Your Right Hand Finance Ltd (YRH)

Data Security Policy

CONTENTS

1 General Purpose 2
2 General Scope 2
3 General Data Rules 2
4 Hard data security 3
5 Equipment Security 4
6 Network Security, Access & Authentication 5
7 Email 7
8 Mass Emailing 8
9 Passwords and Accounts 8
10 Backup 9
11 Application Engineering and Development 9
12 Operational Security 9
13 Responsibilities 10
14 Reporting issues and threats 10
15 Records management 11
16 Policy Compliance 11
17 Terms and Conditions 12
18 Implementation of Policy 13
19 Related legislation 13
20 Feedback and suggestion 13

This Policy has been approved and authorised by:

Name: Jane Ryan	**Position:** Operations Director	**Date:** 01/12/2018	**Signature:**
Reviewed and updated:	06/03/2019		
Due for review by:	25/05/2019		

1 General Purpose

This policy establishes an effective, accountable and transparent framework for ensuring high standards of data security at Your Right Hand Finance Ltd (YRH), a company registered in England under number 06239695, whose registered office is at The IQ Hub Farnborough Business Park, Fowler Avenue, Farnborough, Hants, England, GU14 7JF ("the Company") regarding security of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

2 General Scope

This policy applies across all entities or subsidiaries owned, controlled, or operated by the Company and to all principals, consultants, agents, contractors, and/or employees, including part-time, temporary, or contract employees ("the User").

This policy covers any devices, systems or data attached to the Company's systems. It includes any data or information sent to/from the Company and any data that is owned by the Company that resides on external systems or on devices.

From time to time, the Company or its clients may provide Users with systems or network access in order for them to carry out their contractual service commitments or in support of the Company's operations. The provision of this access carries responsibilities and obligations as to what constitutes acceptable use of the network, systems and data. This policy sets out how this access is to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the User is expected to use common sense when using the Company or client resources. Inappropriate use of these networks or systems could expose the Company or its clients to risk, so this policy sets out the minimum standards on what is and what is not permitted. The scope includes any and all use of Company or Client IT resources, including but not limited to, computer systems, devices, processing of data, email, the network, and internet connections.

3 General Data Rules

3.1 Confidentiality

Without prior written approval from the Company or the client, (whoever owns the data), Confidential data must not be:

- Shared or disclosed in any manner to non-employees of the Company or client; and

Should not be:

- Posted on the Internet or any publicly accessible systems.
- Transferred in an insecure manner, for example on a USB stick or in any other unsecured manner.

Commented [JR1]: Can we put an example here?

Commented [LI2R1]: USB

3.2 Unacceptable Use

The following actions shall constitute unacceptable use of the Company or its client networks. This list is not exhaustive and is included to provide a frame of reference for types of activities that are deemed unacceptable. The User may not use the Company or client networks and/or systems to:

- Engage in activity that is illegal under local or international law or contravenes regulations of any compliance or regulatory authorities governing the Company or its clients.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the Company or its clients.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Make fraudulent offers for products or services.
- Perform any of the following: unauthorised port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques.
- Install or distribute unlicensed or "pirated" software.
- Reveal system, personal or network passwords to others.

3.3 Blogging and Social Networking

Blogging and social networking through the use of Company accounts are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging and social networking are allowed provided that:

- It is done in a professional and responsible manner.
- Confidential or personal data is not disclosed.
- It does not impact the User's contracted services.
- No information detrimental to the Company or its clients is published.
- The User assumes all risks associated with blogging and/or social networking.
- It is made clear that they are the Users personal opinions and not those of the Company or client unless prior written permission has been obtained.
- It adheres to the client's policy on Blogging and Social Networking.

3.4 Web Browsing

The Internet is a network of interconnected computers of which the Company or User has little control. The User should understand that when using the Internet, it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The User is responsible for any information that the User views, reads, or downloads from the Internet and must take full responsibility when using the Company or client networks and adhere to their respective policies.

3.5 Copyright Infringement

The Company's or clients' computer systems and networks must not be used to download, upload, distribute or otherwise handle illegal and/or unauthorised copyrighted content that contravenes the legal rights for the reuse or sharing of the information.

3.6 Peer-to-Peer File Sharing

Peer-to-Peer (P2P) networking is not allowed on the Company network, nor client networks unless written approval is obtained from the Company or the client respectively.

3.7 Streaming Media

Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is permitted on the Company network where required in order for the individual to perform their role. Streaming media on client networks must not be undertaken unless the client Policies permit.

3.8 Monitoring and Privacy

The Company reserves the right to monitor the Company network, systems and or accounts. This may include but is not limited to: transmission and storage of files, data, and messages. The Company reserves the right to monitor any and all use of the computer systems, network, information, data and cloud-based solutions. To ensure compliance with Company policies this may include the interception and review of any emails, or other messages sent or received, and inspection of data stored in provided storage areas, such as personal file directories.

3.9 Circumvention of Security

Using any computer systems to circumvent any security systems, authentication systems, User-based systems, or escalating privileges on Company or client networks or systems, is expressly prohibited.

3.10 Use for Illegal Activities

No individual or supplier contracted through the Company may knowingly undertake illegal activities under local or international law. The Company will take all necessary steps to report and prosecute any violations of this policy.

3.11 Software Installation

Installation of software into Company or Client environments is prohibited unless written consent has been obtained in advance from the owner of the network and systems.

4 Hard data security

4.1 Offices

THE COMPANY does not have a physical office building, however many of the principals, consultants, agents, contractors, and/or employees work from their home or client's office(s). Where the work takes place at a client's office(s) the client shall have responsibility for hard data security. Where work takes place at the principals, consultants, agents, contractors and/or employees home, they will have responsibility for hard data security as laid out in the *Data Protection Policy* 23.1.1 and point 4.2.

4.2 Paperless systems

THE COMPANY operate a paperless information storage policy. No records are retained long term on paper. Printed documents may be produced for the purpose of entering data onto accounting software but are stored in a locked filing cabinet until three months after the end of the financial year to which they relate, when they are transferred to a secure lock up for the correct retention period as per the Data Retention Schedule on the *Directories of Data and Assets and Risk and Systems and Retention Schedule*, after which they are ultimately shredded.

5 Equipment Security

5.1 Overview

Equipment includes laptops, desktops, tablets, mobile phones, and any other device being used for THE COMPANY work and Client work. Where possible all THE COMPANY systems and services are held in the cloud and run by major suppliers, i.e. Microsoft, but Principals and Regional Directors use their own equipment for THE COMPANY work and must adhere to the Data Security Policy.

The Company's business model is underpinned by a network of Service Companies and Suppliers utilising their own supplied hardware. These devices are vital tools in the delivery of client services, with more confidential, personal and sensitive data being stored on them, the risk associated with their use grows. Special consideration must be given to the security of mobile devices and it is the Users responsibility to ensure all reasonable and appropriate measures are taken to protect the Company and its clients' data.

This policy applies to Company and client data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, desktops, notebooks and smart phones. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with Company or client data and owned by the individual or the organisation they work through.

5.2 Protective measures

By its nature, a mobile device is more susceptible to loss or theft than a non-mobile system. All Users must carefully consider the physical security of the mobile devices they use in the delivery of their services and take all reasonable and appropriate protective measures to protect them from theft or the data they contain from falling into unauthorised hands. Loss, theft, or any other security incident related to a mobile device, that at the time was holding Company or client data, must be reported through Data@yourrighthand.co.uk and the client's appropriate channels immediately.

All devices used by Principals and Regional Directors must:

- Have up to date anti-virus and anti-malware software properly licenced and installed
- Have up to date and properly licenced operating systems and applications
- Have data encrypted as a standard
- Have a lock mechanism which needs a password, swipe, pin, biometric or other security device to unlock the system
- Have a backup system for data that is encrypted, off-site, with versioning and retention policies
- Have remote wipe capabilities configured for mobile phones
-

Upon leaving the Company or leaving a Client, all data associated with the Company and/or the Client(s) must be removed from the equipment and all backups (including versions) must be deleted.

Employees will be issued with a the Company laptop and mobile phone. These will have a standard set of software installed that includes anti-virus and anti-malware along with appropriate encryption.

All systems should be capable of monitoring and reporting on access of the systems. Logs should be retained in accordance with business, legal and regulatory requirements.

Equipment should only be connected to trusted wireless networks. If it is not known whether a wireless network can be trusted, but it is to be used for transmitting data, then an approved VPN client must be used.

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defence for protecting Company and client data. The following sections specify the Company's requirements for data security as it relates to mobile devices:

5.2.1 Laptops

Whole disk encryption is required and comes as standard on most laptops. Laptops must require a Username and password or biometrics for login in accordance with the Password and Account section of this policy (9).

Commented [LI3]: I think we should have a guide on this and then ask people to confirm it is done. Most devices do it automatically although Windows 10 needs the settings checking for example – dodgy area – might get them to check themselves how to do it – Liability to us if their devices don't cope??

5.2.2 Smart Phones

The storage of confidential, personal or sensitive data on smart phones is not advisable but if stored, encryption is required PDAs/smart phones must require a password for login in accordance with the password policy.

5.2.3 Other Mobile Devices

Unless specifically addressed by this policy, storing Company data on other mobile devices, or connecting such devices to Company or client systems, is expressly prohibited without prior written consent from the organisation who owns the data.

5.2.4 Storage devices (USB)

the Company provides online systems to transfer details securely. The Company does not restrict the use of personal storage media, provided that the policies for data security are followed. The User must take reasonable precautions to protect against viruses and malware. Any Company or client data must reside within the EU at all times unless prior written agreement has been obtained by the Company or client who owns the data and is in compliance with the GDPR. Any confidential, personal or sensitive data should only be stored on encrypted devices. Data should be securely erased from any storage media when it is no longer needed.

We recommend that USB storage devices are not used. If a USB stick is required to be used the Principal must seek written authorisation by contacting data@yourrighthand.co.uk. All storage devices should be encrypted before storing any client or other sensitive data on them. Passwords should be put on all files stored on a USB stick. This limits the damage that can be done if they are lost. Data should be securely removed as soon as it's no longer required.

Commented [LI4]: Storage Device USB – I have added up to the email address myself as we have advised principals not to use them. I don't think we are IT savvy enough for people to check and encrypt new usb or ones from clients etc.

Confidential, sensitive or personal data should not be stored on mobile devices unless it is absolutely necessary. If confidential, sensitive or personal data is stored on a mobile device it must be appropriately secured and comply with all policies in this document and or client specific policies where they have stronger controls. Data stored on mobile devices must be securely disposed of in accordance with the method stated in the *Directories of Data and Assets and Risk and Systems and Retention Schedule*.

Access to data should only be provided to appropriate individuals – data access should be provided on the principle of least privilege.

Data should not be held on the Company systems for any longer than is necessary. Once the data is no longer required by the Company it must be deleted securely from all the Company systems.

Confidential data should not be sent via unsecured wireless services.

6 Network Security, Access & Authentication

6.1 Overview

The Company and its clients seek to provide secure network infrastructure in order to protect the integrity of its data and mitigate risks of a security incident. As the Company network and clients' networks will be set up differently, a

User must familiarise themselves with the respective client network security direction and policies. The following covers all IT systems and devices that comprise the Company and or client networks or that are otherwise controlled by them e.g. Cloud based hosted systems and data. As a minimum and in order to protect the Company and its clients against security risks Users must adhere to the following basic protections:

Wherever possible, access client networks, systems and data using client supplied equipment or via terminal services or remote desktop technologies. When using the Users own equipment, reasonable measures to protect the Company and clients networks, systems and data, complying with all applicable policies should be taken. The User should take all reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her contracted duties. Existence of access capabilities does not imply permission to use the access.

When accessing client networks, systems and data using the Users service company devices, the User must make all reasonable efforts to ensure suitable antivirus and malware protection is active and up to date on all devices the User uses to deliver the Users contracted services to the Company and its clients. The User should ensure that all software and operating systems are regularly patched and up to date, in order to protect against cyber threats by installing recently released security and vulnerability patches to protect the software, data and hardware that the User uses to deliver the Users contracted services to the Company and its clients.

The User should always check that they only have the minimum level of access to systems, files and data that they require to fulfil the their contractual obligations. This will minimise the overall risks to the User, the Company and the client. When using the Users own equipment to connect to client networks remotely the User should always connect via the client provided VPN where available.

6.2 Wireless access

The User should avoid accessing Company or client systems, data and information from public networks in order to protect confidential, sensitive and personal information. If access to a public network cannot be avoided, then the User must take all reasonable precautions to protect the data and information from being accessed, stolen or amended by unauthorised individuals or entities.

6.3 Connecting to Unsecured Networks

Use caution when connecting to any network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a public network, access provided by a hotel, an open or for-pay wireless hotspot, a conference network, or any other network not under direct control of the Company, client or User. Use of these networks must be in conjunction with taking all reasonable and appropriate measures to safeguard the data and information being processed and stored.

6.4 Inactivity

The User should disable their wireless capability when not using a wireless network. This will reduce the chances that the device could be compromised from the wireless connection points.

6.5 Virtual Private Network Policy (VPN)

A Virtual Private Network (VPN), provides a method to communicate with remote networks, systems and data over a public medium, such as the Internet. For client sites, the User should familiarise and abide by the respective client directed network security access and policies.

6.6 CRM & Application data

All of the Company's core business software applications and file system data storage are hosted offsite. The infrastructure for CRM databases and associated application servers is managed and maintained via a cloud-based application. The Company actively manages the security features of its applications and its CRM for the protection of its Users and clients' data.

The Company's software applications and data are hosted by industry-leading Cloud Service providers, whose data centres have been thoroughly tested for security, availability and business continuity.

The Company's CRM retains limited information about individuals - name, email address, postal address and phone - which are retained for account contact purposes.

The Company takes a multifaceted approach to application security, to ensure the processes in place to care for our own and our clients' data comply with the highest standards of security.

Further details about specific software security can be found on the *Directories of Data and Assets and Risk and Systems and Retention Schedule*.

7 Email

7.1 Overview

Email is an essential component of business communication; however, it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on the Company's liability by providing a written record of communications. The Company recommends that all emails sent by Users using a client's email address are copied to that Principal's or Regional Director's company email address. This can help provide evidence should it be needed in defence of any claim or assertion made by a client should access to the client's system be terminated. This policy outlines expectations for appropriate, safe, and effective email use. Always minimise the personal data to what is necessary for the defence of any claim.

7.2 Scope

The purpose of this section of the policy is to detail the Company's usage guidelines for email. This policy will help the Company reduce risk of an email-related security incident, foster good business communications, both internal and external to the Company, and provide for consistent and professional application of the Company's email principles. Where there is no email policy in place with a client, the User will ensure they apply this policy to all email communications associated with the client.

7.3 Use of Company Email Systems

Common sense should be exercised at all times when sending or receiving email from Company accounts. Email sent from a Company account reflects on the Company, and, as such, email must be used with professionalism and courtesy at all times and for business communications only.

The following activities are prohibited (this list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited.):

7.3.1 Personal use of the Company email system;

7.3.2 Spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes are never permitted.

7.3.3 Forging email header information or attempting to impersonate another person.

7.3.4 Deleting email in an attempt to hide a violation of this or another company or client policy. Further, email must not be deleted when there is an active investigation or litigation, where that email may be relevant.

7.3.5 Unauthorised emailing of any Company data to external email accounts for the purpose of saving this data external to Company systems

These steps must be adhered to:

7.3.6 Access to Company email mobile devices is permitted provided the User takes all necessary steps and precautions to safeguard the data and information from being lost, stolen, unrecoverable or accessed by unauthorised individuals or entities.

7.3.7 All reasonable precautions must be taken before opening email attachments or clicking on imbedded links to prevent activating malware and viruses.

7.3.8 Use all reasonable care and attention when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists, in order to avoid inadvertent information disclosure to an unintended recipient.

7.3.9 The User is responsible for applying all necessary security measures to ensure that confidential, personal and sensitive data is protected against loss or unauthorised use in accordance with all applicable laws and regulations.

7.3.10 The Out of Office functionality within Office 365 should be used if the User will be out of the office for an entire business day or more.

7.3.11 Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the User's email account manageable, reduce the burden on the Company to store and backup unnecessary email messages and to ensure compliance with GDPR.

7.3.12 Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

7.4 Termination

On termination of a contractual relationship, the Company will disable the User's access to the account by password change, disabling the account, or another method. The Company is under no obligation to block the account from receiving email and may continue to forward inbound email to another User or set up an auto-response to notify the sender that the User is no longer engaged through the Company.

7.5 Data loss prevention

The Company may employ data loss prevention techniques to protect against leakage of confidential data at its discretion. Company e-mails are NOT private and can be accessed and read by the Company.

7.6 Legal rights to emails

The Company owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the Company and may be subject to use for purposes not anticipated by the User within the constraints of current laws and regulations.

8 Mass Emailing

The Company makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with the Company's employees or customer base) and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is the Company's intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, the Company requires that email sent to more than twenty (20) recipients external to the Company have the following characteristics:

- The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do) together with a link to the relevant privacy policy. Unsubscribe requests must be honoured immediately.
- The email must contain a subject line relevant to the content.
- The email must contain contact information, including the full contact details of the sender.
- The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

Commented [JR5]: Is this what we are doing?

Commented [JR6]: Is this what we are doing?

Note that emails sent to Company employees, existing customers, Regional Directors, Principals and or persons who have already inquired about the Company's services are exempt from the above requirements.

9 Passwords and Accounts

A solid password policy is perhaps the most important security control the User can employ to protect the data and information that they own, process and manage on behalf of others. The responsibility for choosing robust passwords falls on the User. A poorly chosen or managed password may result in unauthorised access and/or exploitation of the Company and their clients' resources. All Users, with access to the Company and/or its clients' networks, systems and data, are responsible for taking the appropriate steps to select and secure their passwords.

The User should always implement the strongest passwords and passphrases practical and possible, in order to protect against hacking or unauthorised access to data and information. Passwords must always remain confidential, protected and managed appropriately to protect unauthorised access to Company, client systems, data and accounts.

Access to the Company's systems is provided on an as-needed basis and Accounts will be deleted when the User leaves the company.

The following requirements for accounts must be maintained at all times:

- Accounts must only be provided where there is a legitimate business need
- Generic accounts are not allowed, an individual must own each account.
- No-one should share their account details with someone else.
- Accounts must always have an expiry date. Standard expiry dates should be no longer than 90 days. Accounts that have expired must be deleted after a further 60 days of inactivity.
- Accounts for leavers must be locked as soon as the leaver has finished with the business.

Passwords are an integral part of information security and the following requirements for passwords must be maintained at all times.

- Passwords must expire after a maximum of 90 days
- Passwords must be a minimum length of 8 characters – preferably passwords should be long, i.e. 16 or more characters. The longer, the better. Numbers and non-alpha characters such as !, *, %, etc should be used where possible, to further increase security.
- Passwords must not be reused for at least 12 months
- Passwords must not be sequential
- Passwords should never be written down, but password managers are an approved method for storing passwords.

10 Backup

Backups are similar to an insurance policy - they provide the last line of defence against data loss and sometimes can be the only way to recover from a hardware failure, data corruption, or a security incident. Having an appropriate backup policy and adhering to this is amongst the most important protections against loss of data and information.

It is the Users responsibility to implement appropriate safeguards to protect all data and information that the User processes in connection with the Users contractual obligations to the Company and in the delivery of services to its clients. The User should make sufficient provision to be able to recover all data in the event of a hardware failure, disaster or security incident, without adversely impacting on the Company or client's operations. Backup data should be secured to the same standards as any other confidential, personal or sensitive information.

11 Application Engineering and Development

The Company's CRM has an element of customisation which has been performed by a contractor approved by the Company for such purposes. The Company also takes advice on security best practices from this contract developer.

12 Operational Security

The Company understands that formal procedures, controls and well-defined responsibilities need to be in place to ensure continued data security and integrity.

The recruitment process includes standard background verification checks (references and credit check) on all new principals, consultants, agents, contractors, and/or employees. All principals, consultants, agents, contractors and/or employees are provided with adequate training about the information security policies of the company and are required to sign that they have read and understood the company's security-related policies. Confidential information about the company is available for access only to select authorised the Company principals, consultants, agents, contractors and/or employees.

Principals, consultants, agents, contractors and/or employees are required to report any observed suspicious activities or threats. The Data Protection Team takes appropriate disciplinary action against principals, consultants, agents, contractors and/or employees who violate organisational security policies. Security incidents (breaches and potential

vulnerabilities) can be reported by Principals, consultants, agents, contractors and/or employees and clients via email: data@yourrighthand.co.uk.

The Company maintains an inventory of all information systems used by principals, consultants, agents, contractors and/or employees for business purposes. All principals, consultants, agents, contractors and/or employees work on their own laptops/PCs and have read and understood the Data Security Policy. Development activity is only outsourced to suitably approved suppliers.

The company has a *Data Protection Policy*, approved by the Board of Directors.

13 Responsibilities

All formal processes and security standards at the Company are designed to meet regulations at the industry, state and European Union levels.

Use of our service by clients in the European Economic Area ("EEA"), may include the processing of information relating to their clients. We are Data Processors and Data Controllers for the clients from whom we collect data for purposes of the European Union ("EU") General Data Protection Regulation (GDPR). Our EEA based clients, who control their customer data and send it to the Company for processing, are the "Controllers" of that data and are responsible for compliance with the GDPR.

In particular, the Company 's clients are responsible for complying with the GDPR and relevant data protection legislation in the relevant EEA member state before sending personal information to the Company for processing.

As the processors of personal information on behalf of our clients, we follow their instructions with respect to the information they control to the extent consistent with the functionality of our service. In doing so, we implement industry standard security, technical, physical and administrative measures against unauthorised processing of such information and against loss, destruction of, or damage to, personal information as more fully described the Company's *Data Protection Policy*.

14 Reporting issues and threats

Compromise of a password or computer can have a catastrophic impact on network, systems and data security. The User should immediately report any suspicious activity or compromise involving his or her passwords to the Data Protection Team using the email address data@yourrighthand.co.uk. Any request for passwords over the phone or email, whether the request came from THE COMPANY/client personnel or not, should be ignored and immediately reported. When a password is suspected to have been compromised or a system infected / breached, the User must change all of his or her passwords immediately and report the incident

If a security incident or breach of any security policies is discovered or suspected, the User must immediately notify the Company and if associated with a clients, systems, network or data, the client. All incidents must be reported by email to Data@yourrighthand.co.uk

Examples of incidents that require notification include:

- Suspected compromise of login credentials (Username, password, etc.).
- Suspected virus/malware.
- Loss or theft of any device that contains Company information.
- Loss or theft of any ID badges, key card etc.
- An attempt by any person to obtain a User's password.
- Loss on any confidential, personal or sensitive information.
- Any other suspicious event that may impact the Company's or client's information security.

Users must treat a suspected security incident as confidential information and report the incident only to the respective authority within the Company (Data@yourrighthand.co.uk) and the client if applicable. Users must not withhold information relating to a security incident or interfere with any investigations.

The Users report will be looked into immediately. We might ask for the Users guidance in identifying or replicating the issue and understanding any means to resolving the threat right away. Please be clear and specific about any

information you give us. We deeply appreciate the Users help in detecting and fixing flaws at THE COMPANY and will acknowledge the Users contribution openly once the threat is resolved.

15 Records management

Staff must maintain all records relevant to administering this policy and procedure in electronic form in a recognised the Company recordkeeping system.

15.1 Retention

The need to retain data varies widely with the type of data. Some data can be immediately deleted, and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the Company's guidelines on retention are consistently applied. Refer to separate Company and client retention policies for requirements. As a basic principle, Company and client data stored on non-Company or client hardware must only be stored with the express written permission of the data controller, as defined under GDPR. Where written agreement has been obtained for the storage and processing of data and information, the personal data stored should be limited to the data necessary for you to deliver the services and storage should be for no longer than is required to complete the agreed work.

Commented [JR7]: And this would usually be the client.

15.2 Data Destruction

When the Company or client data stored on Users hardware has fulfilled the purpose that it was stored for and where the Company or client have up to date copies of the data in question, the data should be removed from all non-Company and non-client hardware in a timely manner. Where there are defined retention policies covering the data and these timeframes expire, the data must be actively destroyed in accordance with those policies.

On identifying data that should be destroyed the Users should first obtain written confirmation from the Company and or client that the data can be destroyed. Users must not destroy data in an attempt to cover up a violation of local/international laws or Company policy.

When hardware belonging to a User storing any Company or client data that is no longer required, it is the responsibility of the User to ensure that the data is completely unrecoverable and should be securely erased to using appropriate tools.

15.3 Transfer

Users are responsible for ensuring adequate and reasonable steps are taken to protect all Company and client data that is transferred from one device or location to another to assure its security and integrity from unauthorised access or manipulation. Whenever data is being transferred from one device to another it is good practice to encrypt in order to help prevent data loss. This is of particular importance when transmitting data across the internet. Encrypting the data first, provides effective protection against interception of the communication by a third party whilst the data is in transfer. It is also good practice to use encrypted communication when transmitting any data over a wireless communication network (e.g. Wi-Fi) or when the data will pass through an untrusted network. Data can be transformed into an encrypted format and transferred over a non-secure communication channel, yet still remain protected.

15.4 Client data

At all times, Users are responsible for taking appropriate measures to protect Company and client data from becoming lost, stolen or accessed by unauthorised individuals or entities. In doing so the User must ensure that they comply with applicable regulations and abide by local and international law.

16 Policy Compliance

16.1 Compliance monitoring and measurement

This policy will be enforced by the Data Protection Team of the Company. The Company may verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, internal and external audits, and feedback to the policy owner.

16.2 Exceptions

Any exception to the policy must be approved by a board member in advance.

Commented [JR8]: Or by the Management Team?

16.3 Non-Compliance

The Company reserves the right to terminate any third-party contracts through non-compliance to this policy.

16.4 Alteration of this Policy

This policy will be subject to review, revision, change, updating, alteration and replacement in order to introduce new policies from time to time to reflect the changing needs of the business and to comply with current legislation.

17 Terms and Conditions

General Data Protection Regulation (GDPR)
The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller
The entity that determines the purposes, conditions and means of the processing of personal data

Data Processor
The entity that processes data on behalf of the Data Controller

Data Protection Authority
National authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union

Data Protection Team (DPT)
An team of experts on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR

Data Subject
A natural person whose personal data is processed by a controller or processor

The Company
Your Right Hand Finance Ltd, a company registered in England under number 06239695, whose registered office is at The First Floor, The IQ Hub Farnborough Business Park, Fowler Avenue, Farnborough, Hants, England, GU14 7JF

The User
Principals, Regional Directors, consultants, agents, contractors, and/or employees, including part-time, temporary, or contract employees and other people working on behalf of the Company

Personal Data
Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person

Privacy Impact Assessment
A tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data

Processing
Any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling
Any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour

Regulation
A binding legislative act that must be applied in its entirety across the Union

Soft data
Any data that is stored electronically

Hard data
Any data that is stored non-electronically, for example, but not exclusively, printed data on paper

Subject Access Right
Also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them

18 Implementation of Policy

This Policy shall be deemed effective as of 1st December 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

19 Related legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

20 Feedback and suggestion

Users may provide feedback and suggestions about this document by emailing data@yourrighthand.co.uk