CareForIT Limited

ISO 27001:2017

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

POLICY DOCUMENT

Table of Contents

1 Introduction

This document is the Information Security Management System (ISMS) Policy Document of CareForIT Limited. It is the property of CareForIT Limited and is a controlled document.

The purpose of the ISMS Policy Document is to provide an overview of the company, the activities it carries out and the quality standards of operation it conforms to. It is not designed to act as a procedure manual, although it does carry information about where procedures information is located and the detailed information on Documentation Requirements for essential procedures e.g. document control, control of records; internal audit and corrective/preventive action (please see Appendix 3 Procedures Log).

2 Issue Status

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this ISMS Policy Document.

When any part of this ISMS Policy Document is amended, a record is made in the amendment log shown below. The ISMS Policy Document can be fully revised and reissued at the discretion of the Management Team.

The ISMS Policy Document will be reviewed on a six monthly basis as standard. Please note that this ISMS Policy Document is only valid on the day of printing.

Issue	Amendment	Date	Initials	Authorised
1.0	1st Authorised Issue	28/01/14	RT	DFW 28/01/14
2.0	Update following MRT Review	02/05/15	RT	DFW 02/05/15
2.1	Structure Update	15/02/16	RT	DFW
3.0	Annual Review	30/05/16	RT	DFW
4.0	Updates post Internal Audits for Information Security Incident Management Information Security Policy Communication Security Organisation of Information Security	28/02/17	HH	DFW 01/03/17
5.0	6.5 Legal and Regulatory Obligations Update 6.6 Interested Parties Updated	05/05/17	HH	DFW 05/05/17
6.0	Updated 6.5 Legal and Regulatory Obligations to include GDPR	05/06/18	HH	DFW 05/06/18

6.1	Updated post internal audit	12/06/18	HH	DFW 12/06/18
1.0	New versioning to reflect new company CareFor IT	19/11/18	HH	HH 19/11/18
1.1	Add roles and responsibilities links	11/01/19	HH	HH 11/01/19
1.2	Updated Org Chart	05/04/19	HH	HH 05/04/19
1.3	Updates post internal audit results	09/01/20	HH	HH 09/01/20
1.4	Scope expanded and MD signature added	31/03/20	HH	HH 31/03/20

3 Overview of CareForIT Limited

CareForIT is a provider of Software as a Service (SaaS). Our clients subscribe to our service which allows them to access our software via the internet. In return we develop and maintain the software and provide technical support.

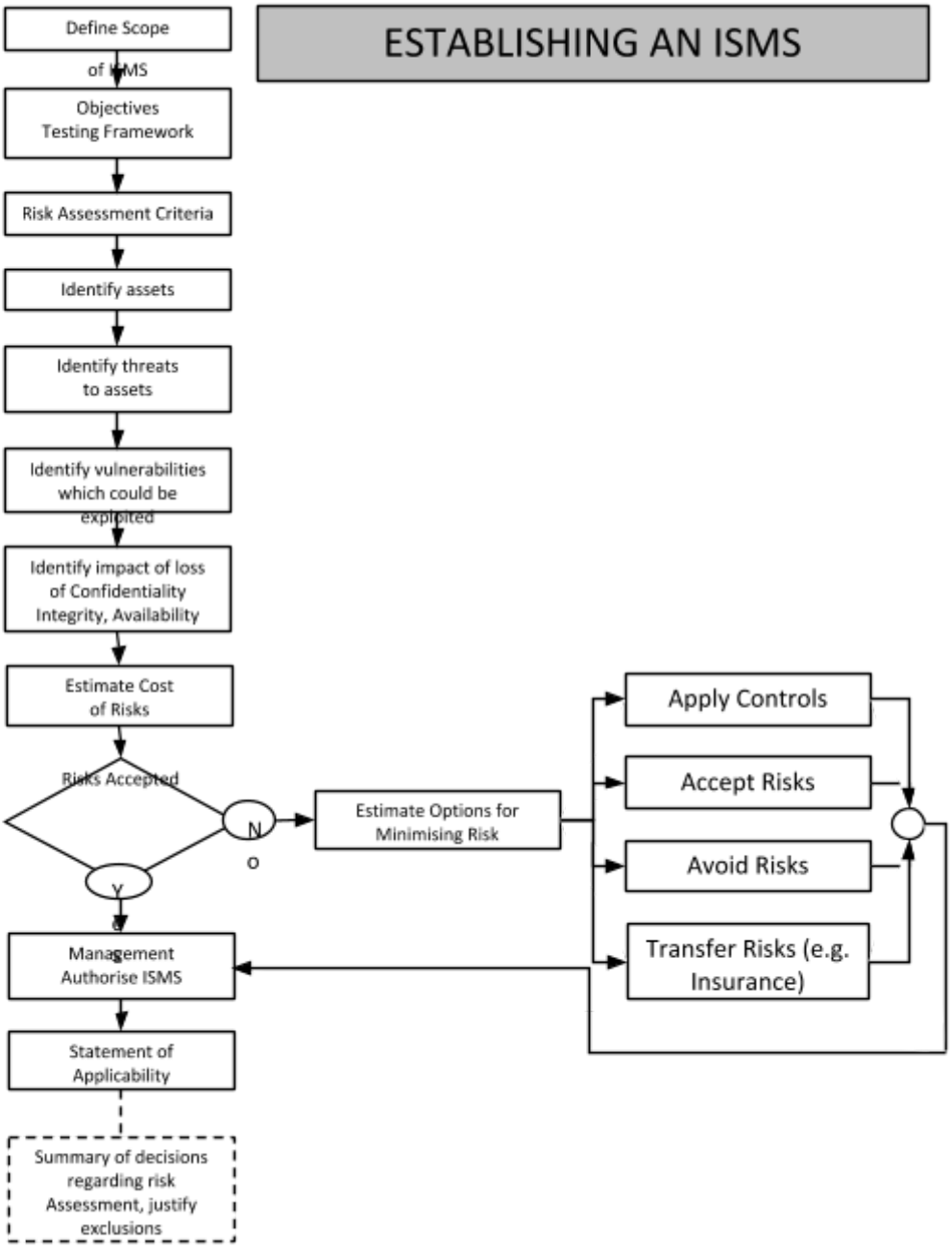
Operating as a SaaS provider means that we hold information and data which can be highly sensitive and business critical to our clients. Although our clients retain ownership of their data it is stored on our network and they entrust it to us; we must therefore make every effort to ensure that their data remains secure, to do otherwise would risk both our clients business and our own.

3.1 Scope of Registration

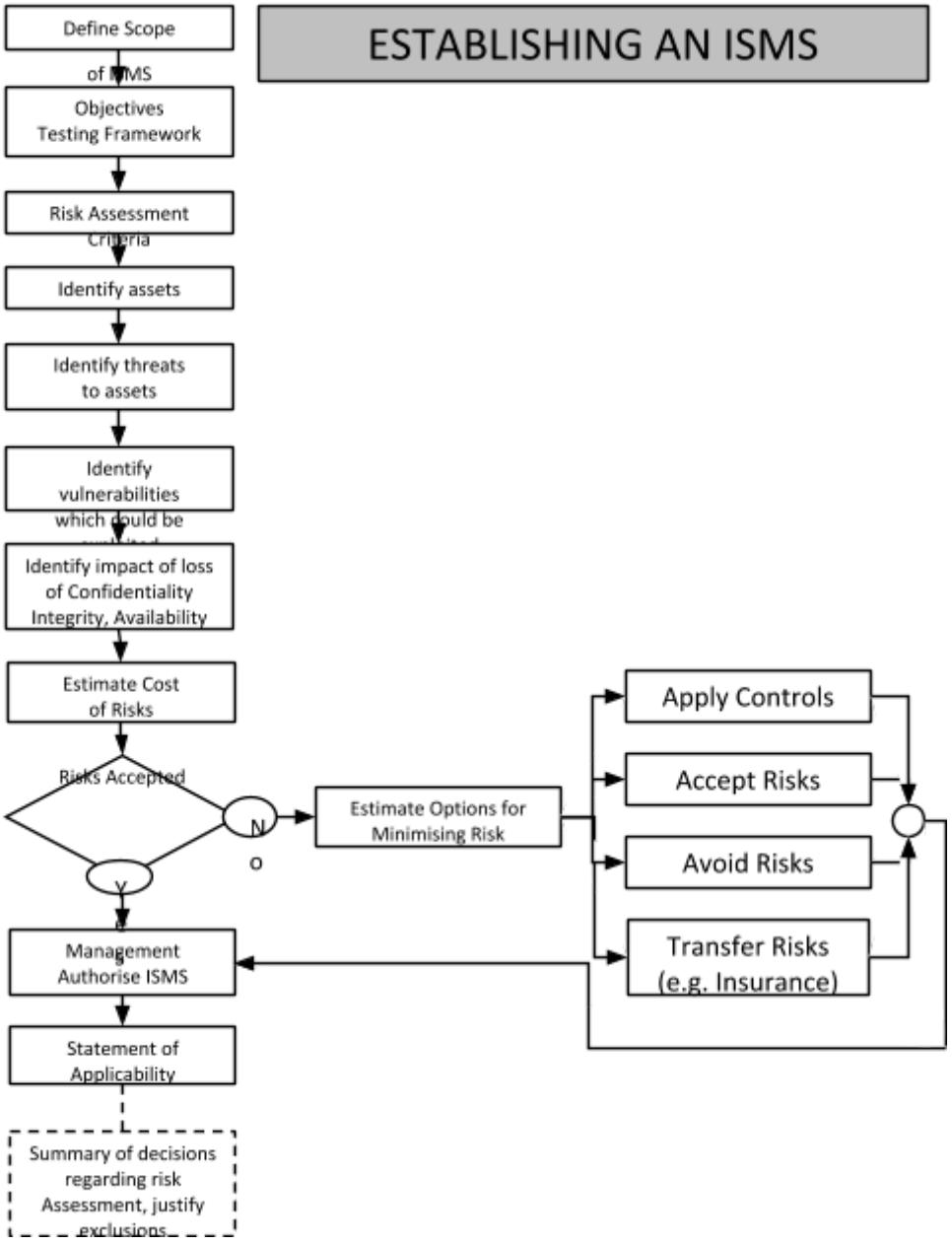
The protection of all information and data assets for the delivery of software design, software development and support. The assets protected are physical locations, hardcopy data, electronic data, policies and procedures, software and licences and physical IT hardware. The boundaries of the Information Security Management System are the physical locations, authorised mobile workers and the endpoints of the organisational network. Supporting technology includes server platforms and network devices within the control of CareFor IT Limited.

4 Information Security Management System

4.1 Establishing an ISMS


ESTABLISHING AN ISMS
Define Scope
of ISMS
Objectives
Testing Framework
Risk Assessment Criteria
Identify assets
Identify threats
to assets
Identify vulnerabilities
which could be
exploited
Identify impact of loss
of Confidentiality
Integrity, Availability
Estimate Cost
of Risks
Risks Accepted
N
o
Y
e
s
Estimate Options for
Minimising Risk
Apply Controls
Accept Risks
Avoid Risks
Transfer Risks (e.g.
Insurance)
Management
Authorise ISMS
Statement of
Applicability
Summary of decisions
regarding risk
Assessment, justify
exclusions

4.2 Implementing and Operating and ISMS



CareForIT Limited has a commitment to quality and a formal information security management system (ISMS) that addresses the following areas:

- Quality
- Performance Monitoring and Review
- Policy and Procedures
- Managing External Relationships
- Financial Management
- Strategic and Business Planning
- Human Resources Development
- Service Innovation

4.3 Documented Information

4.3.1 Control of Documents

All documents (Statement of Intent) are maintained and controlled by the Information Security Officer. Policy and procedure documents are reviewed annually. Any documents requiring amendments are updated, authorised and completed. All updates to documents are signed and dated by the document owner and a member of the Management Review Team. Documents are re-issued as an electronic PDF document and a limited number of hard copies are produced.

Obsolete documents will be archived and restricted by the Information Security Officer, electronic copies of all past versions are kept. All managers hold responsibility for cascading information to staff.

4.3.2 Control of Records

All project records (evidence of past performance) are stored in appropriate electronic folders and managed by respective departments. Hard copies of documents are restricted to a minimum and should not be produced unnecessarily. Electronic records are encouraged over hard copies due to environmental concerns, available storage space and to prevent unnecessary expenditure.

5 Role of Management Review Team

CareForIT Limited's MRT Management Review Team (MRT) are committed to the development and implementation of an Information Security Policy, an Information Security Management System and to frequently review this system. Responsibility has been assigned to ensure that the ISMS conforms to the requirement of the standard and the provision to report on performance to the MRT has been defined.

The Information Security Officer will ensure that CareForIT Limited staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving CareForIT Limited's Information Security Objectives which are aligned with the current business plan.

The MRT is responsible for implementing the ISMS and ensuring the system is understood and complied with at all levels of the business. They are responsible for ensuring that:-

- The Information Security Policy and objectives are established and in line with the strategic direction of the organisation
- Integration of the ISMS into the organisations processes
- That resources needed for the ISMS are available
- Communication covering the importance of effective information security management and conformance to the ISMS requirements in place
- The ISMS achieves its intended outcome(s)
- The contribution of persons involved in the effectiveness of the ISMS by direction and support
- Continual improvement is promoted
- Other management roles within their area of responsibility are supported

An internal audit of procedures and policies is conducted annually. A review of the Information Security Objectives takes place annually. In addition achievement of the quality objectives are measured against quarterly targets set in relation to the business plan. Staff contribution toward the Information Security Objectives is measured in supervision and documented in annual appraisals, carried out as and when necessary considering staff joining dates.

The roles, responsibilities and authorities of the management review team are documented in the Roles and Responsibilities sheet on drive at this link.

6 ISMS Policy

6.1 Introduction

This document is the Information Security Policy for CareForIT Limited. It describes the company's corporate approach to Information Security and details how we address our relationship in relation to this vital area of our business. As a company we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.

This document defines the complete security policy of CareForIT Limited. CareForIT Limited takes the privacy of our employees, freelancers and clients very seriously. To ensure that we are protecting our corporate and client data from physical and electronic security breaches, this policy must be followed and will be enforced to the fullest extent.

Information Security is the responsibility of all members of staff, not just the MRT, and as such all staff should retain an awareness of this policy and its contents and demonstrate a practical application of the key objectives where appropriate to their daily duties.

We also make the details of our policy known to all other interested parties, including external where appropriate and determine the need for communication and by what methods relevant to the information security management system. These include but not limited to contractors, customers and clients and their requirements are documented in contracts, licence agreements, specifications, etc.

Verification of compliance with the policy will be verified by a continuous programme of internal audits.

6.2 Scope of the Policy

The scope of this policy relates to the use of databases and computer system operated by the company at its office in Newton Abbot and at the Rackspace London Datacentre, in pursuit of the company's business providing IT design, development and support services. It also relates, where appropriate to the external risk sources including functions that are outsourced.

6.3 Audience

This policy applies to all employees, management, freelancers, contractors, vendors, business partners and any other parties who have access to company data. This includes physical access to hard copy data and access to the premises where reasonable.

6.4 Integration

We maintain a number of flowcharts that illustrate key business activities and their correspondence to ISMS requirements.

6.5 Legal and Regulatory Obligations

CareForIT Limited complies with all relevant legal and regulatory obligations, including but not limited to:

- General Data Protection Regulation 2018
- Data Protection Act 2018
- Employment Act 2003
- Health and Safety at Work Act 1974
- Equality Act 2010
- UK Electronic Communications Act 2000
- The Telecommunications (lawful Business Practice and Interception of Communications) Regulations 2000
- Computer Misuse Act 1990
- The Electronics Signatures Regulations 2002
- The Telecommunications (Data Protection & Privacy, Direct Marketing) Regulations 1999
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Civil Contingencies Act (2004 & 2005) (UK Government)
- Business Continuity Practice Guide: 2006 (UK Tripartite Authorities: Financial Services Authority (FSA), HM Treasury, Bank of England)
- Copyright, Designs and Patents Act 1988 (CDPA)
- Companies Act 2006 contains several provisions concerning records and communications
- The Human Rights Act 1998 (HRA)
- The Privacy and Electronic Communications Regulations 2003
- Employers' Liability Insurance

6.6 Interested Parties

Further to those legal and regulatory obligations specified in section 6.5 procedure

- WF_RM_0011 Interested Parties

is available as a controlled document that defines who oversees identifying all the interested parties and their legal, regulatory, contractual and other requirements and interests in order to understand their needs and expectations.

6.7 Roles and responsibilities

The roles, responsibilities and authorities of CareForIT Staff are documented in the Roles and Responsibilities sheet on drive at this link. Organisation chart is also available in Appendix 10.1

All employees, freelancers and management are responsible for adhering to the Company Security policy and reporting any activities that do not comply with this policy. This includes physical access to company premises.

Management is responsible for ensuring their direct reports understand the scope and implications of this policy. HR must also ensure that all employees have acknowledged a copy of the Company Security policy.

A copy of the policy is saved on the staff shared drive and can be made available in hard copy for all employees to view when required. Data is monitored by security staff for any unauthorised activities and are responsible for updating access requirements as needed which includes alerting the Company Security Officer to any relevant information.

Any employee who authors or generates company or client data must classify that data according to the criteria outlined above.

Our information Security Officer, who directly reports to the Information Security Manager, is responsible for randomly sampling records to ensure that all required data has been captured and that data is accurate and complete.

6.8 Strategic Approach and Principles

6.8.1 Strategic and Tactical Objectives

The CareForIT key strategic and tactical objectives that the ISMS is intended to help achieve are

- Provide the highest level quality of data security and integrity
- Ensure customers have the highest level of confidence in CareForIT handling sensitive data

- Ensure employees are aware of their responsibilities to achieve the above

6.8.2 Information Classification and Data Types

CareForIT Limited deals with two main kinds of data:-

- Company owned data that relates to such areas as corporate financials, employment records, payroll, etc.
- Private data that is the property of our clients and /or employees, such as contact information, national insurance numbers, etc.

CareForIT Limited is comprised of three classifications of information:-

- Public/Unclassified – This is defined as information that is generally available to anyone within or outside the company. Access to this data is unrestricted, may already be available or can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, corporate financials, etc.
  Employees may send or communicate a public/unclassified piece of data with anyone inside or outside the company, provided it complies with all Company Policies.

- Private – This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and/or people and cannot be distributed outside the workplace. Private data includes, but is not limited to, work phone directories, client contact details, company policies, etc.
  All information not otherwise classified will be assumed to be Private and the Company Security Policy will be adhered to.

  Employees may not disclose private data to anyone who is not a current employee and/or freelancer of the company. This is dependent upon roles and responsibilities of the employee and set out in the Company Security policy.

- Confidential – This is defined as personal or company information that may be considered potentially damaging if released and is only accessible to specific groups and/or employees as well as sensitive data which, if leaked would be harmful to the company. Confidential data includes, but is not limited to, service user information, audit reports, legal documentation national insurance numbers, payroll data, contact information, tax forms security procedures, etc. CareForIT Limited considers it a top priority to protect the privacy of all clients, employees and business partners.
  Employees may only share confidential data within the department of named distribution list in accordance with the Company Security policy.

It is the responsibility of everyone who works for and/or with CareForIT Limited to protect all data whether it is electronic or otherwise recorded. Even unintentional abuse of classified data will be considered a breach of contract and will be dealt with in accordance with the Company disciplinary procedures.

Selected employees, where applicable, are checked by the Disclosure & Barring Service before they

are permitted to access any secure data/information of any description relating to specific projects. If the employee fails the security check they will not be able to have access to any secure data/information and this will immediately invoke standard employment procedures. This is described fully in the Company contract of employment.

6.8.3 Access Control

The Information Security Manager works in conjunction with the Information Security Officer to maintain data access privileges, which will be updated as required when employees/freelancers join or leave the company.

The Information Security Officer assesses all employees/freelancers needs relating to access to information and applies the relevant security level to that member of staff.

The Information Security Officer reviews all access, both physically and electronically, and makes any changes and/or amendments where required. Purchase of new equipment/stationery is undertaken by the relevant authorised personnel and is subject to review by the Information Security Officer at any time.

In general, passwords will be changed every three months and the last 10 passwords may not be reused. Passwords have to be no less than 8 characters in length and consist of both numbers and letters. Passwords must not be written down on paper, but are for certain areas kept secure in an electronic password protected file that is not held on a shared server.

6.8.4 Non-Disclosure Agreements (NDA)

CareForIT Limited is dedicated to protecting the business, including client and employee information. By means of this process it requires all employees, freelancers, outside organisations and others to sign a non-disclosure agreement.

The agreement consists of two documents, both are exactly the same as each other and are signed by both parties. Each party then retains a signed copy for their records and reference. This agreement remains current for a period of three (3) years. Failure to comply with the term and conditions of this document will result in legal action being taken in order protect the company, its employees, freelancers and clients.

CareForIT Limited continually reviews this process in order to minimise potential risk.

6.8.5 Incident Management

To assist with assessment of and decision on information security events all incidents must be reported immediately to the Information Security Officer. The information security officer will assess the incident and it shall be decided if they are to be classified as information security incidents. Initial incident reportee is responsible for reporting the incident via the form available on web internal.

6.8.6 Physical Security

All staff and freelancers are requested to challenge strangers not known to the member of staff. Any unauthorised persons are reported immediately to a manager available at the time of the incident.

Access to the office is via a keypad entry at both the overall building as well as the actual office level. The code at the office is changed six monthly or earlier if required (e.g. following a member of staff leaving).

All data held on remote servers by external parties/suppliers has ISO27001:2005 or similar in place.

6.8.7 Third Party Access

Access to the office and all data is restricted to CareForIT Limited staff. Visitors are required to sign the Visitor Book.

6.9 Business Continuity/Disaster Recovery

CareForIT Limited is dedicated to protecting its business including employee, freelancer and client information. All backed up data is treated as sensitive and restricted and is not passed to any outside organisation as part of a backup process, unless a client requests a copy of their backup data. This reduces and potential risk of data theft.

The Information Security Officer and any other relevant authorised personnel are aware of data loss and have in place a system that in the event of a disaster, will minimise the risk of data loss. The following procedures and practices are now standard:-

6.9.1 Paper based details

- All documents are kept in large secure filing cabinets.
- All areas within the premises are kept as clear as possible to reduce the risk of fire and loss.
- No naked flames are allowed on the premises at any time.
- CareForIT Limited comply with the Health and Safety regulations.
- All paperwork that must be kept, is scanned and held electronically as regulated by the Company Information Security policy.

6.9.2 Electronic data

CareForIT leases hardware as required from Rackspace on an hourly basis for the processing and storage of data. Backups of client databases are taken at regular intervals throughout the day.

File backups of client files are taken daily. All leased hardware is located in Rackspace's London data centre and no data leaves the UK.

Our telephone systems is managed by Voipfone and is capable of being switched to an alternative IP Telephony system.

6.10 Approach to Risk Management

We have carried out a full risk assessment of the potential for a breach of security as documented within our separate Risk Assessment Document.

We aim to produce all opportunities for data to be compromised. This includes the possibility of theft of data.

6.10.1 Action in the event of a policy breach

Access to systems and the premises is controlled by the Information Security Officer. Immediately after a policy breach has been detected, any relevant user is either removed or reset depending upon the most appropriate action in the circumstances.

A formal disciplinary procedure will be evoked where necessary.

6.11 Information Security Objectives

Our objectives are set out in CareForIT's annual Goals and Objectives document and are then disseminated to each department/project for incorporation. Each department is responsible for delivering its objectives and this is monitored via individual meetings, appraisals and team meetings.

CareForIT Limited's Quality Objective are:-

- Existing Services – CareForIT Limited will continue to deliver its services within a secure environment
- Development – CareForIT Limited will conduct annual risk assessments to ensure that risk to information in the care of CareForIT Limited is minimised or eliminated.

6.12 Responsibility, Authority and Communication

The management structure of CareForIT Limited is shown as an organisation chart (see Appendix 1), the chart shows functional relationships and responsibilities.

6.12.1 Management Representative

The Information Security Officer is responsible for the maintenance, measurement and review of our Information Security Management System. The Information Security Officer will ensure that the processes needed for the Information Security Management System are established, implemented and maintained within CareForIT Limited. In addition he/she will report to the MRT about system performance.

6.12.2 Internal Communications

Senior Management utilise CareForIT Limited's internal communication framework in order to disseminate information about the effectiveness of the Information Security Management System.

6.12.3 Implementation

Following the annual audit, results will be collated and circulated through CareForIT Limited's internal communications framework.

6.13 Management Review

Senior Management ensures:-

- That the ongoing activities of CareForIT Limited are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process
- Measurement of CareForIT Limited's performance against our declared Information Security Objectives
- That internal audits are conducted regularly to review progress and assist in the improvement of processes and procedures. The reviews will be discussed as part of CareForIT Limited's Management Review Team meetings
- That employees have the necessary training, support, specifications and equipment to effectively carry out their work
- The management team hold planning and review meetings every month. Minutes of these are taken and the agenda normally includes an update and discussion around the current work of all departments and services.

6.14 Review Input

The monthly MRT meetings review the following information:-

- Risk management and the status of risk assessments and treatment plan
- Monitoring and measuring of results including internal audits
- Fulfilment of information security objectives
- Serious untoward incidents
- Status of preventive, non-conformances and corrective actions
- Follow up on actions from previous management reviews
- Changes in external and internal issues that are relevant to ISMS
- Recommendations/opportunities for continual improvements
- Feedback from interested parties

6.14.1 Implementation

The MRT ensures that:-

- Meetings are scheduled
- A suggested agenda is prepared by a member of the MRT
- Members are invited to add items to the agenda
- An agenda is circulated to members
- Meetings take place
- Actions are defined
- Action notes and brief notes are minuted by a designated member of staff
- Action notes are approved by the Managing Director
- Action notes are circulated amongst members
- Completion of actions is reviewed regularly

6.15 Review Output

The MRT reviews produce the following outputs:-

- Policies and procedures are updated to make operations more efficient
- Operations and services are improved through measurement against targets and actions to improve or rectify specific areas.
- Where resources are lacking, actions are put in place, where possible, to rectify this

6.15.1 Implementation

The MRT ensures that:-

- Corrective actions are identified
- Targets are created
- Improvements are actioned
- Situation is re-evaluated at a specified date

7 Provision of Resources

CareForIT Limited will provide all the resources needed to implement and maintain the Information Security Management System and improve effectiveness of the system. CareForIT Limited will also ensure that the resources needed to enhance the satisfaction and requirements of clients, partners and staff are identified and in place through the annual audit and continual review.

7.1 Human Resources - Competence, Awareness and Training

We maintain a detailed Training Matrix demonstrating who has received what training and when. In addition staff are responsible to keep their Continuous Professional Development (CPD) logs up to date.

7.2 Infrastructure

CareForIT Limited's offices, workspace and associated utilities are managed by the Managing Director. The procurement and management of hardware, software and supporting services such as communication and information systems are also coordinated by the Managing Director.

We maintain a detailed asset register, including serial numbers, description, location and/or person to whom it is assigned.

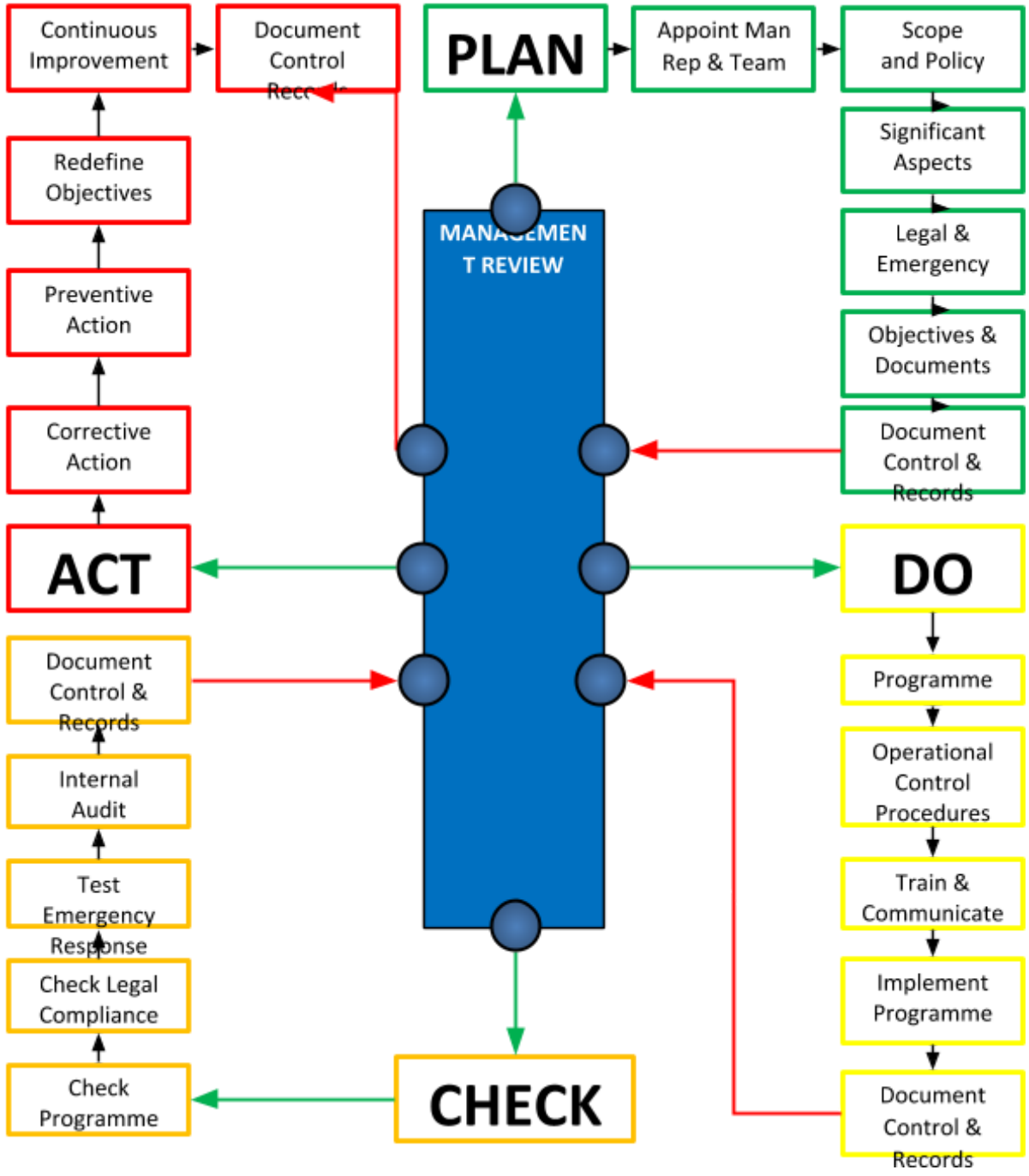
7.2.1 Implementation

Offices, workspace and associated utilities are regularly reviewed to ensure we make efficient use of space. Both hardware and software is reviewed on an ongoing basis to ensure that staff are equipped with fit for purpose IT equipment and software.

IT systems are maintained and serviced by the Managing Director, who in in conjunction with project

staff also prepares and distributes a wide range of information, including:-

- Management Accounts
- Management & Performance Information
- Training Updates


Continuous Improvement
Document Control Recc
PLAN
Appoint Man Rep & Team
Scope and Policy
Significant Aspects
Legal & Emergency
Objectives & Documents
Document Control & Records
Redefine Objectives
Preventive Action
Corrective Action
ACT
MANAGEMEN T REVIEW
DO
Programme
Operational Control Procedures
Train & Communicate
Implement Programme
Document Control & Records
Document Control & Records
Internal Audit
Test Emergency Response
Check Legal Compliance
Check Programme
CHECK

8 Risk Assessment Methodology

CareForIT Limited has identified the following process as a means of conducting regular risk assessments relating to Information Security Issues.

Within each of the areas the risk (if any) are identified together with a rating as to the importance of the risk. The associated consequences or severity of the risk is also rated together with the probable likelihood of the risk occurring.

We use a spreadsheet to collect and analyse the risks identified in the following areas/assets:-

- Building, office, etc. security
- Hardware – desktops, laptops, removable media, etc.
- Software applications
- Infrastructure/servers
- Client information and data
- Paper records
- People and reputation
- Key contacts
- Critical third party suppliers
- Utilities

All typical/likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes) using a ratings scale of:-

(1) Very Low	(2) Low	um	(5) Very High
	(3) Medi	(4) High	

and are expressed across key areas of Vulnerability, Probability and Impact.

Following this analysis, evaluations are drawn as to what the most appropriate action is, together with the estimated cost of the implementing actions to address the identified issue and an estimate of the cost of ignoring the risk. Key evaluation criteria us is:-

(1) Accept Risk
(2) Apply Controls
(3) Avoid Risk
(4) Transfer Risk

8.1 Risk Treatment Plan – Statement of Applicability

The approach to our risk treatment plan has been designed and implemented using the main headings within the standards as a guide to establish that all controls required have been considered and that there are no omissions.

The document identifies to mitigate risks following the process of identification, analysis and evaluations as described in the Risk Assessment Methodology and is directly linked to the aspects of the organisation.

9 Measurement, Analysis and Improvement

9.1 Information Security Standards

In all CareForIT Limited's services there are a specific set of quality measurements developed to be used to audit each service to enable clients to be assured of the quality of delivery.

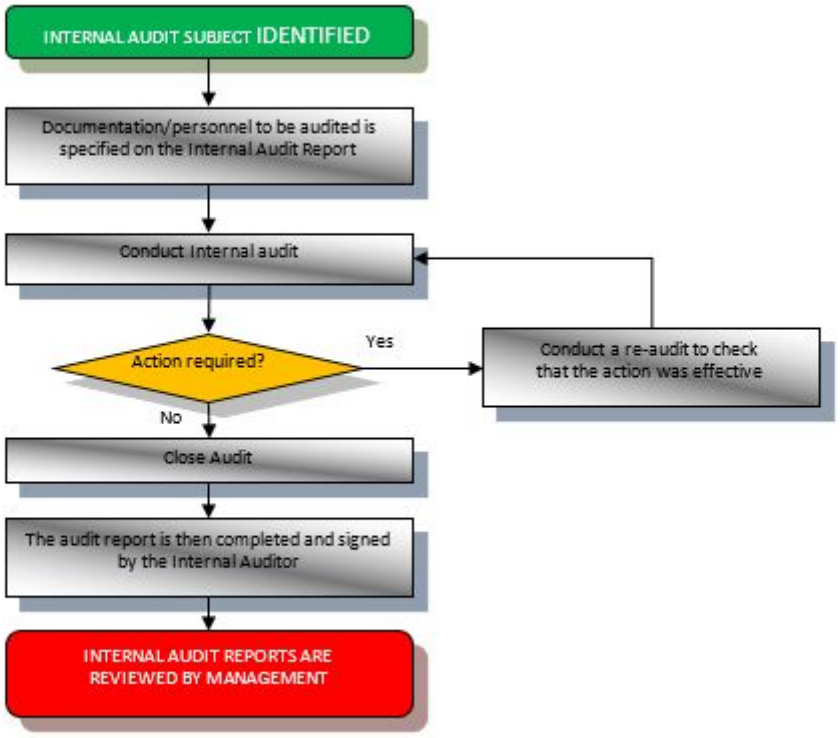
Service Level/Licence Agreements are used to identify the areas of a contract that will be measured and monitored.

Implementation

We review our performance as part of a continuous review of Management Information. These reports help us to assess whether we are meeting our performance targets and provide us with month on month business performance benchmarking information. CareForIT Limited conducts annual audits and provides quarterly reports at MRT meetings.

9.2 Internal ISMS Audits

The internal audit process is set out in the below process flowchart



9.3 Monitoring and Measurement of Processes

9.3.1 Implementation

Where the agreed requirements are not met, an action plan clearly detailing compliance will then be agreed with CareForIT Limited's Managing Director with a timescale for compliance set at 6 months

with the client.

9.4 Monitoring and Measurement of Service

Our approach determines what needs to be measured inclusive of security processes and controls, the methods by which we ensure valid results, the periods and persons involved conducting this activity and the reporting frequency and the responsibility for analysing and evaluating the results. We retain all documents and records involved in the process.

CareForIT Limited establishes at the outset of a new service contract the reporting demands within the licence agreement. This process will be supported with the data reports compiled and will enable the review to monitor performance, effectiveness of delivery, contract compliance and potential service developments. CareForIT Limited provides full information for this purpose on a quarterly and annual basis.

9.5 Analysis of Data

Incident logs are used to record any Information Security incidents or breaches giving cause for concern. These logs are regularly assessed during the Management Review process to identify areas for improvement.

9.5.1 Implementation

The data is collected by client and/or service and is being monitored by Senior Management.

9.6 Continual Improvement

CareForIT Limited will continually improve the effectiveness of the Information Security Management System through the use of the quality policy, quality objectives, audit results, analysis of data, corrective and preventive actions and management review.

9.6.1 Implementation

We review our performance as part of a continuous review of Management Information, client feedback and comments. In particular we review our progress against our business information security objectives (business plan aims), with a view to seeing what we can improve and where. The chart below illustrates this process.


How well are we doing?
How much better could we be?
What must we change to achive this?
Plan for improvement
Implement the improvement
Review
Company Objectives

9.7 Corrective Action and Improvement

Both these areas are reviewed within the agenda for the Management Review meetings and typically cover the action taken to control and correct any non-conformances, noting any consequences of the action taken and themes which may be evident.

In terms of continual improvement, we also review the suitability, adequacy and effectiveness of our ISMS.

9.8 Complaints Policy

CareForIT Limited is committed to giving its clients and customers the best possible service, involving them in the planning of their support and giving them the opportunities to air any complaints that they may have on the service we provide. To this end we operate a full Complaints Policy which can be accessed on the company shared drive.

9.9 Preventative Action

CareForIT Limited has various processes and procedures in place to ensure that preventative action against non-conformances can be introduced, documented and seen through until completion to address the initial problem. The complex nature of some clients we work with, demands that we have flexible but effective processes and procedures in place.

However, CareForIT Limited also uses internal and external audits and risk assessments to continuously improve its service delivery, financial, HR and operational functions.

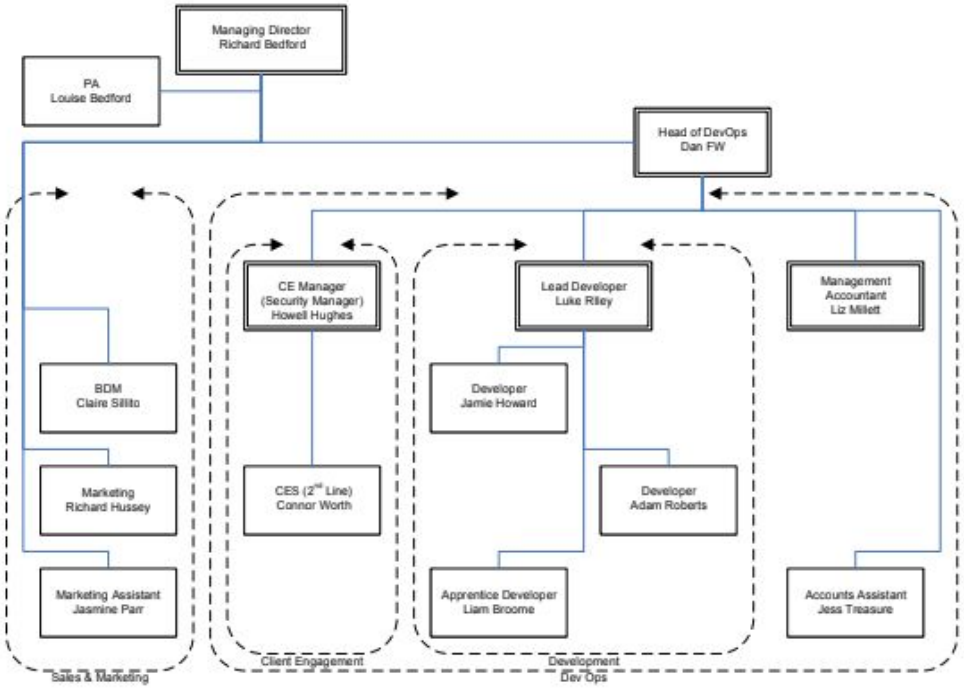
10 Appendices

10.1 Appendix 1 – Organisational Chart

CareForIT Limited reviews and updates its organisational chart on a regular basis and the most recent version is available on Google Drive as follows:-

Google Drive - Employer - Organisational Chart

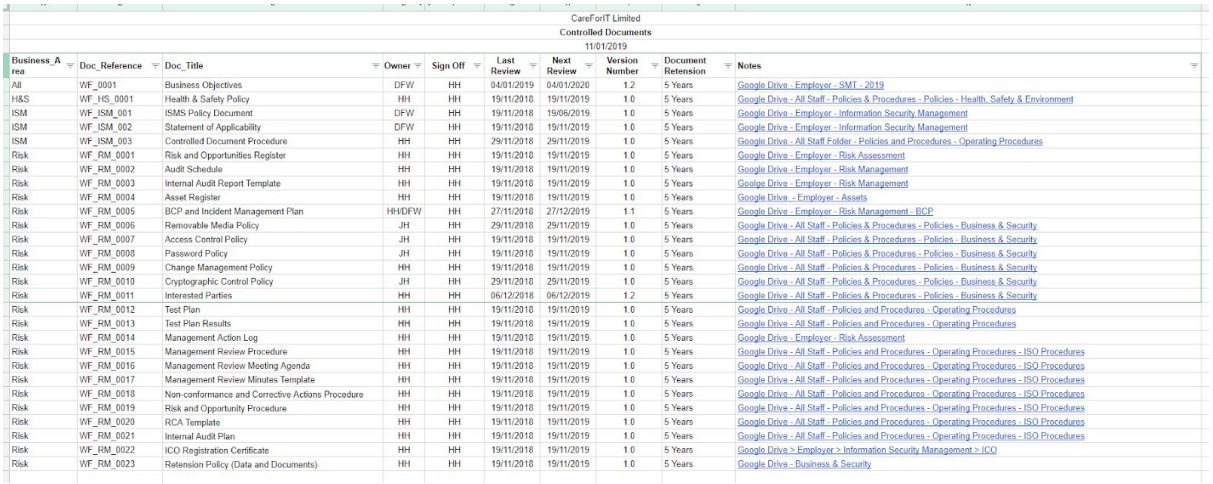
The roles, responsibilities and authorities of CareForIT Staff are documented in the Roles and Responsibilities sheet on drive at this link.



10.2 Appendix 2 – List of Controlled Documents

CareForIT Limited reviews and updates its list of controlled documents on a regular basis and the most recent version is available on Google Drive as follows:-

Google Drive – Employer – Information & Security Management – Controlled Documents



CareForIT Limited
Controlled Documents
11/01/2019

Business_Area	Doc_Reference	Doc_Title	Owner	Sign Off	Last Review	Next Review	Version Number	Document Retension	Notes
All	WF_0001	Business Objectives	DFW	HH	04/01/2019	04/01/2020	1.2	5 Years	Google Drive - Employer - SMT - 2019
H&S	WF_HS_0001	Health & Safety Policy	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies & Procedures - Policies - Health, Safety & Environment
ISM	WF_ISM_001	ISMS Policy Document	DFW	HH	19/11/2018	19/06/2019	1.0	5 Years	Google Drive - Employer - Information Security Management
ISM	WF_ISM_002	Statement of Applicability	DFW	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - Employer - Information Security Management
ISM	WF_ISM_003	Controlled Document Procedure	HH	HH	29/11/2018	29/11/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures
Risk	WF_RM_0001	Risk and Opportunities Register	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - Employer - Risk Assessment
Risk	WF_RM_0002	Audit Schedule	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - Employer - Risk Management
Risk	WF_RM_0003	Internal Audit Report Template	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - Employer - Risk Management
Risk	WF_RM_0004	Asset Register	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - Employer - Assets
Risk	WF_RM_0005	BCP and Incident Management Plan	HH/DFW	HH	27/11/2018	27/12/2019	1.1	5 Years	Google Drive - Employer - Risk Management - BCP
Risk	WF_RM_0006	Removable Media Policy	JH	HH	29/11/2018	29/11/2019	1.0	5 Years	Google Drive - All Staff - Policies & Procedures - Policies - Business & Security
Risk	WF_RM_0007	Access Control Policy	JH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies & Procedures - Policies - Business & Security
Risk	WF_RM_0008	Password Policy	JH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies & Procedures - Policies - Business & Security
Risk	WF_RM_0009	Change Management Policy	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies & Procedures - Policies - Business & Security
Risk	WF_RM_0010	Cryptographic Control Policy	JH	HH	29/11/2018	29/11/2019	1.0	5 Years	Google Drive - All Staff - Policies & Procedures - Policies - Business & Security
Risk	WF_RM_0011	Interested Parties	HH	HH	06/12/2018	06/12/2019	1.2	5 Years	Google Drive - All Staff - Policies & Procedures - Policies - Business & Security
Risk	WF_RM_0012	Test Plan	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures
Risk	WF_RM_0013	Test Plan Results	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures
Risk	WF_RM_0014	Management Action Log	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - Employer - Risk Assessment
Risk	WF_RM_0015	Management Review Procedure	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - ISO Procedures
Risk	WF_RM_0016	Management Review Meeting Agenda	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - ISO Procedures
Risk	WF_RM_0017	Management Review Minutes Template	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - ISO Procedures
Risk	WF_RM_0018	Non-conformance and Corrective Actions Procedure	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - ISO Procedures
Risk	WF_RM_0019	Risk and Opportunity Procedure	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - ISO Procedures
Risk	WF_RM_0020	RCA Template	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - ISO Procedures
Risk	WF_RM_0021	Internal Audit Plan	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - ISO Procedures
Risk	WF_RM_0022	ICO Registration Certificate	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive > Employer > Information Security Management > ICO
Risk	WF_RM_0023	Retension Policy (Data and Documents)	HH	HH	19/11/2018	19/11/2019	1.0	5 Years	Google Drive - Business & Security

10.3 Appendix 3 – Procedures Log

CareForIT Limited reviews and updates its list of procedures as part of the controlled documents log on a regular basis and the most recent version is available on Google Drive as follows:-

Google Drive – Employer – Information & Security Management – Controlled Documents

CareFor IT Limited
Operating Procedures
11/01/2019

Business_Are	Doc_Referen	Doc_Title	Owner	Sign_Off	Last Review	Next_Review	Version Numt	Document Retensic	Notes
All	WF_OP_0001	Client Cancellations Procedure	HH	20/11/2018	20/11/2018	20/11/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures
All	WF_OP_0002	Customer Support & Ticketing Procedure	HH	20/11/2018	20/11/2018	20/11/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures
All	WF_OP_0003	Client Starter Procedure	HH	20/11/2018	20/11/2018	20/11/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures
All	WF_OP_0004	Call Handling Procedure	HH	20/11/2018	20/11/2018	20/11/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures
Risk	WF_OP_0005	Internal Audit Procedure	HH	20/11/2018	20/11/2018	20/11/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures
Risk	WF_OP_0006	Risk Assessment Procedure	HH	20/11/2018	20/11/2018	20/11/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures
Risk	WF_OP_0007	System Development and Maintenance Procedure	JH	20/11/2018	20/11/2018	20/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures - System Development and Maintenance
ISM	WF_ISM_003	Controlled Document Procedure	HH	29/11/2018	29/11/2018	29/11/2019	1.0	5 Years	Google Drive - All Staff - Policies and Procedures - Operating Procedures
Risk	WF_OP_0008	Data Backup and Restore Procedure	JH	21/12/2018	21/12/2018	21/12/2019	1.0	5 Years	Google Drive - All Staff Folder - Policies and Procedures - Operating Procedures

10.4 Appendix 4 - Management Commitment

The CareFor management team fully endorse and support the stated aims of this policy and confirm our ongoing commitment to information security standard as per the ISO 27001 standard.

Managing Director Name: Richard Bedford

Date: 15/04/2020

Managing Director Signature :