep your work computer separate from any family or shared computers.
- Don’t use an administrator account 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.
- Consider using password management software.
- Don’t share your password with other people or disclose it to anyone else.
- Don’t write down PINs and passwords next to computers and phones.
- Use strong passwords.
- Change them regularly.
- Don’t use the same password for multiple critical systems.

11. **Be alert to other security risks**

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

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.
- 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. Don't disclose passwords and other confidential information unless you are sure you are on a legitimate website.
- Use social media, including personal blogs, 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 shredded when no longer required.

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

- Anything that contradicts our equality and diversity policy, including harassment.
- Circumventing user authentication or security of any system, network or account.
- Downloading or installing pirated software.
- Disclosure of confidential information at any time.