Sample Do Not Use

GDPR Toolkit

INFORMATION SECURITY POLICY

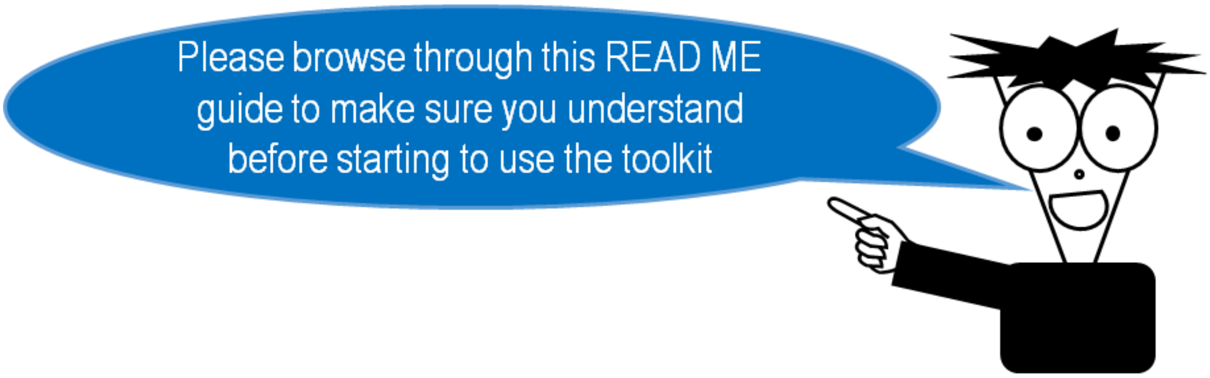
(C)opright Tim Rogers, 2017, Licence available

Do not use as-is, but make necessary amendments relevant to your organisation

GDPRToolkit

INTRODUCTION

Please read the READ ME User Guide first to make sure you know and understand the need to add, amend, or delete in order to reflect your people, processes and technologies as well as the data you hold and the jurisdiction(s) you operate in.


Please browse through this READ ME guide to make sure you understand before starting to use the toolkit

The READ ME User Guide will you help navigate around the GDPR-Toolkit and identify what you need to do for your organisation.

DISCLAIMER

GDPR can be complicated and there are different laws in UK, EU, Jersey and Guernsey. Simply having Templates, Documents, Samples and Guidance does not make you compliant.

The reason for this disclaimer is that I cannot warrant or guarantee materials for every system or circumstance or jurisdiction and the client/user/recipient is obliged to review, test and where necessary customise or take advice to generally assert that they are satisfied before using this “live”.

If DIY isn’t for you, that’s OK. I’m rubbish at electrical work, plumbing or carpentry. Call an expert. There are many out there and data protection is too important for you, your organisation and the people who trust you with their data for you to get it wrong.

SUPPORT

For those organisations without the resources, skills or experience I can help with training or provide support to customise the documents to meet your particular needs. TimHJRogers@AdaptConsultingCompany.com

(C)opright Tim Rogers, 2017, Licence available

INFORMATION SECURITY POLICY

TITLE	ACC GDPR Information security policy.docx	DATE	10/04/18
LOCATION	V:\Data2018\product_GDPRToolkit\ACC GDPR Information security policy.docx	VERSION	Ver 1
AUTHOR	[Author]	Pages	3 of 7
APPROVER	[Approver]		

Contents

1. POLICY

[Organisation name] tasks information security seriously. This policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

Confidential data is secret and valuable.

Common examples are:
Unpublished financial information
Data of customers/partners/vendors
Patents, formulas or new technologies
Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

(C)opright Tim Rogers, 2017, Licence available
Do not use as-is, but make necessary amendments relevant to your organisation

2. PERSONAL AND ORGANISATIONAL DEVICES

When employees use their digital devices to access company emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and company-issued computer, tablet and cell phone secure.

They can do this if they:

1. Keep all devices password protected.
2. Choose and upgrade a complete antivirus software.
3. Ensure they do not leave their devices exposed or unattended.
4. Install security updates of browsers and systems monthly or as soon as updates are available.
5. Log into company accounts and systems through secure and private networks only.

We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others. When new hires receive company-issued equipment they will receive instructions for:

1. [Disk encryption setup]
2. [Password management tool setup]
3. [Installation of antivirus/ anti-malware software]

They should follow instructions to protect their devices and refer to [Information Security Manager] if they have any questions.

3. KEEP EMAILS SAFE

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

1. Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
2. Be suspicious of clickbait titles (e.g. offering prizes, advice.)
3. Check email and names of people they received a message from to ensure they are legitimate.
4. Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can refer to [Information Security Manager]

(C)opright Tim Rogers, 2017, Licence available
Do not use as-is, but make necessary amendments relevant to your organisation

4. MANAGE 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 our employees 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. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their 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 recognize the person they are talking to.
- Change their passwords every two months.

Remembering a large number of passwords can be daunting. We will purchase the services of a password management tool which generates and stores passwords. Employees are obliged to create a secure password for the tool itself, following the above mentioned advice.

5. TRANSFER DATA SECURELY

Transferring data introduces security risk. Employees must:

1. Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request employees to ask our [Security Specialists] for help.
2. Share confidential data over the company network/ system and not over public Wi-Fi or private connection.
3. Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
4. Report scams, privacy breaches and hacking attempts

Our [Information Security Manager] needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to [Information Security Manager].

Our [Information Security Manager] is responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

(C)opright Tim Rogers, 2017, Licence available
Do not use as-is, but make necessary amendments relevant to your organisation

6. ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct our employees to:

1. Turn off their screens and lock their devices when leaving their desks.
2. Report stolen or damaged equipment as soon as possible to [Information Security Manager]
3. Change all account passwords at once when a device is stolen.
4. Report a perceived threat or possible security weakness in company systems.
5. Refrain from downloading suspicious, unauthorized or illegal software on their company equipment.
6. Avoid accessing suspicious websites.

We also expect our employees to comply with our social media and internet usage policy.

Our [Information Security Manager] should:

1. Install firewalls, anti malware software and access authentication systems.
2. Arrange for security training to all employees.
3. Inform employees regularly about new scam emails or viruses and ways to combat them.
4. Investigate security breaches thoroughly.
5. Follow this policies provisions as other employees do.

Our company will have all physical and digital shields to protect information.

7. REMOTE EMPLOYEES

Remote employees must follow this policy’s instructions too. Since they will be accessing our company’s accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage them to seek advice from our [Information Security Manager]

8. DISCIPLINARY ACTION

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action. First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.

Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.

(C)opright Tim Rogers, 2017, Licence available
Do not use as-is, but make necessary amendments relevant to your organisation

We will examine each incident on a case-by-case basis. Additionally, employees who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

9. TAKE SECURITY SERIOUSLY

Everyone, from our customers and partners to our 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

10. DOCUMENT CONTROL

[document owner] is the owner of this document and is responsible for ensuring that this procedure or process is reviewed in line with the review requirements.

Consultation Phase: A document which is circulated for comment to key stakeholders to ensure support for scope, format, and content.

Draft Phase: Ostensibly the last draft, capturing all the points from the previous consultation phase and circulated for comment before being finalised.

Final Phase: A document which is FINAL. This is the baseline document which may subsequently amend over time.

VERSION	DESCRIPTION OF CHANGE	AUTHOR	APPROVAL	DATE OF ISSUE
Consultation	Initial Issue for consultation.	[Author]	[Approver]	March 2018

(C)opright Tim Rogers, 2017, Licence available
Do not use as-is, but make necessary amendments relevant to your organisation