SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

THIS DOCUMENT HAS **THREE** PARTS.

PART 1

INFORMATION AND SECURITY INCIDENT POLICY

PURPOSE: to safeguard all Client confidentiality, integrity and availability of information and supporting systems.

LEGAL CONTEXT: Data Protection Act 1998. Also potential requirements by our Clients as a condition of engaging us including LBG/FSQS & KPL.
See also Spring's Data Protection Policy.

POLICY: All Employees and Associates of Spring CCR Ltd must ensure that any and all Client information is managed in both a physical and digital sense and as set out in this policy.

APPLICATION: The following requirements apply to Directors and Staff of Spring CCR Ltd., all Spring Associates, Suppliers and Licensees as Appendix 2 and in respect of all Clients and form an integral part of the general obligation to maintain the confidentiality of both Spring CCR Ltd information and that of Clients.

1. IN BRIEF:
    1. Protect all Client information held.
    2. Prevent unauthorised access to, or use of, Client information.
    3. Protect Client systems from infection by interaction with Spring website or use of memory stick/flash drives or your own actions.

© Spring CCR Ltd 2016

4. Follow the procedure below in the event of any Security Incident i.e. breach or suspected breach – e.g. loss of laptop/memory stick/flash drive etc.
5. This Policy must be reviewed annually at a team meeting and team members must review the current situation regarding any potentially sensitive client data.

2. IN MORE DETAIL

1. Before any data (see Appendix I for data definition) is received by Spring it must be confirmed that this information is required by Spring and if not this data must not be received or must be deleted.
2. In order for Spring to complete its work for its clients there is no requirement for 'sensitive personal data' as defined in Appendix I. Wherever possible Spring staff and associates are to avoid receiving this type of data.
3. If sensitive personal data is received by accident or other event, the procedure in section 4 must be followed.
4. All required personal data must be stored on a secure and separate logical drive (e.g. password protected [min 8 characters in length] and encrypted memory sticks or flash drive as provided by Spring) used solely for the purpose of that Client's sensitive information.
5. You must not share required personal data with any person, organisation or entity unless required to do so by an authorised body e.g. court of law. In the event you are required to provide/share information you should inform the person whose data is to be disclosed at the earliest possible opportunity and inform a Director likewise.
6. You must ensure that any Client information held on **ANY** portable device which includes memory sticks and flash drives and phones are

© Spring CCR Ltd 2016

encrypted or password protected (for more information see the Spring Network Security Policy).

7. Do not yourself, or allow others to, make any unauthorised change or gain access to any Client information held by you.
8. You must prevent introduction of any 'bug' (malware) into Client systems especially if you supply anything that could carry 'malware' as part of your delivery of Services to Client. For example, if you intend to transfer data from a USB storage device (memory stick/flash drive) to a Client or Spring system you MUST have prior checked the USB device for malware/infection. If in doubt, contact a Spring Director before taking any such action.
9. In the event that any Employee or Associate is responsible for the introduction of 'malware' into a Client system, Spring CCR Ltd. will be liable for consequential costs and will have the right to recover such costs from that person.
10. You must notify a Director of Spring immediately if you find or suspect any 'bug' in any part of our Spring website including Client specific areas or in any device you are using or in any interaction you may have with any Client system.
11. If changes are made to the Spring website operating system or access systems that affect a Client Specific Secure Area(s) e.g. for course material download, a Director must notify the Client(s) no less than 14 days prior to making proposed changes and (see 6. below) arrange for testing and 'fixing' if required.
12. Any and all Client information that you request to be held on the Spring website must be kept separate, held secure and not be accessible by any other party. You must obtain confirmation in writing/email from the Spring *Web Administrator to this effect.
13. All Client information at your premises must be kept in a locked cabinet or locked premises.

© Spring CCR Ltd 2016

14. **Specific to Lloyds Banking Group** if the Spring website carries LBG information, it is the responsibility of a Director to task the *Website Administrator to arrange for security testing with LBG along with regular repeat testing.
15. **Specific to Knowledgepool**:
    a. KP require "*all LBG personal data including but not limited to Delegate lists, sign in sheets and or attendance lists must be protected against unauthorised or unlawful processing and against accidental loss destruction or damage"*.
    b. KP require *"all such data provided by Knowledgepool must only be shared with Knowledgepool and not with LBG".*
    c. KP require *"all such data must always be encrypted/password protected before sharing with Knowledgepool to ensure protection of colleague data".*

    In respect of:
    - 15.a - by complying with Clauses 1 and 2 of this Spring Policy you are already meeting this obligation. By discussing with project owners ways to reduce the number of touch points in communication of personal information such as delegate lists, you will further minimise risk.
    - 15.b - the important situation to avoid is being the conduit of personal information between KP and LBG.
    - 15.c – where possible encrypt and where not, seek agreement with intended recipients of any personal information as to how they want it protected before sending it.

    NOTE: Our policy in this specific KP regard is to act in the interest of practicality and common sense. Thus, if KP consistently sends unencrypted information in any format that contains delegate names or limited personal data (e.g. name and employee number), you are to

© Spring CCR Ltd 2016

assume there is no need to encrypt *the same* information if you are required to send it back to KP simply to fulfil some administrative task on their behalf.

16. All desk and portable computers and electronic devices capable of storage must carry effective anti virus protection and firewalls.
17. All Spring staff and associates should operate a clear desk policy. This means that no personal information pertaining to Spring will be left unattended at any time. This applies to any working area. Upon completion of work at the end of the working day, all personal information must be stored securely.
18. All client information and personal data that is no longer required (e.g. upon completion of contract) must be disposed of securely. Data held in physical format must be shredded or returned to Spring. Digital data must be deleted from the device on which it is held, so that it is no longer accessible. All Spring staff and associates holding digital data must contact Spring with regard to the correct deletion procedure.
19. The exit strategy for the termination or decommissioning of Spring Client information and/or infrastructure at the end of a contract is agreed on a contract-by-contract basis. All Spring staff and associates are required to contact Spring in this regard on completion of each contract.

3. PROCEDURE IN THE EVENT OF A SECURITY INCIDENT

A Security Incident is any event that is, or you suspect may be, a risk to Client and/or Spring confidentiality, integrity and availability of information and supporting systems. This procedure may also be considered to bear a

© Spring CCR Ltd 2016

similarity to a 'Whistleblowing Policy' in that it enables any member of Spring to freely report any perceived issues that might impact us or our customers.

Put simply, but not exclusively, you should ask yourself "Is this event causing or likely to cause, risk of any kind (however minor) to our Client(s) or Spring's confidentiality and security of information and systems?'

If the answer is "Yes" you must follow the procedure below:

1. If the removal of the cause is simple and you can affect a remedy easily, quickly and safely, take such action as you think fit and **in any event** follow the next steps.
2. Notify a Director of Spring of the incident as soon as you can and always within 24 hours.
3. Notify the Person or Manager representing Client who is in charge of your current project or service delivery of the incident as soon as you can and always within 24 hours.
4. Write full details of what has happened that is causing or likely to cause risk to Client and email them to *both* Spring Directors as soon as you can and always within 24 hours.
5. The Director(s) must contact the Client senior person connected with the service delivery involved as soon as possible and always within 48 hours.
6. The Director(s) must investigate the event, diagnose cause and analyse findings.
7. All communications must be recorded safely and kept confidential.
8. The Director(s) must allow and assist a Client to audit and take any necessary remedial actions for any reason connected with a security incident and especially if a breach occurs.

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

4. PROCEDURE IN THE EVENT RECEIVING SENSITIVE PERSONAL DATA

Wherever possible Spring staff and associates should avoid receiving sensitive personal data, as defined in Appendix I. If sensitive personal data was received by accident the following procedure must be followed:

1. Before any further action is taken inform a Spring director that 'sensitive personal data' has been received and the form it takes. Do not forward or share.
2. Where relevant inform the data provider of the Spring policy to not hold 'sensitive personal data'
3. Return and/or destroy the data securely as agreed with the Spring Director and the data provider
4. Document the details (not the data) and outcome of the above and send to the Spring director

© Spring CCR Ltd 2016

Appendix I - Definitions

Data
There are three types of data:

1.Personal data means data which relate to a living individual who can be identified

2. Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,

(b) political opinions,

(c) religious beliefs or other beliefs of a similar nature,

(d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) physical or mental health or condition,

(f) sexual life,

(g) the commission or alleged commission by them of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

© Spring CCR Ltd 2016

3.Anonymous/Aggregate data means any data which relates to any individual but which cannot be identified to that person

WEBSITE TECHNICAL SUPPORT
* Mark Mapstone, WordPress, Websites & Book Publishing, 16 St Andrews Court, Woodbury Avenue, Wells, BA5 2XX Tel: 07818 613577
Email: mark@markmapstone.com Web: www.https://markmapstone.com/

Appendix 2 – Suppliers & Licensees

RTrio Ltd.
3D Learning Ltd.
Spring CCR Ltd.
Outserve Ltd

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

PART 2
NETWORK SECURITY POLICY

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,

© Spring CCR Ltd 2016

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.

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

2. IN MORE DETAIL

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

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

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

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

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

© Spring CCR Ltd 2016

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)

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

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

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

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

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

PART 3

CYBER SECURITY PROCESS

The Spring cyber security process is set out below and should be read in conjunction with Parts 1 & 2 of this document:

1. Spring Network Security Policy
2. Spring Information Security Policy and Security Incident Policy

The process is not designed to be exhaustive but should be consistent and and reviewed regularly.

PURPOSE: To ensure Spring systems and relevant data are secure

RESPONSIBILITIES: It is the responsibility of the Spring directors to ensure that the process is followed and acted on

© Spring CCR Ltd 2016

SPRING INFORMATION & SECURITY INCIDENT POLICY, NETWORK SECURITY POLICY & CYBER SECURITY PROCESS

31st January 2020

1. Assess what data we process and its level of sensitivity
2. Assess the systems we use to process the above data for adequate security based on what data we hold
3. Base our network security policy on the above

Implement our security policies

4. Educate and inform staff and associates of the security policies and make aware of threats
5. Annually check and review the policies for adequacy and compliance
6. Document the review and any subsequent changes or recommendations

© Spring CCR Ltd 2016