
squire technologies
the signalling specialists to the telecoms industry

squire technologies

GDPR IT Security Policy

Date: 09/05/2018

Version: 1.1

Document Number: SQ001540

Change History

Version	Change Made	Author	Authorised	Date
1	Document Created	BK		22/02/2018
1.1	Added Formatting	PC		09/05/2018

squire technologies

Contents

1 Introduction

1.1 Background

This policy sets out the measures to be taken by all employees to protect our IT systems such as our computers, devices, storage devices and third party systems that we use day to day in running our business.

It is essential that we have such a policy in place to not only ensure the integrity of our business but also to ensure we comply with various requirements set out in law, particularly relating to data protection and the protection of our clients' and employees' personal data, privacy and confidentiality. Regarding data protection, this policy should be read in conjunction with our Data Protection Policy and associated data protection policies.

We take the security of our business, systems and processes seriously and place high importance on protecting the privacy and confidentiality of our clients and employees. As such, this policy sets out the company approach to ensuring that security. The approach set out in this policy document is applicable to all employees, whether permanent, temporary or contract staff.

2 Responsibilities

2.1

All employees have a responsibility to maintain security of our business, systems and data, however the Board of Directors are ultimately responsible for ensuring adequate security controls are in place across the business and that policies and procedures are complied with by all employees. Specifically, they are responsible for:

- Ensuring all systems are compliant with our security requirements.
- Ensuring systems and policies are up to date with current threats and vulnerabilities.
- Ensuring that employees are only granted with access to or control of systems that are appropriate for carrying out their role.
- Ensuring that suitable backups (including off-site) of systems are taken, particularly of data stored on those systems.
- Assisting employees in understanding and complying with this policy.
- Providing employees with appropriate security training and keeping them up to date with the latest threats.

3 Key security principles

3.1

All systems are to be protected against unauthorised access.

3.2

All data stored on systems are to be managed securely and in line with our Data Protection Policy.

3.3

All employees including part-time, temporary and contract workers are to familiarise themselves with this policy and adhere to its requirements, always.

3.4

All systems are to be maintained, patched, updated by the employee responsible for that system or by our External IT Maintenance Company (Prodigy).

3.5

All employees are responsible for reporting breaches of security relating to our systems to their manager in line with our Data Breach Policy.

3.6

This policy relates to all systems and devices used by our employees, including, but not limited to, access to PCs, laptops, tablets and smartphones, software running on these devices and third party software running on the internet ("in the cloud").

squire technologies

4 Software security

4.1

All software in use on the systems which the employee has control over will be kept up to date with any relevant software updates, patches or fixes. These should be automated wherever possible.

4.2

Where a security flaw is identified in software where no fix is available, the software must either be upgraded to a new version that fixes the flaw or withdrawn from the system until a fix is found. Where the flaw allows external access vulnerabilities, the system must be disconnected from the outside internet.

4.3

No employees will install software onto any system, including their own work devices, without permission from their manager.

4.4

All software will be installed by our external IT Maintenance Company (Prodigy) unless express permission is granted by the employee's manager for the employee to install it themselves.

5 Anti-virus security

5.1

Systems that are vulnerable to virus infection (e.g. computer and device operating systems) will be protected by suitable anti-virus or firewall software. All such software will be kept up to date with the latest software updates and virus definitions.

5.2

Systems that are vulnerable to virus infection will be scanned for infection at least once a week.

5.3

No external storage devices (e.g. USB sticks, external hard drives, etc.) should be attached to any systems without first being scanned for viruses. Where possible USB ports and other connecting ports on devices should be disabled to prevent accidental use.

5.4

Any employee detecting a virus must report it immediately to their manager for investigation and appropriate action.

5.5

Any action by an employee to deliberately introduce a virus or malicious program onto a company system will be considered a criminal offence under the Computer Misuse Act 1990 and dealt with in line with disciplinary procedures.

6 Hardware security

6.1

Wherever possible all systems will be in rooms which can be securely locked when not in use or unattended.

6.2

All devices should be locked when not in use (using appropriate software locks, e.g. screen locks, screensavers, etc.), to prevent unauthorised access.

6.3

All visitors will be supervised at all times and not left unattended with access to any of our systems.

6.4

All devices should be transported and used securely. Any devices with access to our systems and data that are lost or stolen should be reported immediately to the Manager of the person responsible for that device.

6.5

The Company will maintain an asset register of all systems and devices used within our business

7 Access security

7.1

All systems and devices will be protected by a secure password or other secure log-in system.

7.2

1.1. All passwords must:

- Be at least 12 characters in length (where permitted)
- Be made up of a mix of lowercase and uppercase letters, numbers and symbols (where permitted)
- Be randomly generated where possible
- Avoid using repetitive characters, common words or expressions
- Avoid using words or expressions linked with the business name or can be easily guessed
- Kept secret to each employee
- Not be shared or written down

7.3

If an employee forgets their password they should use approved means for requesting a forgotten password depending on the system in question. If in doubt, advice should be sought from the employees Manager.

7.4

Where a system supports it, two-factor authentication should be enabled.

7.5

Where multiple passwords are required, a password locker may be used provided it, itself is locked down with an adequate password and access to the locker is in line with this security policy.

7.6

All systems should be “screen” locked automatically after 5 minutes of non-use.

7.7

Access to any personal data on our systems must only be via a secure, non-public, internet connection.

8 Use of cloud and online systems

8.1

Where systems are used online (e.g. for storage, CRMs, etc.) due diligence must be carried out to assess their suitability from a security perspective. Our Data Protection Policy also requires this from a data protection perspective.

8.2

Access to these online systems must be controlled, specifically:

- Devices should be locked with a password, in line with this policy
- Where possible, automatic sign-ins or remembering of a user, including saving passwords in browsers should be avoided
- Two-factor authentication for login should be enabled, where available

9 Use of email

9.1

All emails must be collected using authorised access applications using an encrypted connection.

9.2

All employees must abide by the rules set out in the Data Protection Policy regarding sharing personal data via email.

9.3

All employees must be mindful that an email can by spoofed to look like it comes from someone within the business, when it hasn't. They should particularly be on the lookout for fraudulent emails requesting the transfer of monies on the instructions of a senior manager. If the employee is in doubt to the authenticity of the email, they should check with the person who the email allegedly came from, in person. When large amounts of money are involved the authorising employee should phone the person ahead of sending the email to avoid raising concern.

9.4

Email attachments in emails from people you do not know, will not be opened unless the attachment has been checked for viruses, this includes .zip .pdf and Microsoft Office files. Employees should also avoid following links to external websites within emails unless it is clear the email and the link are genuine.

10 Remote access to systems including from home, in public or using personal devices

10.1

Where systems are accessed remotely or from home they should be done so using devices that adhere to the requirements set out in this policy as if those devices were used at work, this includes when employees access systems using their own devices (e.g. in terms of password security, locking of devices, etc.)

10.2

Employees must observe if there is a risk that any unauthorised third party would be able to view personal data whilst they, themselves, are viewing the data on a device (e.g. whilst at a client's premises, whilst travelling on public transport, etc.) to prevent unauthorised viewing of personal data. Screen guards should be used whenever possible, in such situations.

10.3

No personal data will be transferred to personal devices belonging to an employee without authorisation from the employee's manager.

11 Policy review

This policy will be reviewed periodically by the Board of Directors to ensure it is still relevant and up to date with any changes in the law, guidance or precedents set.