SPRING NETWORK SECURITY POLICY

16th May 2016

INTRODUCTION:
This policy does not intend to be an exhaustive list of all network security issues but intends to set out fundamental standards and responsibilities that are actionable by Spring staff and associates. As such it is deemed by the Directors that this policy is:

1. Consistent with Spring existing policies and works with those policies, including:
    a. Spring Cyber Security Process
    b. Spring Information Security Policy and Security Incident Policy
    c. Spring User Access Management Policy
2. Is adequate taking into consideration the clients, type of work and classes of data Spring is dealing with
3. Is relevant at the time of writing and will be reviewed annually

PURPOSE: To ensure all systems used by Spring are secure to safeguard all Client confidentiality, integrity and availability of information and supporting systems.

POLICY: All Employees and Associates of Spring CCR Ltd must ensure that any and all Client information is kept secure in both a physical and digital sense.

APPLICATION: The following requirements apply to all networks used by all employees, contractors and associates of Spring CCR Ltd

1. IN BRIEF:
    1. Protect all Spring client information held.
    2. Prevent unauthorised access to Spring systems and data
    3. Protect Client systems from infection.
    4. Avoid using devices that you/we do not own e.g. public devices.

2. IN MORE DETAIL

SPRING NETWORK SECURITY POLICY

16th May 2016

Before getting into the policy proper it is worth understanding what a network is when reading and applying this policy.

DEFINITION: *Network - A **computer network** is a set of **computer (devices)** connected together for the purpose of sharing resources.*

As such, for the purpose of this policy this will include any and all of the following devices/systems that have access to Spring data and systems:

- Any laptop or desktop computer
- Any mobile phone, tablet or mobile computing device
- The Internet/World Wide Web (e.g. the Spring website)
- The Spring email system (currently provided by Google Apps for Work)
- Cloud Systems (e.g. Dropbox)

Bring your own device - BYOD

As many associates and employees use their 'own devices' for working on Spring clients the following applies to all devices that store, view and process Spring data. The difference between Spring devices and BYOD is that maintenance of that device and the following fundamental standards are the responsibility of the owner of the device.

Encryption

All devices that store and process personal client data (see Spring Information Security and Security Incident Policy for more information) should be encrypted as follows:

All Windows Desktops and laptops - From Windows 10 onwards encryption is a standard functionality and can be turned on -

http://windows.microsoft.com/en-gb/windows-10/turn-on-device-encryption

Mac Desktops and Laptops - https://support.apple.com/en-gb/HT204837

iPhone and iPad - Setup passcode. Encryption is defaulted on ios 8 and above when using a passcode - https://support.apple.com/en-gb/HT202064

Android Setup passcode - Default on Android 5 when using a passcode

USB Stick - Spring will provide secure USB sticks to all staff and associates. No other USB sticks or removable storage devices should be used for Spring client data (this includes CD's, DVD's SD cards etc)

Other Devices - If you intend to use any device not listed above for Spring work please contact a Spring director.

Spring will provide technical support and will review encryption regularly.

Anti Virus
All Mac and PC's should have anti-virus installed and be updated regularly

Anti malware & key logging
All Mac and Pc's should be installed with anti malware updated regularly

Cloud services

Spring use the following services:

- Google Apps for Business
- Dropbox

Usage, privacy and data protection are covered by Spring policies and the

cloud service providers policies as below:

- Google Apps for Business - https://support.google.com/work/answer/6057301?hl=en&rd=1
- Dropbox - https://www.dropbox.com/security

Compliance with EU data protection law is covered by:

Google - https://support.google.com/work/answer/6056694?hl=en
Dropbox - https://www.dropbox.com/en/help/9208

Special note - EU data protection
As of the time of writing, 9th May 2016, the previous Safe Harbour legislation has been discontinued and the discussion and ratification process of the new EU and US Privacy Shield is underway but not complete. We have reviewed our processes and in line with ICO (Information Commissioners Office) advice will await final acceptance of the new laws which are expected June 2016. Further information - https://iconewsblog.wordpress.com/2016/02/11/safe-harbor-calmer-waters-on-the-horizon/

Passwords

To access any Spring data a secure access approval is essential and for the majority of systems this will be via character based passwords. The following is guidance for effective passwords. All passwords used in relation to Spring data should be:

1.Strong e.g. at least 8 characters including upper and lower case, numbers

and special characters

Example
Good #1Hu56Nk8%q

Bad Pa$$w0rd

2. Be unique e.g. not the same password for Google email and Dropbox
3. Be changed regularly (maximum usage 12 months)
4. Not shared or stored insecurely e.g. written in a book/on post it note

Device access and application access security
All devices should have an access codes

Windows and Mac - passwords on user accounts to login
Smart Phones and Tablets - Passcodes (which will also turn on the encryption)

Two Factor Authentication (2FA)
All Spring web accounts will have Two Factor Authentication applied

Adding two factor authentication to any web account will significantly increase your security. 2FA adds an additional piece of information that only you can access when logging in. Many web accounts use an application on your phone to generate a 6 digit code which changes every 60 seconds. This should make it very hard for a 3rd party to access your account without your permission

Links to setup 2FA on:
Google - https://www.google.com/landing/2step/
Dropbox - https://www.dropbox.com/en/help/363

Appendix 1 Definitions

'Own device' - any computer, phone, tablet, storage device or equivalent used to view, process or store Spring data

'Two Factor Authentication', also known as 2FA, two step verification or TFA (as an acronym), is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand - such as a physical token.

Appendix 2 Links

In writing this policy we have taken into consideration

1. ICO guidance on BYOD relevant to data protection - https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf