



## CONTENTS

1. INTRODUCTION
2. RESPONSIBILITIES
3. REVIEW
4. INFORMATION CLASSIFICATION
5. ACCESS CONTROLS
6. SECURITY SOFTWARE
7. EMPLOYEES JOINING AND LEAVING
8. YOUR RESPONSIBILITIES
9. PROTECTING YOUR OWN DEVICE(S)
10. PASSWORD GUIDELINES
11. BE ALERT TO OTHER SECURITY RISKS

## 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](mailto: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.







