

# KashFlow HR GDPR FAQs



## Table of Contents

Introduction .....	3
IRIS Data Protection Officer .....	3
Frequently asked questions .....	4
Risk analysis.....	4
Information systems.....	5
Physical security .....	6
Personnel security .....	7
Organisation .....	8
Security policy .....	9
Asset management.....	10
Incident management .....	11
Business Continuity .....	12
Compliance.....	13
Appendix 1: IRIS Information security and acceptable use policies .....	15
Appendix 2. IRIS Software Group data protection policy .....	26
Appendix 3: Acceptable use of assets .....	36
Appendix 4: Critical incident process .....	41
Appendix 5: IRIS Business Continuity Plan statement.....	51
Appendix 6: ISP03- HR.....	52
Appendix 7: Rackspace.....	54
Appendix 8: Insurance cover confirmation .....	65

## Introduction

The following document outlines frequently asked questions regarding the policies and procedures that KashFlow have in place to ensure best practice in terms of data protection and company management. This is designed to support our GDPR compliance strategy. This document will cover how KashFlow manages data security, critical incidents, use of assets, HR, remote working, product development, mobile apps, network security, access controls, data backups, cryptography, supplier relationships, physical security and business continuity.

This document has been completed by members of the IRIS & KashFlow Product Management, IT, Dev Ops, Development & Business Continuity teams, under the overarching governance of a Data Protection Officer.

## IRIS Data Protection Officer

In June 2016, IRIS appointed a Data Protection Officer (DPO) to meet the requirements of Articles 37 to 39 of the General Data Protection Regulation.

At IRIS, the DPO role includes the following tasks:

- a) To inform and advise IRIS decision-makers, who carry out processing of their obligations under the relevant data protection laws.
- b) To monitor compliance with data protection law, and in accordance with IRIS policies in relation to the protection of personal data; including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations and any related audits.
- c) To provide advice where requested regarding data protection impact assessments (DPIAs), and to monitor DPIA performance in line with Article 35 of the GDPR.
- d) To co-operate with the Information Commissioner's Office, and to act as the contact point on any issues relating to the processing of personal data.

In line with their responsibilities under GDPR, the IRIS Product Management team ensure that the DPO is involved properly, and in a timely manner, in all issues which relate to the protection of personal data. The DPO has therefore been consulted in relation to product gap analysis and risk assessments in respect of data protection and GDPR – a project initiated at the end of 2016.

The DPO reports directly to the Chief Information Officer and, in line with GDPR Article 38, does not receive any instructions regarding the exercise of his statutory tasks.

Any individual affected by the personal data processing carried out by IRIS may contact the DPO ([dataprotection@IRIS.co.uk](mailto:dataprotection@IRIS.co.uk)). The DPO is bound by confidentiality concerning the performance of statutory tasks in accordance with the law.

## Frequently asked questions

### Risk analysis

1: Does KashFlow have access to, process or store any client assets (including data) in the delivery of its service?

A: Yes, KashFlow processes and stores client assets, including data. This includes personal and sensitive data as defined by the Data Protection Act.

2: Where does KashFlow hold client data?

A: KashFlow holds client data on servers based on the UK mainland.

3: How many KashFlow members of staff have access to clients' data?

A: Less than 15 KashFlow staff have access to client data.

4: Does KashFlow use sub-contractors to help in the delivery of its service?

A: KashFlow uses sub-contractors to help in the delivery of its consultancy services.

5: How does KashFlow use ICT systems to deliver its service?

A: KashFlow uses its own ICT systems to help deliver its service. Further information about ICT policies can be seen below:

We permit the use of removable media	<input checked="" type="checkbox"/>
We permit remote working	<input checked="" type="checkbox"/>
We allow staff to connect their own devices to our ICT systems	<input checked="" type="checkbox"/>

6: Where does KashFlow deliver its service from?

A: KashFlow delivers its service from a leased premises in Leeds.

## Information systems

1: What accreditations and certificates does KashFlow hold in relation to its ICT services?

A: Please see Appendix 1 for a copy of the ISO27001 certificate.

2: Has a technical risk assessment been performed on the KashFlow HR system to identify a set of proportionate risk treatment controls?

A: A technical risk assessment is performed on the KashFlow HR system every time there is a significant change in a risk component.

3: Does KashFlow have security operating procedures in place to govern the use of ICT systems?

A: KashFlow has security operating procedures in place to control the use of ICT systems, and these cover home and mobile working.

4: Are access controls in place to ensure information is only available to KashFlow HR users who require access?

A: Controls are in place to ensure information is only available to KashFlow HR users who require access. This is documented in the Access Control Policy.

5: Are acceptable use policies in place which outline the rules for acceptable use of information and assets?

A: Yes, policies are in place which outline rules for the acceptable use of information and assets.

6: Does KashFlow have policies and controls in place to manage the risks of working in non-secure environments?

A: Yes, policies and controls are in place to manage the risks of staff working in non-secure environments.

7: Are backup copies of information and software taken by KashFlow regularly?

A: Backup copies of KashFlow information and software are taken regularly, and are tested in accordance with our backup policy.

8: Has the security of KashFlow's ICT systems been evaluated through penetration testing?

A: KashFlow's ICT systems were penetration tested by CESG in March 2017.

## Physical security

1: Has a review of KashFlow's security risk assessment been carried out at sites used to process or store client assets in the last 12 months?

A: KashFlow's security risk assessment is reviewed annually and changes are made accordingly.

2: What controls do KashFlow have in place to ensure the physical security policies are fit for purpose?

A: A regime is in place to test the physical security controls against the operational requirements.

3: Are processes and controls in place to ensure that equipment and cabling is protected and maintained so as to preserve the confidentiality, integrity and availability clients' assets?

A: Yes, processes and controls are in place to ensure that equipment and cabling is protected and maintained.

## Personnel security

**1: Are background verification checks carried out on KashFlow employees and contractors who have access to client assets?**

A: Background verification checks are carried out on all KashFlow employees who have access to client assets.

**2: Does KashFlow keep full and up to date personnel security records of all employees in order to review clearance in advance of its expiration?**

A: Full and up to date personnel security records are kept for all employees.

**3: Are organisational and individual responsibilities for information security clearly defined in the terms and conditions of employment contracts?**

A: Yes, organisational and individual responsibilities for information security are clearly defined in the terms and conditions of employment contracts.

**4: Are non-disclosure agreements in place with all staff who have access to client assets?**

A: Non-disclosure agreements are in place with all staff who have access to client assets.

**5: Are mechanisms in place to ensure KashFlow employees and contractors receive appropriate information security awareness training upon appointment, and regular updates to organisational policies and procedures, as relevant for their job function?**

A: All staff and contractors receive appropriate information security training relevant to their job role. This includes Cyber Essentials training. This training is incorporated into the new starter induction process, and is renewed annually.

**6: Is a disciplinary process in place for employees and contractors who have committed a security breach?**

A: Relevant disciplinary procedures are in place for any employee or contractor who commits a security breach.

**7: Upon termination of employment, is there a process in place to ensure assets are returned and rights to assets revoked?**

A: A process exists to ensure assets are returned and rights revoked upon an employee having their job role terminated.

## Organisation

1: Does KashFlow have a senior individual responsible for the security of client information?

Vincenzo Ardilio	Alex Cutler
Data Protection Officer	Chief Information Officer
<u>Vincenzo.Ardilio@iris.co.uk</u>	<u>Alex.Cutler@iris.co.uk</u>

2: Are the security roles and responsibilities of KashFlow employees clearly defined and documented in accordance with the information security policy?

A: Yes, all security roles and responsibilities for KashFlow staff are clearly defined and documented.

3: Are processes in place to ensure KashFlow is kept up to date on relevant current and emerging:

Information security best practice	<input checked="" type="checkbox"/>
Government policy and legislation	<input checked="" type="checkbox"/>
Threats and vulnerabilities	<input checked="" type="checkbox"/>
Technologies	<input checked="" type="checkbox"/>

4: Is a corporate approach to risk management in place which enables the escalation of project risks to programme and/or organisational level risk registers?

A: Yes, processes are in place that allow the easy escalation of project risks to programme or organisational level risk registers if required.

5: Is a process in place to manage a change to systems, such as capacity management or separation of testing environments?

A: Yes, processes are in place to easily allow the management of changes to the system.

## Security policy

1: Is a security policy in place that sets out KashFlow's overall approach to protecting valuable assets?

A: Various security policies have been created and put in place, which outline KashFlow's approach to protecting valuable assets. This policy has been approved by senior management, made accessible to all staff, been reviewed in the last 12 months.

This security policies reference the following:

The importance of security to KashFlow	<input checked="" type="checkbox"/>
Legislation and regulation that KashFlow is required to be compliant with	<input checked="" type="checkbox"/>
Staff responsibilities for information	<input checked="" type="checkbox"/>
Incident and breach management policies	<input checked="" type="checkbox"/>
Business continuity arrangements	<input checked="" type="checkbox"/>
Staff training and awareness requirements	<input checked="" type="checkbox"/>

Please see Appendices 2, 3, 4, 5, 6 and 7 for the policy documents.

## Asset management

1: Has an owner been assigned to all information assets which require protection?

A: Yes, an appropriate owner has been assigned to manage all information assets which require protection.

2: Is an asset register in place that identifies and records the value of sensitive assets which require protection?

A: Yes, an asset register is in place that identifies and records the value of all sensitive assets.

3: Does KashFlow have policies in place which detail how client assets should be handled?

Yes, KashFlow has policies in place which detail how client assets should be handled, copied, stored, transmitted, destroyed and returned.

4: How are these procedures communicated to staff?

A: All security policies are centrally available to staff and can be accessed any time.

## Incident management

1: Do KashFlow have policies in place which set out how information security incidents, and breaches to the confidentiality of data, should be managed and who it should be escalated to?

A: KashFlow have policies in place which outline how information security incidents and data breaches should be managed. They include the following information:

Individual responsibilities for identifying and reporting security incidents and information security breaches	<input checked="" type="checkbox"/>
A reporting matrix including escalation points	<input checked="" type="checkbox"/>
An up to date list of relevant internal and external contact points	<input checked="" type="checkbox"/>
A timeline detailing at which point the policy should be implemented	<input checked="" type="checkbox"/>

See Appendix 5 for further details.

2: In the event of a loss or breach to a client's assets, what action would KashFlow take first?

A: In the event of a loss or breach of a client's assets, KashFlow would notify the customer without undue delay. See attached incident management procedure for details at Appendix 5.

## Business Continuity

1: Does KashFlow have business continuity and disaster recovery plans to maintain or quickly resume any services supplied?

A: Business continuity and discovery plans are in place to ensure any disruption caused is minimal. Please see attached BCP statement in Appendix 6.

2: Are processes in place to ensure business continuity management arrangements are tested and reviewed?

A: Yes, we review our business continuity management arrangements every 12 months.

## Compliance

1: How does KashFlow ensure that relevant legislation and regulation is understood?

A: To ensure KashFlow understand relevant legislation and regulation, contact with relevant authorities is maintained and changes are reviewed to determine the impact for businesses. All relevant legislation and regulation is referenced in internal policies, plans and procedures.

2: In the past 12 months, has KashFlow assessed its compliance with relevant legislation and regulation, such as the Data Protection Act?

A: KashFlow has assessed its compliance with relevant legislation and regulation, and an action plan has been created to address weaknesses. In particular, a 'GAP' analysis has been carried out in respect to the upcoming GDPR.

3: Are processes in place to ensure that KashFlow assess the risks to assets that are shared with delivery partners and third-party suppliers?

A: Yes, processes are in place to ensure that KashFlow assess the risks to assets that are shared with delivery partners and third-party suppliers.

4: How does KashFlow gain assurances that delivery partners and third-party suppliers are compliant with its security policies?

Information security requirements are detailed in contracts	<input checked="" type="checkbox"/>
The need to meet recognised standards (such as ISO27001: 2013) is stipulated	<input checked="" type="checkbox"/>
The organisation's compliance is measured through self-assessment	<input checked="" type="checkbox"/>



## Appendix 1: IRIS Information security and acceptable use policies

Version number	1
Author	Vincenzo Ardilio
Date of issue	27 March 2017
Document type	ISMS Policy summary
Replaces	N/A
Approved by	Executive Committee
Approval date	
Data Protection Impact Screening	No PIA required

IRIS has approved an Information Security Management System (ISMS) to provide uniform control and guidelines for everyone using KashFlow's information systems. This is an overview of the ISMS, which contains the key 'dos and don'ts'. All staff must agree to observe these day-to-day requirements to help keep our information and systems secure.

Please refer to the full ISMS for more detailed explanations of the standards listed in this summary.

### Passwords and access to systems, information and premises:

#### Do

1. Only access and use information, applications and systems in line with your authorised job accountabilities – this refers to the “need to know” principle.
2. Use the internet connection provided by IRIS with your business mobile device whenever you are working from IRIS premises.
3. Use different passwords and log in credentials for business and personal matters.
4. Protect devices with a PIN, password or auto-lock.
5. Use a strong password of at least eight mixed characters (passphrases of three random words are easier to remember and are more secure).
6. Be aware of who can see personal and business-sensitive information displayed on your computer monitor or device when you are working. Be especially vigilant in open-plan areas, public places and at home.
7. Always lock your computer or device when leaving it unattended (such as by pressing 'ALT+CTRL+DEL' or activating the locking mechanism on your device).

## Don't

1. Use another user's ID or password, disclose your own to anyone else, or use a generic user ID or password.
2. Allow others to share your access card, or allow anyone you don't recognise to enter IRIS premises without checking their ID.
3. Write down your passwords and leave them in an unsecured environment.
4. Use remote access to IRIS applications and systems unless authorised to do so.

## Using email and the internet:

### Do

1. Be suspicious of unexpected emails from unknown or unexpected senders – do not click on links in these emails or open attachments. Report to the IT Service Desk before doing anything further.
2. Be extremely careful when addressing emails. Make sure you are sending the email to the right person. Danger areas are auto-complete and 'reply to all'.
3. Take into account that IRIS monitors internet use, websites visited and files downloaded.
4. Treat emails as official communications, and use the same rules of grammar, content and record-keeping as for other business communications.

### Don't

1. Include any personal information in a 'normal' email that you would not be happy to put onto a postcard ('normal emails' are unencrypted emails sent over the public internet).
2. Use email for any illegal activity, or to compromise the security or operation of any computer system or network.
3. Use the internet for illegal, unethical or personal business activity, in a way that would compromise security or for peer to peer file sharing.
4. Create, send or forward any email or social media messages which may be considered discriminatory, defamatory, intended harassment or hatred.
5. Visit, interact with or download content from offensive, obscene, pornographic or violent websites.
6. Bypass official corporate systems to connect to the internet – for example, by using mobile broadband cards, pairing hotspots, external modems, wireless usb, or any other mechanisms. However, mobile computing facilities may be used when working remotely.

## Making changes to your work device

### Do

1. Only upgrade new applications or allow software upgrades from a recognised source, and ensure they do not impact the device's functionality or security, nor incur additional costs. Please contact IRIS's IT service desk if in doubt.
2. Ensure that changes to configuration or maintenance of the device are carried out by IRIS IT staff, or their designated agent.

## Keeping information and IT secure

### Do

1. Take extra care with USB sticks, removable storage and portable devices, and do not store confidential information on them unless the information is encrypted.
2. Use secure printing for confidential or potentially sensitive information. Secure printing is explained in detail in the ISMS.
3. Store corporate information in secure shared drives rather than on the local drive of your device.
4. Be aware of your obligations under data protection legislation when dealing with or using personal data – see IRIS Data Protection Policy for more details on this.
5. Shred paper records containing confidential information, or use confidential waste bins.

### Don't

1. Disclose or publish corporate or confidential information belonging to IRIS or its customers, unless authorised and permitted by IRIS's policies and procedures or as required by law.
2. Create or maintain a blog, Wiki or social media site on behalf of IRIS without express permission to do so.
3. Dispose of potentially important company information without the approval of the information owner.
4. Lend business mobile devices allocated to you to anyone external to the company, including friends and family.
5. Introduce any viruses to IRIS systems. This includes any computer codes that will adversely affect the performance or security of our systems or networks.
6. Damage, alter or disrupt IRIS computers systems or networks, including obtaining passwords, encryption keys or anything that would allow unauthorised access by you or anyone else.
7. Connect devices to our networks, unless the IT Technical Manager has approved the device.

## Miscellaneous

### Do

1. Remember that mobile devices and communication systems supplied by IRIS (including email and the internet) are provided for business activities. Reasonable and appropriate personal use is permitted, but this must not impact on productivity and must be within the strict limits set out in full in the 'Acceptable Use' Policy. Keep in mind use may be monitored.
2. Remember that intellectual property created or developed by IRIS employees during working hours and/or with IRIS equipment is IRIS's property.
3. Avoid actual or potential conflicts of interest, such as accessing IRIS customer data for private business purposes.

### Don't

1. Use social media for personal use during working hours.
2. Make or accept premium calls, reverse charges, international calls and similar, unless for essential business purposes.
3. Use IRIS systems to engage in any activity which causes, or could be construed as causing harassment, discrimination or victimisation.
4. Abuse licence agreements by copying or installing third party software multiple times (unless allowed by the licence agreement).

## Serious misconduct

Any actions or activities (intended or accidental) causing, or with potential to cause the compromise of IRIS computer systems, information or networks is serious misconduct. This includes:

- Security breaches or disruptions of network communications. Disruption may include network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.
- Unauthorised port scanning or security scanning. This can only be sanctioned by the IT Director (Group Systems) for the purposes of testing network security.
- Network monitoring which will intercept data not intended for the employee's host, unless this activity has been authorised.
- Circumventing user authentication or security of any host, network or account or running password cracking programs.
- Interfering with, or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent of interfering with or disabling a user's session.
- Downloading, installing or executing any file containing malware which may damage or compromise computer systems or data.
- Unauthorised copying or altering configuration or system files.
- Interfering with IRIS's or another organisation's email service.
- Downloading or introducing tools or utilities that may potentially be used for hacking activities and undertaking any such activity on any system whether owned or managed by the company or not.
- Providing or selling company information, customer data or personal data without approval and for personal gain
- Defacing websites, downloading and distributing pornography, running a gambling operation or undertaking any other activity using company resources that would bring the company into disrepute.

## IRIS Information Security Management System Summary of Policies

All staff have a personal responsibility to familiarise themselves with the policies included in the ISMS. The full set of standards are published on the KashFlow system and is available to all staff. The following is a brief outline of the purpose of each Policy in the ISMS:

### Acceptable Use Policy

The purpose of the Acceptable Use Policy is to ensure that all computer systems and networks owned or managed by IRIS are operated in an effective, safe, ethical and lawful manner, and it is the responsibility of every computer user to know these requirements and to comply with them.

### Access Control Policy

The purpose of the Access Control Policy is to ensure that information systems resources and electronic information assets owned or managed by IRIS are available to all authorised personnel. The Policy also deals with the prevention of unauthorised access through managed controls to create a secure computing environment.

### Anti-Virus Policy

This Policy is about protecting networks, systems and equipment from malicious code and malware. Laptops and mobile devices are most at risk as they may only be connected to the network periodically. The appropriate use of Anti-Virus software will lessen the risk of the company experiencing this type of security incident.

### Business Continuity/DR Policy

The purpose of the IT Business Continuity/DR Policy is to ensure that IRIS has the appropriate resources available for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a Business Continuity/DR capability, that will enable the organisations to prepare for, respond to and recover from disruptive incidents when they arise. The scale of events covered by this Policy ranges from minor or partial system unavailability (business continuity) through to total system loss (disaster recovery).

### Cloud Computing Policy

The purpose of the Cloud Computing Policy is to ensure that the confidentiality, integrity and availability of the company's information is maintained when services are delivered through a Cloud Computing environment. As the Cloud can be private or public, local or international it is important to ensure that arrangements are supported by a Service agreement, meet the company's requirements for information security, and enable statutory and legislative obligations to be met.

### Communication and Mobile Devices Policy

The purpose of the Communication and Mobile Devices Policy is to advise acceptable use with regard to mobile devices (including mobile phones), and communication systems used for business activities. With the convergence of data and voice and video communication systems, the ability to connect remotely to internal systems, and the wide range of options offered by mobile devices, it is essential that these technologies be used by authorised persons for legitimate business activities.

## Computer Systems and Equipment Use Policy

The purpose of this Policy is to advise users of the company's expectations regarding the acceptable use of the technology provided to them.

### Cyber Crime and Security Incident Policy

The purpose of the Cyber Crime and Security Incident Policy is to ensure that the correct procedures are followed should systems be affected by a security incident or other event. The impact an event will have on business continuity will depend on how well it is handled.

### Email Policy

The purpose of the Email Policy is to document how electronic mail systems and services are to be used. Email has become a major communication channel and a common means of conducting day-to-day business. Compliance with these Policies is essential to ensure that important email documents become part of the corporate knowledge-base and to ensure compliance with information management and legal requirements.

### Encryption Policy

The purpose of the Encryption Policy is to ensure that encryption keys are securely managed throughout their life cycle. This includes their creation, storage and the manner in which they are used and destroyed.

### Firewall Management Policy

The purpose of the Firewall Management Policy is to ensure that the external perimeter defence for IRIS is configured, managed and maintained to prevent the occurrence of a major security threat.

### Hardware Management Policy

The purpose of the Hardware Management Policy is to ensure that the correct procedures are followed with regard to the purchase, deployment, maintenance and replacement of computer hardware and other devices.

### Information Management Policy

The Information Management Policy sets out the guidelines for managing the data and information stored in the files and directories that comprise the electronic information repositories of IRIS.

### Internet Use Policy

The purpose of the Internet Use Policy is to ensure that the internet is used for business purposes, and to ensure that users conduct their online activities in an appropriate, responsible and ethical manner.

### Laptop And Tablet Security Policy

The purpose of this Policy is to inform those who have been allocated a laptop computer or tablet of the company's requirements for its use and care. Theft, loss or damage to portable computers is becoming increasingly commonplace. The costs of replacement are not just financial and include loss of data, lost productivity, increased insurance premiums and the time to configure and set up a new machine. There

are also risks associated with the loss or exposure of sensitive, unique or personal information, including reputation, commercial advantage and privacy and this Policy seeks to mitigate these risks.

### **Legal Compliance Policy**

The purpose of the Legal Compliance Policy is to ensure that staff understand the implications of privacy, confidentiality, copyright, intellectual property, misrepresentation and other relevant legislation in respect to information and information systems.

### **Network Management Policy**

The purpose of the Network Management Policy is to protect IRIS's internal computer systems and networks from abuse or exploitation and defines the parameters for managing, designing and connecting to the company's computer systems.

### **Online Services Policy**

The purpose of the Online Services Policy is to provide the guidelines for configuring systems to safely enable business transactions to be carried out over the Internet as an alternative service channel. The term "business" can apply to anything, from providing information online to making payment for a service online, and refers providing and using online services.

### **Password And Authentication Policy**

This Policy describes the authentication requirements for accessing internal computers and networks and includes those working in-house as well as those connecting remotely. Every person, organisation or device connecting to internal IT resources and networks must be authenticated as a valid user before gaining access to IRIS's computer systems, networks and information resources.

### **Personnel Management Policy**

The purpose of the Personnel Management Policy is to ensure that those using and managing IRIS's computer systems and networks act in a responsible and ethical manner. It is also intended to minimise the threat of an internal security breach.

### **Physical Access Policy**

The purpose of the Physical Access Policy is to protect IRIS's IT resources from harm, abuse or exploitation and describes the parameters for controlling the environmental conditions for critical computing devices.

### **Remote Access Policy**

This Policy describes the security requirements for remote access connections to IT resources. It covers a wide variety of technologies and methods of effecting the connection.

### **Software Management Policy**

The purpose of the Software Management Policy is to ensure that the correct processes and procedures are followed when purchasing, developing, deploying, maintaining and replacing software applications. It assists with compliance with industry standards, encourages consistency throughout IRIS, and ensures that software continues to meet the needs of the business.

## Special Access Policy

Special Access relates to System Administrator and Domain Administrator rights. The purpose of the Special Access Policy is to ensure that only those users needing special access rights and enhanced privileges to manage the company's computer systems and networks are granted them with the appropriate controls.

## Appendix 2: IRIS Software Group data protection policy

Version number	1
Author	Vincenzo Ardilio
Date of issue	27 March 2017
Document type	Policy
Replaces	Data Protection Group Compliance Policy 2010
Approved by	Executive Committee
Approval date	
Data Protection Impact Screening	No PIA required
Date of next review	March 2018

### Introduction

IRIS acts in the capacities of Controller and Processor of personal data. We are a Processor in respect of the personal information entrusted to us by our customers in our products and solutions. We are a Controller in that we make decisions on how and why we will use personal data. For example, as an employer, we hold records about our staff. Also, as a commercial organisation, we directly market our products to prospective customers, and some data used in these campaigns will be classed as personal.

IRIS is committed to fulfilling its obligations under the General Data Protection Regulation (GDPR), and any subsequent data protection legislation. We have produced this policy to provide assurance to our customers and staff.

Later in this document we provide an explanation as to how responsibility for data protection compliance is delegated. This document also sits alongside the IRIS Information Security Management System, and is subject to ongoing review, at least annually, in light of changes in law guidance and working practice.

## Statement of data protection policy

IRIS will use personal data legally and securely regardless of the method by which it is collected, recorded and used, and whether we hold it within our products, on a Group network or device, in filing systems, on paper, or recorded on other material such as audio or visual media.

IRIS regards the proper and good management of personal data as crucial to the success of our business. Observing good data protection practice plays a huge role in maintaining customer confidence. We ensure that IRIS respects privacy and treats personal data lawfully and correctly.

We will ensure that:

- There is someone acting in the statutory role of Data Protection Officer on behalf of the IRIS Group of companies. This person is IRIS Software Group Ltd's Data Protection and Security Manager.
- Responsibility for each system or product's data protection compliance is assigned to one or more specific individuals.
- Our collection and use of personal data complies with the data protection principles, data subject rights, relevant regulations and codes of practice, wherever we are acting as Controller.
- We provide appropriate privacy notices through whatever means we collect personal data, such as on application forms, products, web pages and via telephone wherever we are acting as Controller.
- Appropriate technical and organisational measures for all of our products and Group IT systems are implemented to ensure a level of security appropriate to the risks.
- Everyone managing and handling personal data understands that they are contractually responsible for following the good data protection practice set out in this policy and the supporting guidance and standards.
- Everyone managing and handling personal data is appropriately trained, supervised and audited.
- Our privacy notices make clear to anyone that wants to make enquiries about our personal data processing, can do so through the Data Protection Officer or the product's designated data protection representative.
- Our handling and processing of personal information are regularly risk-assessed and evaluated.
- A corporate procedure is in place to report and investigate personal data breaches without undue delay.
- We keep the statutory records required under GDPR as well as any further records required to demonstrate compliance, such as risk assessments, policies, working procedures, records of consent and so on.

In addition, where IRIS is acting in the capacity of data Processor, we will:

- Provide our customers with appropriate guarantees in respect of the technical and organisational measures we have in place to protect personal data and to protect the rights of data subjects.
- Process the personal data only on documented instructions from the customer, including with regard to transfers to a third country or an international organisation.
- Ensure that persons' authorised to process the personal data entrusted to us are under an appropriate statutory obligation of confidentiality.

- Assist the customer, as far as possible, by appropriate technical and organisational measures, to fulfil the customer's obligation to respond to data subjects exercising their rights as set out in the data protection legislation
- At the choice of the customer, delete or return all the personal data after the end of the processing contract, and delete copies, unless the law requires us to store the personal data for longer

## Staff roles and responsibilities

### All Staff

All staff will:

- a) Routinely assess the kind of information they use whilst carrying out their work and whether they have responsibility for any personal data.
- b) Ensure they understand how this policy, its associated guidance notes and their local working procedures affect their work and use personal information accordingly.
- c) Follow local procedures that apply to the systems and products they have access to in order to handle personal data appropriately.
- d) Report data breaches and “near misses” in line with the corporate Critical Incident Procedure.

### Senior Management

Senior Management Team members will:

- a) Identify information assets they are responsible for which involve or affect the processing of personal information.
- b) Act as Information Asset Owners (IAOs), meaning they'll:
  - Take ownership of information assets and the extent of compliance with data protection rules.
  - Lead and foster a culture that values, protects and uses personal data ethically.
  - Understand what information is transferred in and out of the information asset(s) they are responsible for.
  - Know who has access and why, and ensure that use of the asset is monitored.
- c) Ensure that a record of processing activities is maintained in line with GDPR requirements for data Controllers (See 'Statutory Records' section).
- d) Ensure that a record of the categories of processing activities carried out on behalf of each customer is maintained in line with GDPR requirements for data processors (See 'Statutory Records' section).
- e) Understand and address risks to the asset(s), provide assurance to the CIO and Data Protection Officer, and ensure that any data risk incidents are managed in line with the Corporate Critical Incident Procedure.
- f) Appoint Information Asset Managers (IAMs) to have routine responsibility for the data protection compliance of information assets within their business unit. The aim is for clear and documented accountability for the compliance of all information assets.
- g) Ensure the Data Protection Officer has access to the register of information assets and all records associated with compliance.
- h) Ensure that the Data Protection Officer is present where decisions with data protection implications are taken, and that all relevant information is passed to the Data Protection Officer in a timely manner in order to allow provision of adequate advice.
- i) Ensure that the principles of data protection by design and default are applied to each new or major update to projects or proposals (including product development) involving the use of personal information or with potential to affect privacy. The Data Protection Officer must be

informed at an early stage of the proposal, and any corporate templates provided to meet the requirements of data protection by design and default should be used.

- j) Ensure that staff (including temporary staff and contractors) that have access to personal data also have access to instructions that include the actions they must take to protect personal data and privacy.
- k) In consultation with HR, to ensure that arrangements are in place to vet individuals (such as staff and contractors) to HMG Baseline Personnel Security Standards (BPSS) before giving access to financial data, payment card information and special category personal data for the first time.
- l) Ensure staff training needs have been communicated to the Data Protection Officer.

## Information Asset Managers

Managers who are Information Asset Managers (IAMs) will:

- a) Have day-to-day responsibility for the compliance of information assets assigned to them by the IAO.
- b) Implement control measures as required or delegated by the IAO.
- c) Where delegated, maintain the statutory records on behalf of the IAO (see 'Statutory records' system).

## Line Managers

All Line Managers will:

- a) Ensure new recruits receive training, including on the job training, on local working procedures to ensure they handle personal data in a compliant and secure way.
- b) Ensure their staff have access to training and materials including guidance, checklists and templates provided by IRIS to ensure compliance with data protection regulations.
- c) Ensure that data breaches and 'near misses' are reported in line with the Corporate Critical Incident Procedure.

## HR Services

HR Services will be responsible for the following:

- a) BPSS checks for new staff who will have access to special category personal data, financial data and payment card information, before access to systems holding such data is given.
- b) Ensure that new members of staff are made aware of this policy document at recruitment and induction stage, and also that a specific confidentiality provision is included in contracts of employment and job descriptions.

## Data Protection Officer

The Data Protection Officer will:

- a) Inform and advise the business, including any employees who carry out processing of their data protection obligations.
- b) Monitor data protection compliance against the relevant legislation and company policies in relation to the protection of personal data, the assignment of responsibilities, awareness raising and training of staff involved in the processing of personal data.
- c) Provide advice, where requested, as regards data protection impact assessments and the monitoring of the performance.
- d) Act as IRIS Group's contact point for the Information Commissioner's Office including consulting, where appropriate, with regard to any matter relating to the IRIS Group's data processing.
- e) Ensure that this Data Protection Policy, the associated documents, and guidance are kept up to date and communicated to staff in an appropriate manner.
- f) Arrange for the provision of advice and training to staff on request.
- g) Manage the notification of IRIS's processing to the Information Commissioner's Office.
- h) Investigate personal data breaches and data security incidents in liaison with the Information Asset Owner and provide recommendations to the Chief Information Officer.
- i) Act in an independent manner, and will not perform duties or tasks that would give rise to a conflict of interests.

## The Data Protection principles and Data Subject rights

### The Data Protection principles

Personal data shall be:

- a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, in regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').
- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

### Data subject rights

Data subjects have:

- a) The right to receive from IRIS any information relating to processing of personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- b) The right of access to their own personal data, a description of how it is being used, the source, how to exercise their rights and to complain etc.
- c) The right to rectification.
- d) The right to erasure ('right to be forgotten').
- e) The right to restriction of processing.
- f) The right to data portability.
- g) The right to object.
- h) The right not to be subject to automated individual decision-making and profiling.

## Statutory Records

### ‘Data Controller’

Where IRIS acts as a ‘Data Controller’, they will supply:

- a) The name and contact details of the Controller and, where applicable, the joint Controller, the Controller's representative and the Data Protection officer.
- b) The purpose(s) of the processing.
- c) A description of the categories of data subjects and of the categories of personal data.
- d) The categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organisations.
- e) Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards where relevant.
- f) Where possible, the envisaged time limits for erasure of the different categories of data.
- g) Where possible, a general description of the technical and organisational security measures in place.
- h) Records that demonstrate compliance with the data protection principles (for example, data protection by design and default records, risk assessments, training records and so on).

### ‘Data Processor’

Where IRIS acts as a ‘Data Processor’, they will maintain a record of all categories of processing activities carried out on behalf of a Controller, containing:

- a) The name and contact details of the Processor or Processors, and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the Data Protection officer.
- b) The categories of processing carried out on behalf of each Controller.
- c) Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.
- d) Where possible, a general description of the technical and organisational security measures.

## Definitions

**'Information asset'** is a body of information that is defined and managed as a single entity so that it can be understood, shared, protected and exploited effectively. For example, an information asset may be a product, database, IT system, file or filing system. In the context of managing personal data processing, it can also be useful to classify vendors, outsourced data processors (such as cloud hosts), software and hardware as information assets.

**'Personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**'Processing'** means operations, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**'Restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future.

**'Profiling'** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

**'Filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

**'Controller'** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**'Processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**'Recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

**'Consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**'Personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**'Genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

**'Biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

**'Data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

**'Representative'** means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

**'Enterprise'** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

**'International organisation'** means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

**'Third country'** means a country outside of the EU.

## Appendix 3: Acceptable use of assets

### 1. Objective

To provide a secure network environment for staff and information systems by ensuring all workstations and servers are appropriately configured with up to date antivirus, operational and security patches.

This policy defines the company requirements for all staff for working with computer equipment including workstations, laptops, tablets and all network servers. The policy must be read in conjunction with the Staff Handbook.

- Preventing the misuse of company information processing facilities.
- Protection against installation and use of malicious software.
- Ensure legal compliance with Intellectual Property Rights (IPR).
- Defines requirements for the exchange of information (e-mails, messaging or use of the internet).

### 2. Scope and Index

This procedure applies to all use of assets by KashFlow staff. Any breach of these requirements may be considered misconduct and be subject to disciplinary measures.

This procedure details the controls required by the following control objectives defined in Annex A of ISO27001:2013:

SoA Ref	Requirement
A.8.1.3	Acceptable use of assets
A.8.1.4	Return of Assets
A.8.2.3	Handling of assets
A.8.3.1	Management of removable media
A.8.3.2	Disposal of media
A.8.3.3	Physical media transfer
A.11.2.5	Removal of assets
A.11.2.6	Security of equipment and assets off-premises
A.11.2.7	Security disposal or re-use of equipment
A.11.2.8	Unattended user equipment
A.11.2.9	Clear desk and clear screen policy

### 3. Procedure

Access to KashFlow information processing facilities and systems shall be granted only where there is a legitimate business need.

Employees shall only gain access to and use information assets and information processing facilities for which they are specifically authorised.

Employees shall be allowed to use KashFlow information processing facilities for limited personal use, in addition to business use, consistent with local management requirements.

KashFlow information will only be accessed via VPN on KashFlow laptops or controlled home devices.

Employees shall note that failure to adhere to this Acceptable Use Policy will increase the risk of an information security breach for which they shall be held responsible and may lead to disciplinary action.

### 3.1 Usernames and Passwords

Employees shall be issued with a unique username and a confidential password. Passwords shall always be selected carefully and shall be kept confidential by committing them to memory.

Rules for robust password selection are defined by Active Directory. These include:

- Minimum 8 characters in length.
- Special characters, numbers and upper/lower case required.
- Changed after 90 days.
- The new password cannot be the same as the previous.

### 3.2 Malicious Software Control

Employees shall remain vigilant to the threat of malicious software to KashFlow computers at all times. Employees shall never run software or open any files without first ensuring that they are free of malicious software. Emails from unknown sources shall be treated as suspect, and reported to the IT team for investigation and reported back to the employee.

Employees using remote access using non-company devices shall be responsible for maintaining and updating their malicious software controls. They shall seek advice from the IT Team on how to do this.

### 3.3 Protection of Copyright Material

The penalties to KashFlow and employees for using unauthorised software can be significant. Employees shall only use software that has been purchased by the company. Employees shall not take copies of any KashFlow supplied software nor load any software that has not been sourced by the company.

### 3.4 Email Usage Principles

KashFlow provides email to assist employees in the performance of their jobs. Whilst its use should be primarily for official company business, incidental and occasional personal use of email shall be permitted, on the understanding that:

- Personal messages shall be treated the same as business messages.
- Personal use of the email system shall never impact the normal traffic flow of business related email.

KashFlow shall reserve the right to purge identifiable personal email to preserve the integrity of the email systems. Email shall only be used where the transmission of such information is in compliance with relevant legislation and regulation (such as that relating to credit card transactions and the Payment Card Industry Data Security Standard).

No employee shall send, forward or receive emails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company, or which may be harmful to the morale of employees. Examples of prohibited material include:

- Sexually explicit messages.
- Unwelcome propositions, requests for dates, or love letters.
- Profanity, obscenity, slander, or libel.
- Ethnic, religious, or racial slurs.
- Political beliefs or commentary.
- Any message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs.

All email traffic, including attachments, shall be monitored and reviewed, and any action deemed appropriate shall be taken.

All employees shall ensure compliance with all relevant legislation.

All information shall be owned by the company and not by individuals.

The email system shall not be used for personal financial gain.

Contractual commitments shall only be made via email by those so authorised. Any such communication shall be filed securely for later access and comply with the latest legal guidance regarding electronic mail signatures.

### 3.5 Instant Messaging and Video Calls

Should only be used for business use only.

### 3.6 Internet Usage

KashFlow provides its employees with internet access to assist them in the performance of their jobs. Whilst its use should be primarily for official company business, incidental and occasional personal use of the internet is permitted, on the understanding that:

- Personal use of the internet shall never impact the business-related Internet access or upon KashFlow operational activities.
- Access to social networks is allowed during break times.
- KashFlow reserves the right to curtail an employee's internet access to preserve its reputation and the integrity of its systems.
- Messages shall not be posted on any internet message board or other similar Web based service that would bring KashFlow into disrepute, or which a reasonable person would consider to be offensive or abusive. The list of prohibited material is the same as those for email.
- Employees shall not place on the Internet any opinion or statement that might be construed as representing KashFlow.
- Employees shall not leave their name, other identification, including the address of the computer in use, which may allow others to locate or identify the company.

- KashFlow shall report any illegal activity to the police. Employees shall also be liable to KashFlow's own disciplinary process.
- Internet access shall not be used for personal financial gain, or to host a website on any KashFlow network.
- An employee's use of the system shall not have a noticeable effect on the availability of the system for other users. Employees shall not participate in on-line games or have active any web channels that broadcast frequent updates to their computer.
- Employees shall not visit Web sites that display material of a pornographic nature, or which contain material that may be considered offensive. Employees shall notify IT team immediately should accidental access to such material occur. No disciplinary action shall be taken against employees who accidentally access sites containing dubious or unethical material providing they advise IT team in a timely manner. However, in order to avoid disciplinary action, it is the employee's responsibility to ensure that such unauthorised access does not happen on a frequent basis.
- Employees shall not download any files or software from the Internet, or capture any images that are displayed, as there may be any number of issues concerning copyright, malicious software and overall functioning of the computer.
- Employees shall not enter their email address on a Web site unnecessarily as this might expose KashFlow to security risks such as malicious software attacks or unwanted junk messages.
- Employees logged in at a computer shall be considered to be the person browsing the Internet. Under no circumstances shall employees browse the Internet from an account belonging to another employee.
- IT team shall monitor and log all Internet access by employees and reserves the right to disclose this information to any relevant authority.

### 3.7 Data Protection

KashFlow is required by law to comply with the Data Protection Act 1998, as amended from time to time, when processing personal data. Employees have a personal responsibility to ensure that they make an active contribution towards meeting these legal obligations.

In certain circumstances failure to comply with the Data Protection Act 1998 may result in employees being personally liable for such non-compliance.

### 3.8 Use of Equipment Off-Premises

Employees are allocated assets as required by their role, some of these may be allowed off-site as required.

Employees shall exercise appropriate care when using the company's information assets outside the normal office environment. This particularly applies when information is processed on laptops, tablets and mobile telephones. Users must be aware of the risk of information leakage from the use of displays screens in public places and must never view company sensitive information that might be seen by others. If in doubt wait for until a private area is available.

### 3.9 Clear Desk and Clear Screen

Employees shall ensure that the confidentiality of sensitive information is not breached whilst such files and documents are in their possession.

To facilitate such control, KashFlow operates a **Clear Desk Policy**. This means that desks and other working areas shall be cleared of all sensitive information when employees leave them unattended for any purposes.

Employees who are dealing with sensitive information shall secure it in appropriate storage whenever they leave their work station. Similarly, employees shall ensure that the confidentiality of records or facilities to which they have authorised access is not breached when they are away from their desk.

Clear Screen Policy: Whenever leaving a workstation/laptop activated but unattended, employees must lock the screen by either pressing 'CTRL/ALT/DEL' or the 'WINDOWS KEY/L'. This will blank the screen and lock the workstation so that it requires a log in password to activate.

### 3.10 Management and Disposal of Media

It is unlikely that media will be used to store sensitive information. If temporary storage is required, IT team must be contacted to determine the requirements and possible controls required (i.e. encrypted memory stick).

Data shall be transferred from any media received into secure storage on the network. Media must then be forwarded to the IT team to arrange secure destruction.

Hard discs are all securely destroyed through an approved disposal company.

### 3.11 Secure Disposal or Re-Use of Equipment

All equipment no longer required must be returned to the IT team, who will:

- Amend the location in the Asset Register.
- Store the equipment in a secure location until disposal/re-use can be arranged.
- For disposal ensure any data storage drives are securely wiped (i.e. using software available to over-write data) or the data storage drives are physically destroyed. This may be carried out in-house or via an approved sub-contractor, certificate of destruction to be supplied.
- For re-use ensure any data stored is deleted as above before the device is re-allocated. The Asset Register is amended accordingly.

### 3.12 Paper Waste

All paper waste is collected in secure bins and securely shredded via an approved secure disposal company.

If staff identify documents that are particularly sensitive (financial or personnel), they are responsible to direct shred using the office based shredders.

## Appendix 4: Critical incident process

### Introduction

The following section outlines why IRIS has a critical incident process, and what our definition of a 'critical incident' is. It also covers what a 'personal data breach' is, and walks you through IRIS's critical incident process, as well as explains the different roles and responsibilities employees will play during a critical incident procedure.

### Why have a Critical Incident Procedure?

There are many reasons why it's essential to have a critical incident procedure, such as:

#### Commercially

- Making customers feel assured that their data is stored safely and that procedures are in place to maintain its security.

#### Regulatory

- We can't comply with data protection law (Data Protection Act 1998 and GDPR) without a personal data breach procedure.
- PCI-DSS and Cyber Security Essentials dictate that we have a data breach procedure.

#### Financial

- Not having a data breach procedure can lead to unlimited financial risk through regulatory fines and litigation.

#### Good business practice

- We want to learn from critical incidents to avoid future repetition.
- It's crucial we get the business back up and running normally as quickly as possible.
- A clear data breach procedure can improve the monitoring of data and the ability to interpret the reports, which can help to identify incidents before they have an impact.
- Increase staff confidence as they know that a process exists to keep IT services working.

## What do we mean by 'Critical Incident'

Within IRIS, this is defined as:

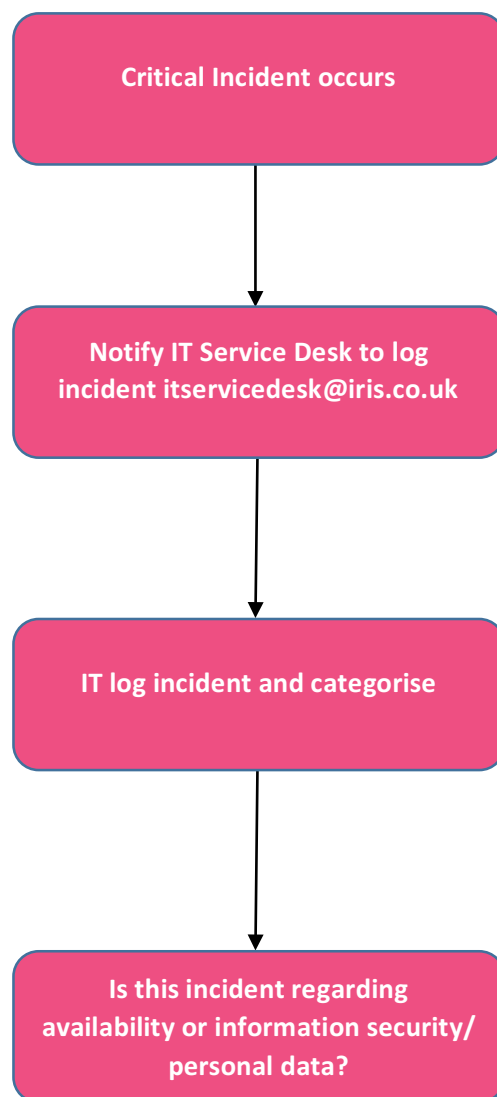
- a) An incident that prevents all site users accessing one or more critical business systems. This could be one system accessing all sites, or one site in its entirety.
- b) An incident that could have a detrimental effect on customer delivery or services.
- c) Loss or potential loss of control of confidential data (this would include actual personal data breaches and 'near misses').
- d) Unauthorised access to systems or facilities (including offices).

## What do we mean by 'personal data breach'?

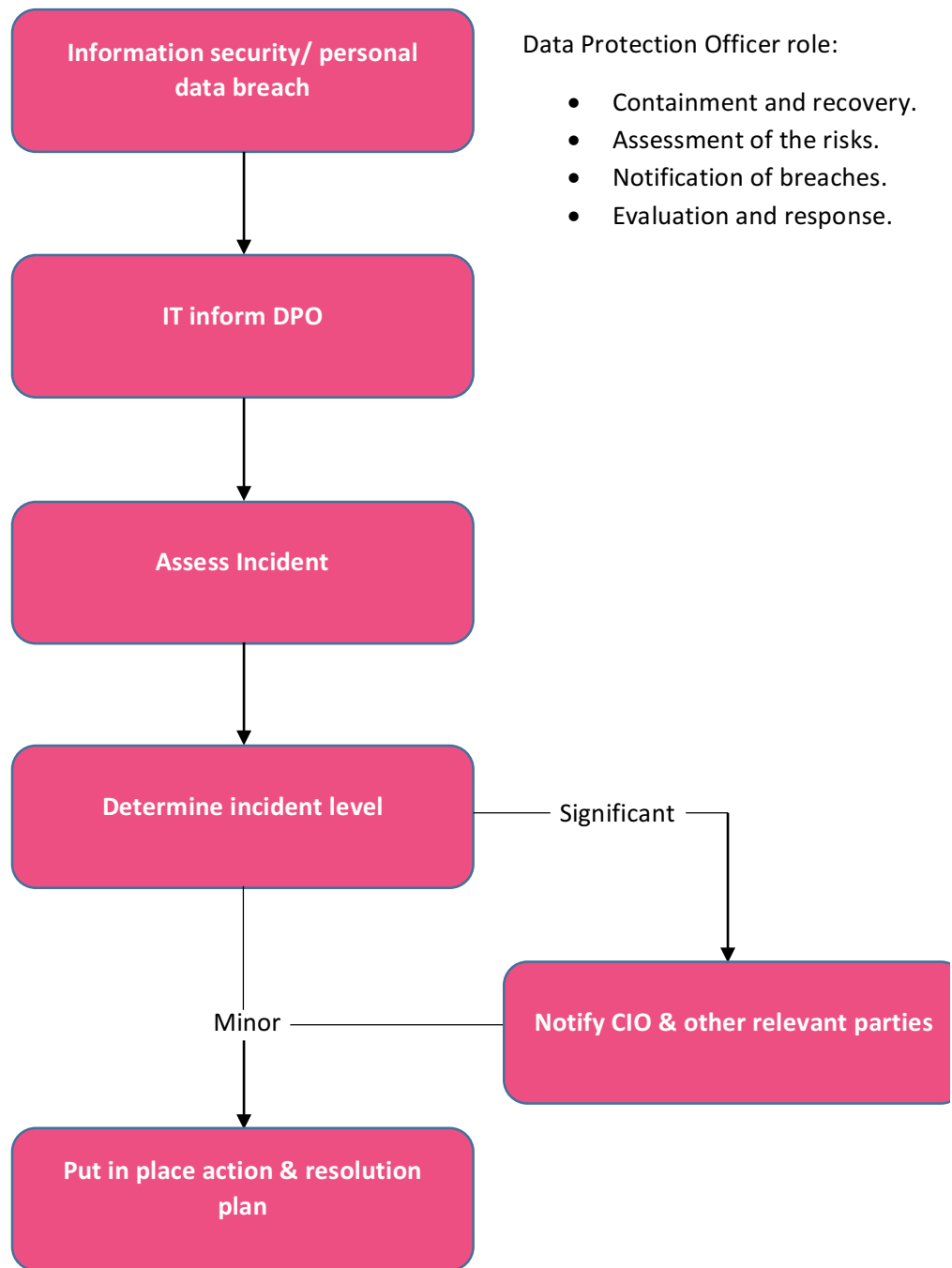
According to GDPR article 4, a 'personal data breach' means a breach of security leading to the accidental or unlawful **destruction, loss, alteration, unauthorised disclosure of, or access to** personal data transmitted, stored or otherwise processed.

**Any serious data breaches must be reported to the ICO within 72 hours.**

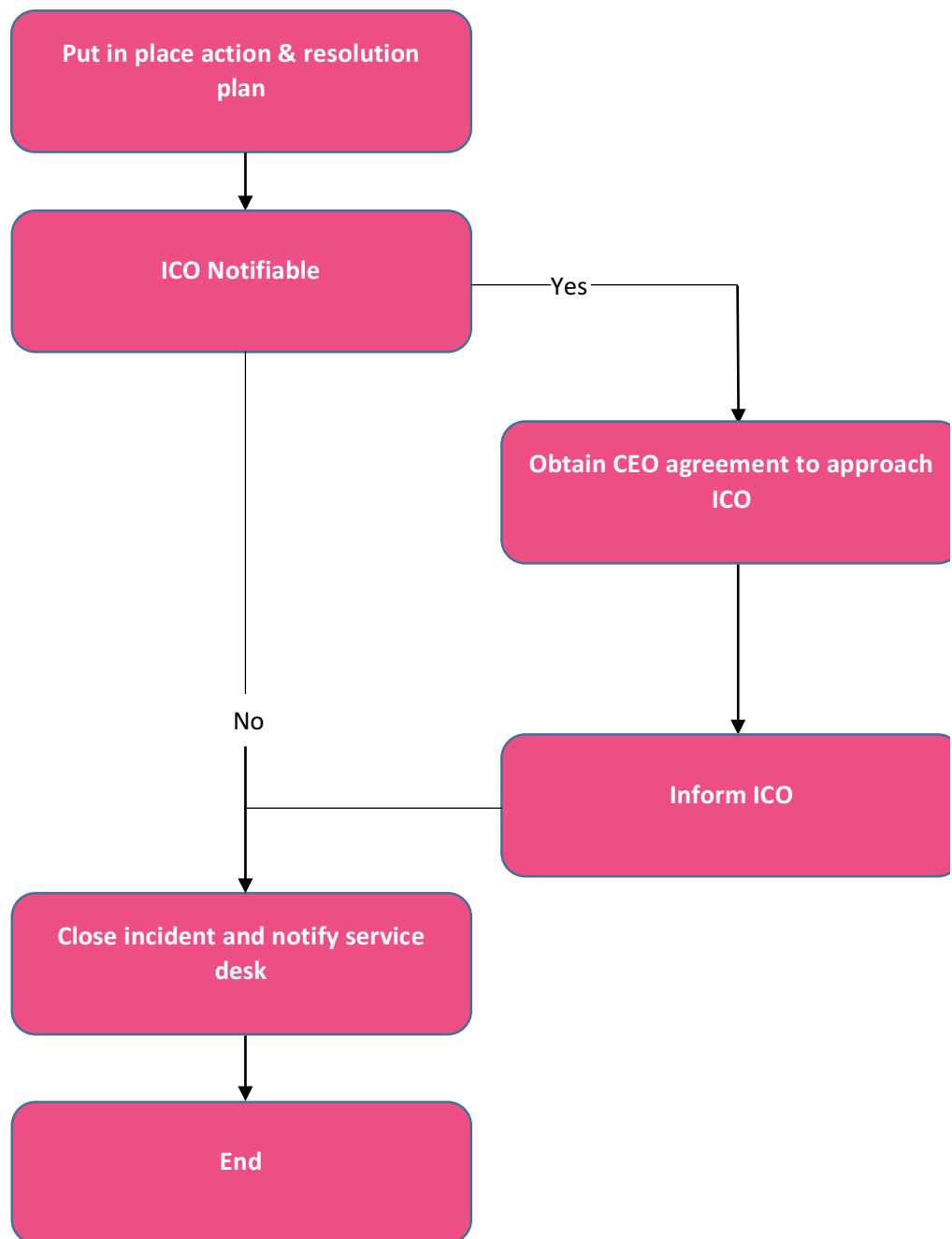
## Critical Incident Stage 1



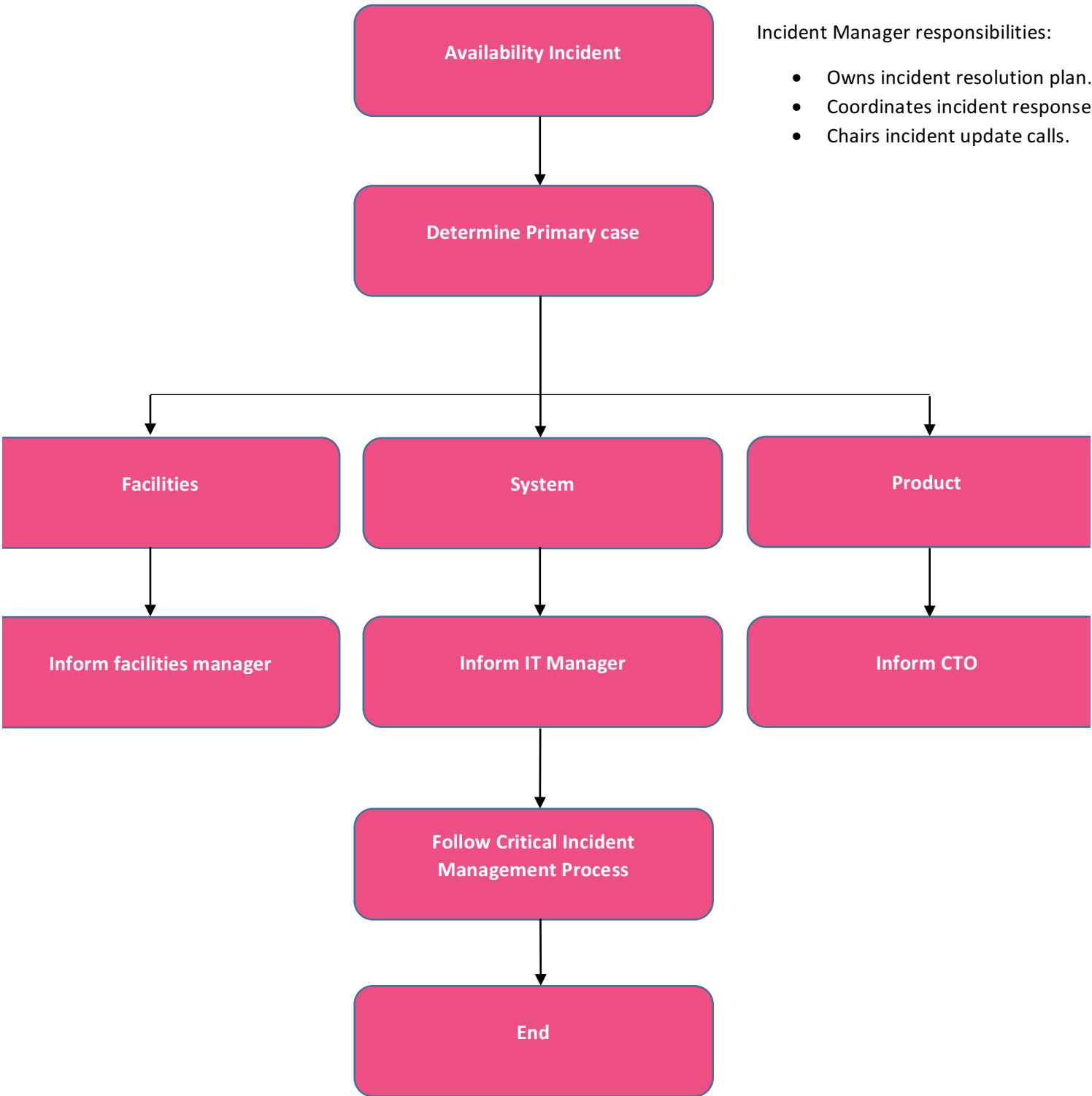
## Information security/ personal data incident Stage 2



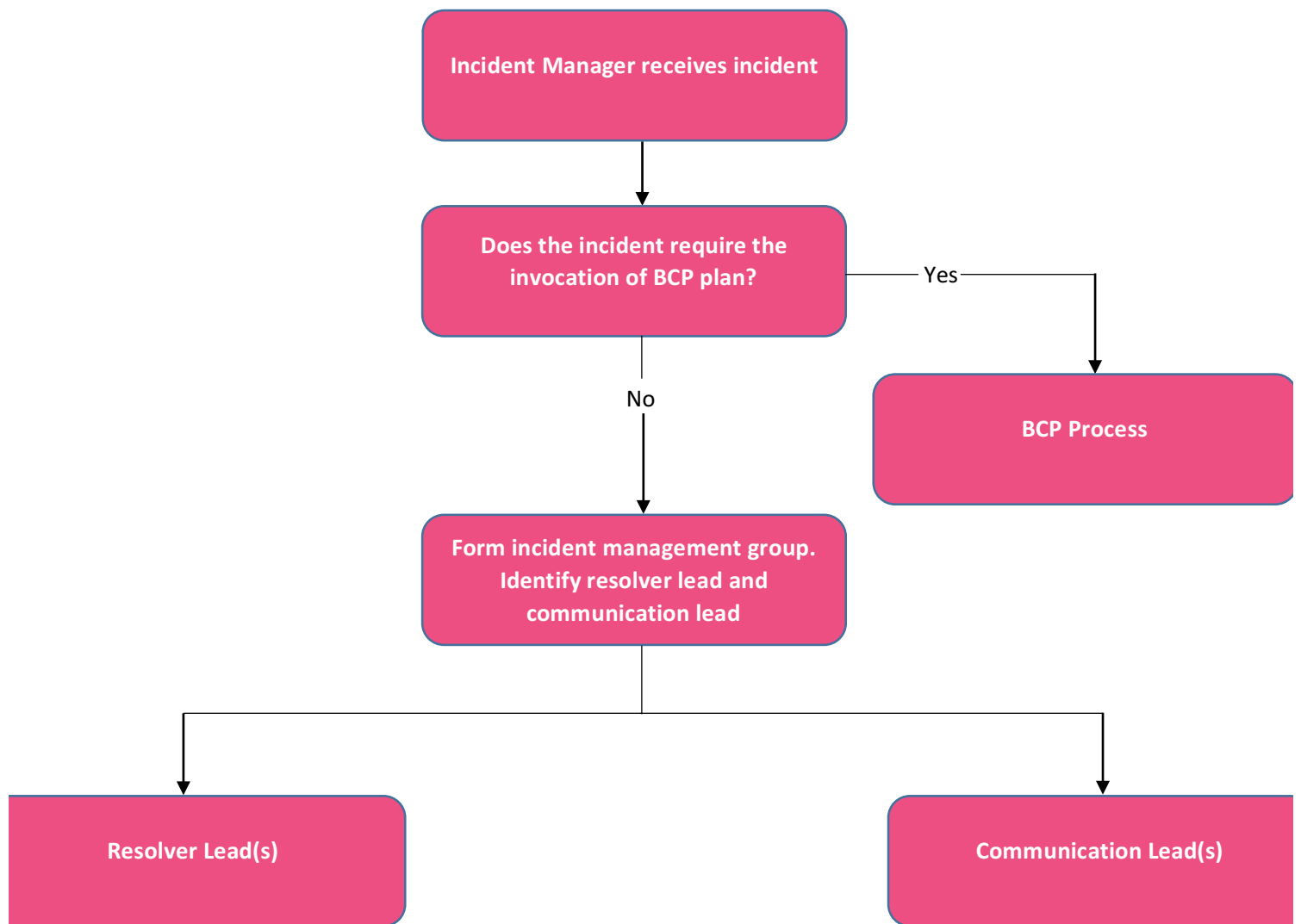
### Information security/ personal data incident Stage 3



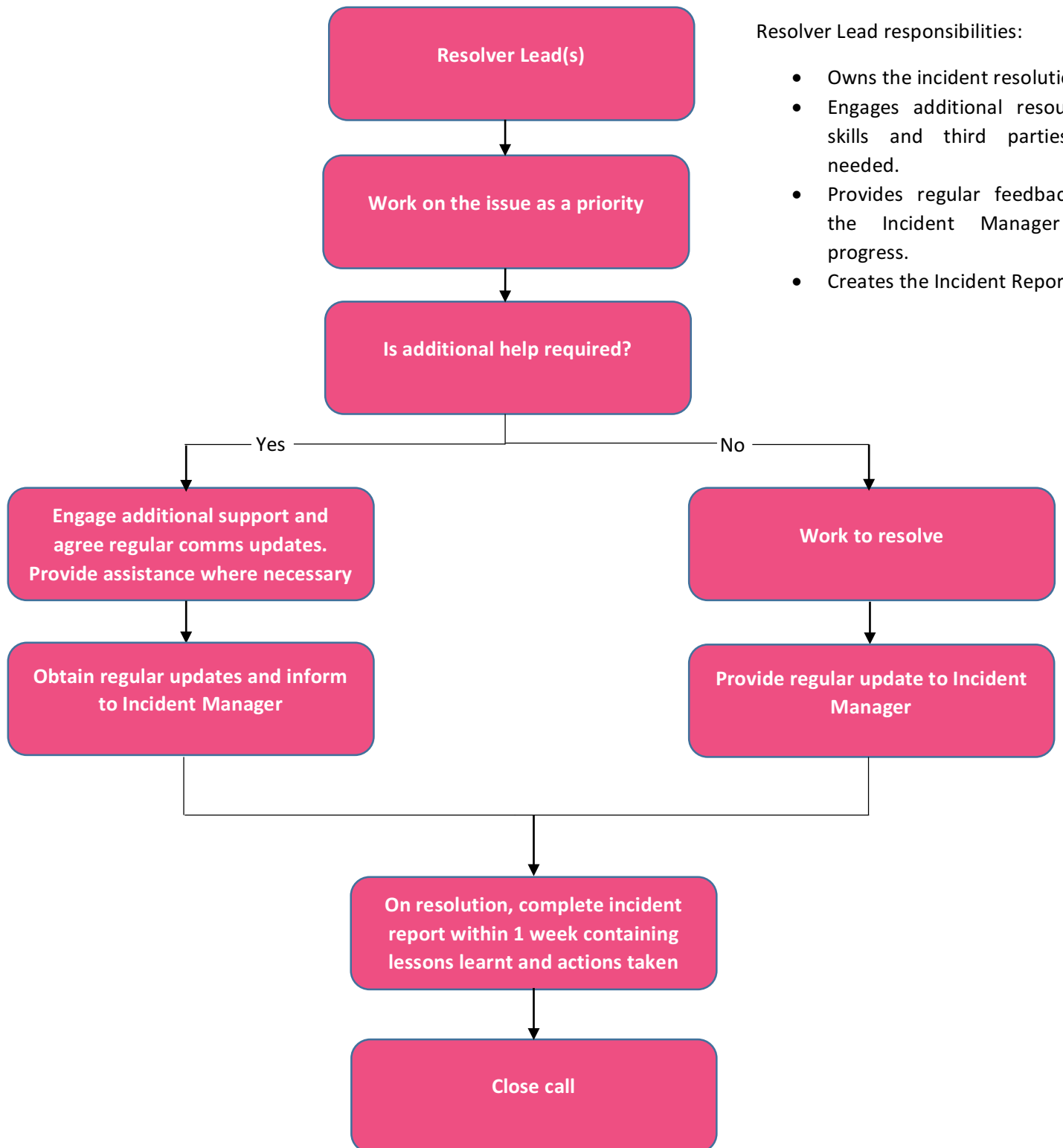
Availability incident Stage 2



## IRIS Critical Incident Management Process



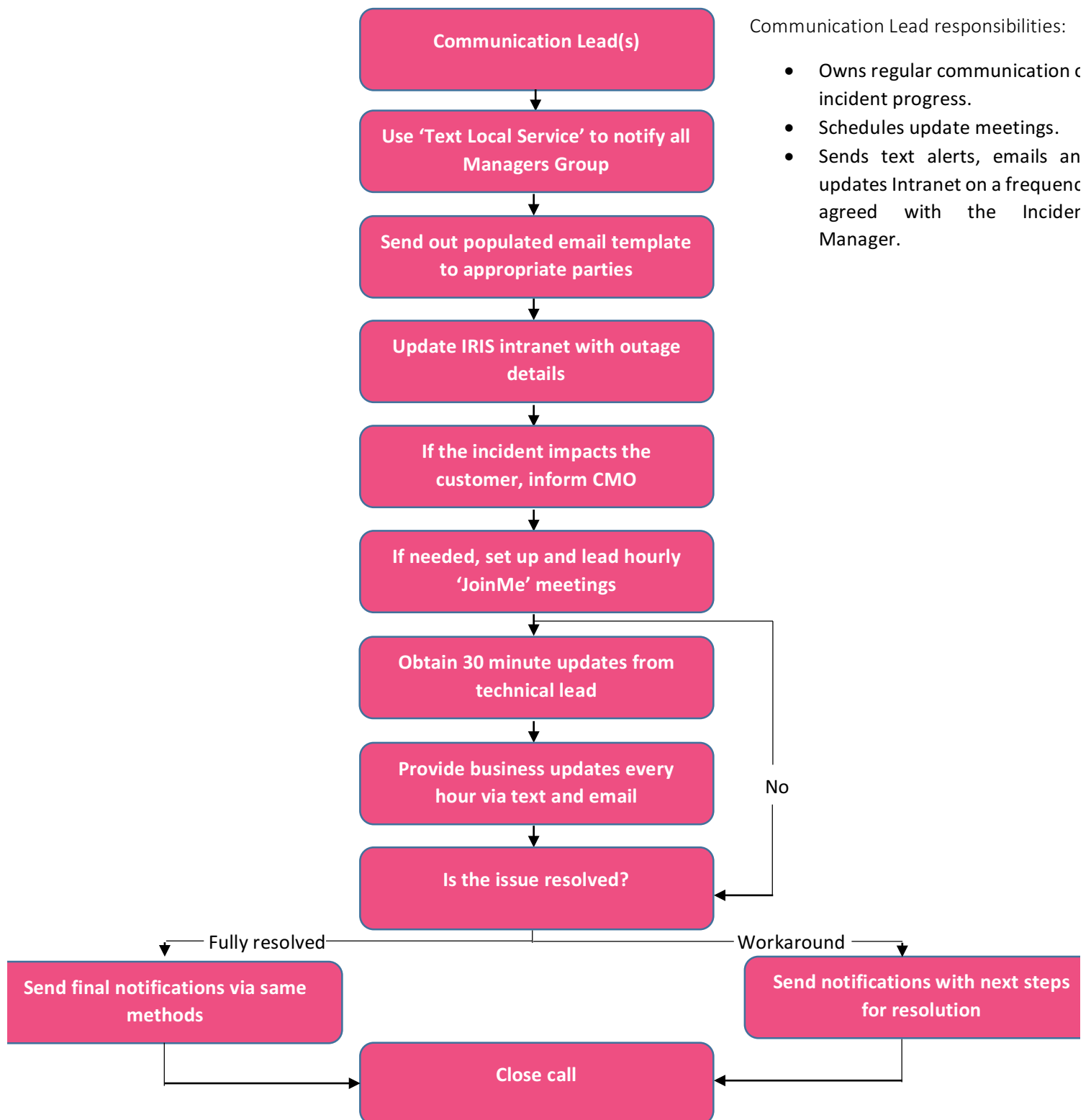
## IRIS Critical Incident Management Process – Resolver Lead



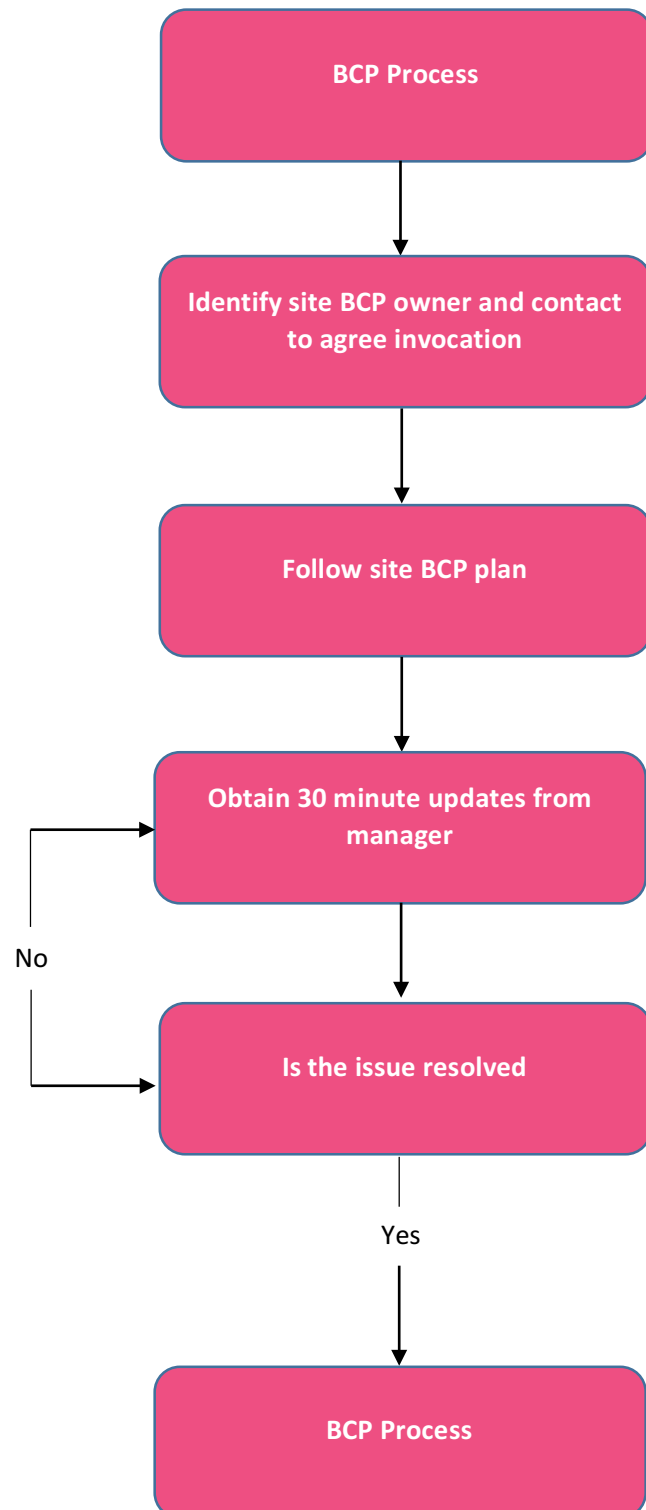
### Resolver Lead responsibilities:

- Owns the incident resolution.
- Engages additional resources, skills and third parties as needed.
- Provides regular feedback to the Incident Manager on progress.
- Creates the Incident Report.

## IRIS critical incident management process – Communication Lead



## IRIS critical incident management process – BCP



## Appendix 6: IRIS Business Continuity Plan statement

The IRIS Group's policy is to maintain the continuity of its activities, systems, facilities and processes and where these are disrupted by any event to enable it to return to 'normal' operations as soon as possible, taking fully into account the impact of any delay on quality of service, reputation and finances.

The objectives of business continuity planning are to ensure that IRIS:

- Understands its critical activities and maintains the capability to resume operations within agreed timeframes, following the deployment of a contingency planning response.
- Increases resilience by protecting critical assets and data (electronic and otherwise) through a co-ordinated approach to management and recovery.
- Minimises impacts using a focused, well-managed response activity.

In compiling business continuity plans IRIS commits to the following:

- Taking all reasonable measures to prevent and avoid any disruption to normal operations.
- Considering continuity planning and resilience implications in all process, project, change and system developments.
- Making advance arrangements for the recovery of infrastructure components (e.g. accommodation, transport, telecommunications, equipment and supplies).
- Making advance arrangements to re-locate or re-organise operations to allow critical processes to continue.
- Providing resilience for information systems and data, or alternative ways of working in the event of their failure. All new systems and processes to be in line with IRIS's Information Security Policy
- Protecting staff, visitor and third party welfare during and following an incident.
- Ensuring the effectiveness of plans and recovery arrangements through robust and regular testing and training.
- Updating plans following significant changes to contingency planning requirements. Such changes may occur as part of organisational change planning and management.

This policy will, unless otherwise stated, apply to all IRIS Group companies and will not be limited to recovery of IT infrastructure alone.

**This policy has been approved by the Chief Executive.**

## Appendix 6: ISP03- HR

### 1. Objective

To ensure all staff are assessed before starting employment are managed during their time at KashFlow, and that appropriate actions are taken on termination.

### 2. Scope and Index

This procedure applies to all staff employed by KashFlow.

The procedure details the controls required by the following control objectives defined in Appendix A of ISO27001: 2013:

SoA Ref	Requirement
A.7.1.1	Screening
A.7.2.2	Information security awareness, education and training
A.7.3.1	Termination or change of employment responsibilities

### 3. Procedure

#### Pre-Employment Screening

Any concerns will be discussed with the Line Manager and if not resolved shall be escalated to a HR team to give guidance. Records are maintained in the personnel files.

- a) Interview process coordinated by the department head.
- b) Verification of critical training, copies of appropriate certificates.
- c) Credit checks, DBR and police record checks dependent on the job role.
- d) Positive verification of two work related references, records of verification kept in personnel files.
- e) Positive verification of identity and living address. Photo-ID (driving licence or passport).
- f) If not a UK national, confirmation of the right to work in the UK.
- g) Accepted and signed contract. Accepted and signed contract.

#### Induction

- a) Completion of the Induction Sheet, carried out by the HR team and IT Team. Induction training covers initial personnel requirements and introduction to the company, health and safety, quality, IT induction and information security awareness. There will be signed acceptance of the awareness training and IT Policies by the new starter.
- b) Issue of Access Rights following the requirements of ISP06.
- c) Issue of building access card.

## Ongoing Control

- a) Employees shall receive regular appraisals from their Line Manager. The appraisal will identify additional training requirements that can be used if required to compile an individual or company training plan.
- b) Regular updates on Information Security controls, awareness and objectives identified shall be e-mailed to all staff, coordinated by the Technical Systems Manager / Technical Operations Manager.
- c) Any serious issues or concerns will be handled following the process defined in the Staff Handbook including disciplinary actions.

## Change in Responsibilities/Roles

- a) The new Line Manager shall assess the requirements of the new role and compare to the employee's previous role and complete raised an IT ticket if a change in access requirements is evident (ISP06).
- b) Actions must be recorded to ensure security is maintained with the changing responsibility and access of the employee.
- c) It may be that new equipment is required or previously issued equipment must be returned.
- d) There may be specific staff vetting requirements for the new role that did not occur when the employee originally started work.
- e) They may be security controls that are required or may no longer be required.
- f) The timing of the actions depends on the role of the employee and risks to the company.

## Termination

- a) The Line Manager / HR team must raise an IT ticket when an employee leaves the company or hands in a letter of resignation. Actions must be recorded to ensure security is maintained. The timing of the actions depends on the role of the employee and risks to the company.
- b) If there are concerns on the access available to the employee once they have handed their notice in, the Line Manager must inform the Technical Systems Manager / Technical Operations Manager to assess the risk and agree and carry out actions to protect information security. It may be some of the actions on termination being carried out early such as return of keys, restriction in access or change of codes.
- c) On termination, all actions taken shall be recorded on the ticket. These include:
  - Return of assets such as laptops/phones etc.
  - Email accounts re-directed to Line Manager.
  - Return of building keys if applicable.
  - If the employee was in possession of codes for any secure locks, arrangements shall be made to change the codes immediately.
  - Removal of access rights on the system.

## Appendix 7: Rackspace

### Introduction

The standard KashFlow HR Private Cloud Platform is located within the tier 3 data centre of our Hosting Service Provider Rackspace in Slough, UK. Being a tier 3 data centre all components (such as network and power) are redundant throughout, with Rackspace offering exceptionally high levels of uptime.

KashFlow have a dedicated account manager within Rackspace and leverage the fanatical support agreement that ensures over 99% of their support calls are answered within 5 minutes. KashFlow raise support tickets as soon as they are notified of any customer incident (which could be platform related) during normal KashFlow Support hours. Outside of support hours Rackspace monitor the systems 24/7 fixing any platform faults and informing KashFlow once complete.

The platform is built upon Windows Clustering and load balancing for web services, SQL clustering for database services and Terminal Services for Legacy Payroll customers. All customers' databases are isolated, and data is stored in individual customer's SQL Server databases. This shared architecture is scaled to be able to run all customer services in the event of a hardware failure. Automatic failover of services to hot components is in place for resilience.

All servers are operating at low levels of CPU and memory utilisation, and are monitored by both Rackspace and KashFlow. Should CPU and memory utilisation become an issue, then capacity is increased.

The platform is secured within Rackspace on their own segregated network and fronted by Cisco firewalls – access into the data halls are tightly controlled and Rackspace pride themselves on being ISO27001 accredited which is the only auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls.

All KashFlow data is shipped to servers located at a separate geographical Rackspace datacentre via a secure 2 factor VPN connection.

### Rackspace fanatical support

Rackspace is different from other providers. In an industry highly focused on technology, they choose to focus on exceptional service as much as on robust IT. It's their goal to provide the best service you have ever experienced. Your complete satisfaction is their sole ambition - anything less is unacceptable.

Fanatical Support is their name for the outstanding service they provide. Their driving purpose is to take care of all businesses utilising Rackspace, to make sure things go as smoothly as possible.

## Rackspace fanatical support promise

Rackspace promise to meet or exceed expectations in the following 5 areas:

<b>Responsiveness</b>	They are available 24/7/365 by phone or ticket to support the infrastructure dedicated to KashFlow and take special care to assist with urgent requests.
<b>Ownership</b>	They take personal responsibility for KashFlow's infrastructure and services. They empower their employees to make decisions and take actions on our behalf. A live escalation contact will be readily available to us at all times. They will follow through on their commitments to us.
<b>Resourcefulness</b>	They employ creative and practical solutions for our private cloud service, including issues related to the network, hardware or operating system.
<b>Expertise</b>	They will always have subject matter experts available who know how to identify problems and offer solutions. Their support teams will provide advice to us about our environment using their industry and technology expertise.
<b>Transparency</b>	They actively listen and provide us with direct and individualised communications. Their answers to our questions will be straightforward and honest, and they will not avoid tough questions. They never use scripts, but instead provide personal responses addressing our specific issues.

## Security

KashFlows's Private Cloud infrastructure is protected by some of the industry's most potent security tools and techniques:

- Their data centres are physically protected 24/7 by on-site security guards, and only Rackspace data-centre staff have physical access to the data halls.
- Security engineers monitor both Rackspace-managed devices and external threats.
- Server operating systems are hardened to Rackspace internal standards on installation. They apply new security patches as new threats emerge.
- Managed antivirus service is powered by Sophos, and fully managed by their experts.
- Fully managed firewalls.

## System performance monitoring

Rackspace provide KashFlow with the following performance monitoring service:

**Rackwatch** – 24/7 port monitoring service which checks the availability of our servers, confirming our hardware is operating correctly.

## Backup and restore

Rackspace's Managed backup services provide encrypted backups to tape utilising a full / differential backup strategy.

Rackspace carefully balance the need to restore data quickly against the need to minimise performance impact on our systems.

## Service level metrics

The following metrics are defined from Rackspace to KashFlow:

**Network Connectivity:** 100% available, excluding maintenance.

**Data Centre:** 100% available including power and cooling, excluding maintenance.

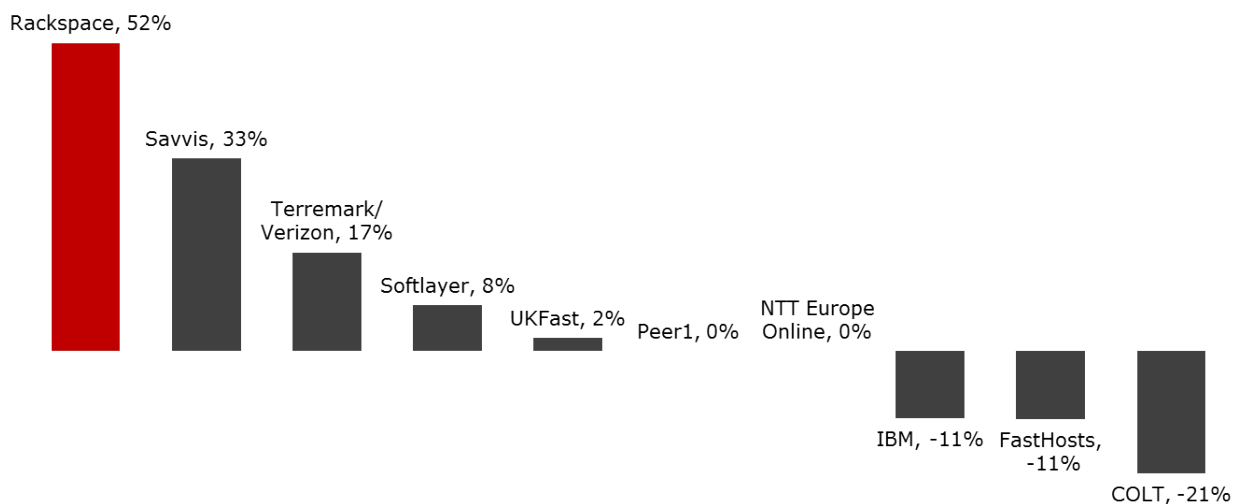
**Hardware Problems:** Fixed within 1 hour of fault diagnosis.

## Customer service metrics

Rackspace survey their customers quarterly, measuring on an ongoing basis the impact of the Rackspace relationship.

In addition, they rate every single fault resolution (or 'ticket') for transactional customer satisfaction. For this purpose, they use the variant question "Based upon the work completed in this ticket, how likely would you be to recommend Rackspace to a friend or colleague?"

On an annual basis, they commission independent research which compares customer satisfaction of a range of hosting providers. The results are shown below:



Source: Vanson Bourne

Vanson Bourne is a specialist research-based IT marketing consultancy. This independent research collated the responses from 376 purchasers on Managed Hosting Services.

## Infrastructure and datacentre specifics

Rackspace's multi-homed Cisco Powered Network is built on hardened routers and audited by Cisco, which assists in obtaining maximum-security protection. The network also incorporates a patented Denial of Service mitigation service to protect against external threats. Together these enable them to deliver on their 100% network guarantee (excluding Rackspace maintenance periods).

KashFlow use Rackspace data centres in the UK, which are:

- Engineered with fully redundant connectivity, power, heating, ventilation and cooling to avoid any single point of failure
- Staffed 24/7 by highly trained technical support staff

Multiple levels of security ensure only data centre Operations Engineers are physically allowed near our routers, switches and servers. This enables them to deliver on their 100% infrastructure availability guarantee.

## Physical security

<b>No public access</b>	Public access to Rackspace data halls is strictly forbidden. This removes the need for anyone other than highly trained Rackspace Engineers to be allowed into the data halls. It also helps them provide a higher level of service than anyone else in the industry.
<b>Video surveillance</b>	Live video surveillance of each data centre facility is monitored 24/7. All entrances to the building and data centre are monitored to ensure only authorised personnel enter sensitive areas.
<b>Onsite security personnel</b>	Rackspace's onsite security team monitors each data centre building 24/7. Their security personnel provide the first layer of security for access to the data centre.
<b>Biometric security</b>	Biometric scanners are used to restrict access to each data centre. The biometric security systems represent the second layer of security for access to the data centre. Within the organisation, only Rackspace engineers are authorised to access restricted areas.
<b>Pass cards</b>	In conjunction with the biometric scanners, access to each facility is restricted to those who hold a Rackspace pass card. The pass cards are also required for moving from room to room within the data centre. Their security pass card system is the third layer of security in the data centre.

## Power systems

Each data centre gets its power from commercial utility underground conduits.

There is a 10-minute battery backup to provide continuous power if a short failure of the mains utility supply occurs. We also have multiple diesel generators with full-load capability, on standby to provide long-term power in an emergency.

**UPS systems:** The power systems are designed to run uninterrupted even in the unlikely event of a total power outage. All your staging and production systems are fed with conditioned UPS power which will run

if utility power fails. Their UPS power subsystem is N+1 redundant with instantaneous failover in case the primary UPS fails.

**Diesel generator systems:** Their on-site diesel generators will automatically start in the event of a power surge or power system failure. The power subsystems are designed to cut over immediately with no interruption in the event of a power failure. Both are regularly tested to ensure they will function properly in the event of a power system failure.

## Cooling

KashFlow's HR main data centre has a closed loop chilled water system. It is cooled by 5 x 1.5MW chillers in an N+1 arrangement (8 at maximum capacity).

Each data hall is configured in a hot and cold aisle arrangement. An 800mm pressurised plenum is fed by computer-room air-handling units in an N+25% arrangement connected by a flow-and-return chilled water loop.

## Smoke detection & fire suppression

Early warning of any fire hazards at the facility is provided by Protec Stratus high sensitivity smoke detection systems. These are backed up by Protec fire alarms.

In the unlikely event that the worst should happen, fire suppression is provided by dry pipe double knock sprinklers. This requires two smoke detectors in a single zone to trigger an alarm. The sprinkler head bulb will then only burst when the temperature exceeds 60 °C in that immediate area.

## Rackspace network

The Rackspace Network has been engineered from the ground up to accommodate the high availability demands of outsourced solutions.








































**Connectivity:** Rackspace provides a fully resilient and redundant network infrastructure onto which we base the KashFlow HR Private Cloud. Their entirely switched network employs Cisco 6500 chassis-based switches running Host Standby Routing Protocol (N+1 hot failover). This ensures data can be routed even in the event of device or link failure. Internet connectivity is provided via multiple links to Tier 1 bandwidth providers. Coupled with our Cisco-powered infrastructure, this enables us to maintain 100% network availability, excluding Rackspace maintenance periods.

**BGP4 routing:** Rackspace runs the Border Gateway Protocol (BGP4) for best case routing. Should one of their providers fail, packets leaving our network are automatically redirected through another route via a different provider.

**Bandwidth utilisation:** The Rackspace UK Network is running at approximately 20% capacity at peak times. This enables them to accommodate even the largest spikes in traffic. As network utilisation reaches 30%, they automatically add more network capacity. This helps to ensure KashFlow do not experience network degradation, even if one of their providers has an outage.

## Rackspace customers

Below are some examples of the many customer's currently utilising Rackspace for hosting services:

eCommerce	      
Publishing and Media	     
Public Sector	      
IT / Telecoms	    
Financial and Legal	       
IT Services / SaaS	     

## Rackspace partners

As the world's leader in hosting and cloud computing, Rackspace has forged close working relationships with key infrastructure vendors. As a result, they have exceptional access to equipment supplies, software updates and patches and vendor level expertise, including:

### Red Hat

Rackspace has always been a staunch supporter of the open source community. They were the first Red Hat Premier Hosting Partner in Europe. Recognised as the experts in deploying and managing Linux configurations, Red Hat is also a Rackspace customer. They have more certified Red Hat engineers at Rackspace than at any other company apart from Red Hat.



### Microsoft



Since 2006, Rackspace has been an accredited Microsoft Gold Certified Partner for its expertise in Microsoft Hosting. This makes it one of the six initial Application Infrastructure Providers in the world.

Microsoft named Rackspace winner of the Advanced Infrastructure Solutions, Hosting Solutions Partner of the Year in 2007, 2005 and 2003.

### VMware

VMware provides virtualisation software for Rackspace's private cloud solutions. This is a proven solution for customers needing flexibility of virtualisation and the security and robustness of a dedicated infrastructure. The KashFlow HR Private Cloud is built upon VMware.

### Dell

Rackspace partners with Dell to offer reliable and highly scalable, managed hosting server and storage platforms.

### Cisco

Cisco provides end-to-end enterprise network solutions from the most comprehensive line of networking products available in the Industry. Rackspace uses Cisco networking products exclusively and has a certified Cisco Powered Network.

## Rackspace awards & certifications

### Policies, Procedures and Controls

ISAE 3402 is an international auditing standard intended to provide customers and prospects with third party validated visibility of a service provider's controls.

Rackspace is subject to an ISAE 3402 Type II (SOC1) audit annually covering all data centre facilities globally. A report on the audit is generated each November to report the results for the past year, and these are

available to current and potential customers subject to signature of appropriate Non-Disclosure Agreements.

### Information Security

All hosting operations performed in Rackspace's UK data centres have been certified compliant to multiple ISO standards.

Their certifications and links to the certificates can be viewed on the Rackspace website by following this link: <https://www.rackspace.com/en-gb/certifications-uk>

### Customer Service

At the National Customer Service awards for 2010, Rackspace won both:

- The award for Front Line Customer Service Team for 2010.
- The most coveted overall award, Customer Service Team of the Year.

This is the second consecutive year they have been recognised by these awards: in 2009 Rackspace also won "Customer Service Team of the Year for B2B" and the highest honour "Customer Service Team of the Year"

Rackspace received the 'Employer of the Year' award in the National Business Awards in November 2011. In parallel Rackspace was awarded the Ruban d'Honneur for Customer Focus in the European Business Awards. In both national and European awards, the Customer Focus awards are presented to the organisation that can best demonstrate that it has the customer at the heart of its business. Such a prestigious award highlights the superior support that Rackspace provides for their customers, arguably the best in the country.



## Employee Engagement and Development



In 2011 and 2012, The Sunday Times Best Companies Awards recognised Rackspace as an outstanding place to work. This is a reflection of the track record Rackspace has established over five years.



Rackspace was the highest placed IT services provider in the Financial Times UK's 50 Best Workplaces ranking for 2012. In 2009 Rackspace was also awarded a Laureate award for being placed in the top 50 for five (now six) consecutive years.

## Environmental Sustainability



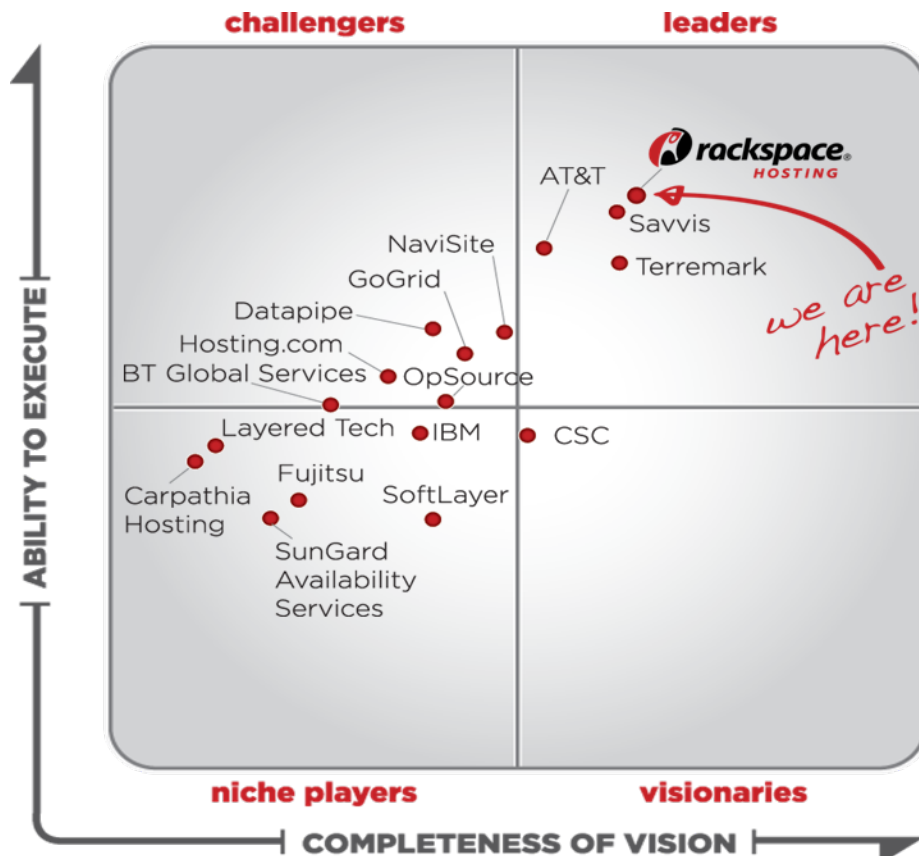
In 2010 Rackspace was named IT Operator of the Year in the prestigious Green IT Awards 2010. Over 75 organisations were nominated for The Green IT Awards and winners were selected by readers of the Green IT magazine and its website. The Green IT Awards are a benchmark by which IT companies are measured for environmental performance. The awards also showcase the role played by green marketing and sustainability communications in informing people about green issues, products and lifestyle choices, and provides examples of excellence and best practice in communicating sustainability and green issues.

## Rackspace vision

To understand the kind of relationship KashFlow can expect with Rackspace, you may want to understand their vision, and the values below.

**Rackspace is recognised by Gartner as a leader for vision and ability to execute.**

Gartner Group is the leading industry analyst focusing on the information technology sector. Their 2012 “Magic Quadrant” for Managed Hosting including Cloud positions Rackspace squarely as a **Leader**.



Source: Magic Quadrant for Managed Hosting including Cloud, Gartner, 2012

Rackspace's Core Values, summarised below, reflect who they are, and help move them towards their vision of service leadership.



- 1. Fanatical Support in all they do:** Rackspace really are fanatical about their people, their services and their customers. They live, eat and breathe customer service.
- 2. Results first, substance over flash:** It's all about delivery, Rackspace invest only in what delivers end results to their customers. If it's not good for you, then it's not good for them.
- 3. Committed to greatness:** They are dedicated to building Rackspace into something great, as well as delivering an outstanding service. They also strive to be an organisation that makes a positive impact on the world, making a real difference to our own lives, and the lives of our customers.
- 4. Passion for their work:** To bring the commitment you expect to Rackspace's service, they have to be passionate about what they do. Rackers are pretty special people – they only hire people who are committed, dedicated, with the courtesy, patience, friendliness and empathy to ensure you have an outstanding experience.
- 5. Full disclosure and transparency:** They always tell it like it is. There are no smoke screens at Rackspace and so they promise complete transparency to customers on any issues that arise, no matter how minor. It's all about trust.
- 6. Treat Rackers like friends and family:** Happy staff leads to happy customers. Being a part of Rackspace really does feel like a surrogate family, helping each other out and showing they care comes naturally.

## Appendix 8: Insurance cover confirmation



**Tracey Haswell**  
Senior Client Advisor – Vice President

Marsh Ltd  
Southampton International Business Park  
George Curl Way,  
Southampton, SO18 2RZ  
+44 (0) 2380 302546  
Fax +44 (0) 118 965 4282  
www.marsh.com

19 October 2017

**To Whom It May Concern**

Dear Sirs

### **CONFIRMATION OF INSURANCE Perennial NewCo Limited**

As requested by the above client, we are writing to confirm that we act as Insurance Brokers to the client and that we have arranged insurance(s) on its behalf as detailed below:

#### **EMPLOYERS' LIABILITY**

POLICY HOLDER:	Perennial NewCo Limited
INSURER:	Hiscox Insurance
POLICY NUMBER:	HU PI6 9268943 (96)
PERIOD OF INSURANCE:	19 October 2017 to 18 October 2018 both dates inclusive
LIMIT OF LIABILITY	GBP 10,000,000
DEDUCTIBLES:	Nil

#### **PUBLIC & PRODUCTS LIABILITY**

POLICY HOLDER:	Perennial NewCo Limited
INSURER:	Hiscox Insurance
POLICY NUMBER:	HU PI6 9268943 (96)
PERIOD OF INSURANCE:	19 October 2017 to 18 October 2018 both dates inclusive
LIMIT OF LIABILITY	GBP 10,000,000
DEDUCTIBLES:	GBP 1,000 in respect of Third Party Property Damage

#### **PROFESSIONAL INDEMNITY**

POLICY HOLDER:	Perennial NewCo Limited
INSURER:	AIG Europe Ltd
POLICY NUMBER:	34032243
PERIOD OF INSURANCE:	19 October 2017 to 18 October 2018 both dates inclusive
LIMIT OF LIABILITY	GBP 7,500,000
DEDUCTIBLES:	GBP 25,000 each and every claim



Registered in England and Wales Number: 1507274. Registered Office:  
1 Tower Place West, Tower Place, London E3 5BU. Marsh Ltd is  
authorised and regulated by the Financial Conduct Authority.



**CYBER LIABILITY**

POLICY HOLDER:	Perennial NewCo Limited
INSURER:	AIG Europe Ltd
POLICY NUMBER:	34032587
PERIOD OF INSURANCE:	19 October 2017 to 18 October 2018 both dates inclusive
LIMIT OF LIABILITY	GBP 5,000,000
DEDUCTIBLES:	GBP 50,000 each and every claim

We have placed the insurances which are the subject of this letter after consultation with the client and based upon the client's instructions only. Terms of coverage, including limits and deductibles, are based upon information furnished to us by the client, which information we have not independently verified.

This letter is issued as a matter of information only and confers no right upon you other than those provided by the policy. This letter does not amend, extend or alter the coverage afforded by the policies described herein. Notwithstanding any requirement, term or condition of any contract or other document with respect to which this letter may be issued or pertain, the insurance afforded by the policy (policies) described herein is subject to all terms, conditions, limitations, exclusions and cancellation provisions and may also be subject to warranties. Limits shown may have been reduced by paid claims.

We express no view and assume no liability with respect to the solvency or future ability to pay of any of the insurance companies which have issued the insurance(s).

We assume no obligation to advise yourselves of any developments regarding the insurance(s) subsequent to the date hereof. This letter is given on the condition that you forever waive any liability against us based upon the placement of the insurance(s) and/or the statements made herein with the exception only of wilful default, recklessness or fraud.

This letter may not be reproduced by you or used for any other purpose without our prior written consent.

This letter shall be governed by and shall be construed in accordance with English law.

Yours faithfully,  
For and on behalf of Marsh Ltd

  
**Mrs Tracey Haswell**  
Senior Client Advisor