
24 June 2019
# Contents

1 Overview of the Integrated Management System (IMS) ............................................. 7
  1.1 Purpose ................................................................................................................. 7
  1.2 Scope of the IMS ................................................................................................. 7
  1.3 Documents of the IMS ...................................................................................... 7
  1.4 Policies .............................................................................................................. 8
  1.5 Organisation Chart and Job Descriptions ........................................................ 8
  1.6 Training Records ............................................................................................. 8
  1.7 Processes and Procedures .................................................................................. 8
    1.7.1 Job Function (JF) Procedures ......................................................................... 9
    1.7.2 Business Management (BM) Procedures .................................................... 9
    1.7.3 Information Security (IS) Procedures .......................................................... 9
    1.7.4 Business Continuity (BC) Procedures .......................................................... 9
    1.7.5 Anti-Corruption (AC) Procedures ................................................................. 9
    1.7.6 Management System (MS) Procedures ....................................................... 9
  1.8 Approved Suppliers ......................................................................................... 9
  1.9 Work Instructions ........................................................................................... 10

Integrated Management System (IMS) – Essentials .................................................. 11

Information Security and Business Continuity Management – Essentials ................ 12

Acceptable ICT Use and Information Security Agreement ....................................... 13

Quality Policy ........................................................................................................... 15

Information Security Policy ....................................................................................... 16

Business Continuity Policy ........................................................................................ 17

Anti-Corruption Policy .............................................................................................. 18

Data Protection Policy .............................................................................................. 19

Environmental Policy .............................................................................................. 20

Anti-Slavery Statement ............................................................................................. 21

Appendix 1 – Legal and Regulatory Compliance ..................................................... 23

Appendix 2 – Context and Interested Parties ........................................................... 27

Appendix 3 – Processes ........................................................................................... 41

Appendix 4 – Guide to Opportunities and Risks ....................................................... 45

Appendix 5 – How to Maintain a Risk Register ....................................................... 49

Appendix 6 – Maintain a Business Impact Analysis ................................................ 55

Appendix 7 – Information Security Guide Part 1 – Overview .................................... 57
<table>
<thead>
<tr>
<th>Procedure Number</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>JF-13</td>
<td>Help Desk Support</td>
<td>161</td>
</tr>
<tr>
<td>JF-14</td>
<td>Remote Service and Maintenance</td>
<td>165</td>
</tr>
<tr>
<td>JF-15</td>
<td>On Site Service and Maintenance</td>
<td>167</td>
</tr>
<tr>
<td>JF-16</td>
<td>Return Used Items to Stock</td>
<td>171</td>
</tr>
<tr>
<td>JF-17</td>
<td>Technical Documentation</td>
<td>173</td>
</tr>
<tr>
<td>JF-18</td>
<td>Customer Support</td>
<td>174</td>
</tr>
<tr>
<td>JF-19</td>
<td>Alarm Receiving Centre Operation</td>
<td>177</td>
</tr>
<tr>
<td>BC-1</td>
<td>Business Continuity</td>
<td>181</td>
</tr>
<tr>
<td>BC-2</td>
<td>Emergency Lighting for the ARC</td>
<td>185</td>
</tr>
<tr>
<td>BC-3</td>
<td>Disruption of the ARC</td>
<td>186</td>
</tr>
<tr>
<td>BM-1</td>
<td>Starting and Finishing a Role</td>
<td>188</td>
</tr>
<tr>
<td>BM-2</td>
<td>Manage Provider</td>
<td>191</td>
</tr>
<tr>
<td>BM-3</td>
<td>Maintain Details of Legal and Regulatory Requirements</td>
<td>192</td>
</tr>
<tr>
<td>BM-4</td>
<td>Internal and External Communications</td>
<td>194</td>
</tr>
<tr>
<td>IS-1</td>
<td>Computer Data Backups</td>
<td>196</td>
</tr>
<tr>
<td>IS-2</td>
<td>Mobile Computing</td>
<td>198</td>
</tr>
<tr>
<td>IS-3</td>
<td>Network Management</td>
<td>201</td>
</tr>
<tr>
<td>IS-4</td>
<td>Change Control</td>
<td>203</td>
</tr>
<tr>
<td>IS-5</td>
<td>Working in Secure Areas</td>
<td>206</td>
</tr>
<tr>
<td>IS-6</td>
<td>Information Classification, Handling and, Clear Desk and Screen</td>
<td>209</td>
</tr>
<tr>
<td>IS-7</td>
<td>Access Control and Rights Review</td>
<td>219</td>
</tr>
<tr>
<td>IS-8</td>
<td>Intellectual Property</td>
<td>221</td>
</tr>
<tr>
<td>AC-1</td>
<td>How to Respond to (Potential) Corruption</td>
<td>224</td>
</tr>
<tr>
<td>DP-1</td>
<td>Data Protection Impact Assessment (DPIA)</td>
<td>225</td>
</tr>
<tr>
<td>DP-2</td>
<td>Data Subject Access Request (DSAR)</td>
<td>226</td>
</tr>
<tr>
<td>DP-3</td>
<td>Notification of Rights and Processing</td>
<td>230</td>
</tr>
<tr>
<td>MS-1</td>
<td>Control of Documents</td>
<td>232</td>
</tr>
<tr>
<td>MS-2</td>
<td>Control of Records</td>
<td>235</td>
</tr>
<tr>
<td>MS-3</td>
<td>Internal Audit</td>
<td>237</td>
</tr>
<tr>
<td>MS-4</td>
<td>Response to Non-Conformity or Incident (including Corrective Action)</td>
<td>239</td>
</tr>
<tr>
<td>MS-5</td>
<td>IMS Review Meeting</td>
<td>242</td>
</tr>
<tr>
<td>MS-6</td>
<td>Preventive Action</td>
<td>246</td>
</tr>
</tbody>
</table>

Annex 3 – Information Asset Register ................................................. 247
Approved Free and Open Source Software ..................................................... 259


Changes........................................................................................................... 277
1 Overview of the Integrated Management System (IMS)

1.1 Purpose

Our Integrated Management System (IMS) enables us to implement the following:

1. Quality Management in accordance with ISO 9001;
2. Information Security Management in accordance with ISO 27001;
3. The requirements of the NHS Information Governance Statement of Compliance (IGSoC);
4. Business Continuity Management;
5. Anti-Corruption Management.

1.2 Scope of the IMS

Voice Connect design, develop, supply and support the following:

- Integrated telephony and multiple media computer messaging products and services;
- An Alarm Receiving Centre (ARC) that provides a lone worker monitoring service;
- A Payment Portal that enables a cardholder to make secure payments.

Our IMS covers all of our operations.

We exclude the following sections of ISO 9001.

Section 7.1.5.2 Measurement traceability
We do NOT use any monitoring or measuring equipment.

1.3 Documents of the IMS

The IMS consists of the following documents.

- IMS Manual
- Organisation Chart
- Business Impact Analysis
- Risk Register
- Statement of Applicability

We give the IMS Manual and Organisation Chart to each new employee that joins the company. If either document changes, we distribute the changed document to all employees. Where appropriate, we also provide these documents to contractors.
1.4 Policies

The IMS contains the following five policies and operates based on the first four shown in **bold italics**.

*Quality Policy*
*Information Security Policy*
*Business Continuity Policy*
*Anti-Corruption Policy*
*Environmental Policy*

Also, employees must agree to, and sign, the following.

**Acceptable ICT Use and Information Security Agreement**

1.5 Organisation Chart and Job Descriptions

The Organisation Chart is a separate document that shows the structure of Voice Connect, with the names and Job Titles of all employees. It is updated and distributed to everyone, whenever someone joins or leaves the organisation, or changes roles. Each Job Title on the Organisation Chart corresponds to a Job Description.

| NOTE | Annex 1 contains the Job Descriptions. |

(1) Most employees do one or more procedural job functions. Some also do non-procedural job functions, such as administration or management. Each Job Description specifies the following:

(a) Principal Job Function (JF) procedures; refer to Section 1.7.1 (Page 9);
(b) Other applicable procedures, listed in the remainder of Section 1.7 (Page 8);
(c) Additional non-procedural job functions.

(2) Each Job Description also specifies the Knowledge and Skills that the employee requires. These are an amalgamation of any Knowledge and Skills required by the following:

(a) Any procedure(s) that the employee does;
(b) Any additional non-procedural job functions.

1.6 Training Records

(1) Each employee’s Training Record contains the following.

(a) The Knowledge and Skills that the employee had when he/she joined Voice Connect.
(b) Any Training that Voice Connect has provided to the employee.
(c) Any Training that Voice Connect schedules for the employee (to acquire any required skills as specified on the employee’s job description).

(2) The cumulative training required by all the employees of Voice Connect, enables the organisation to plan and implement a schedule of training for its employees.

1.7 Processes and Procedures

The IMS has six categories of procedures, which the following sub-sub-sections describe.

| NOTE | Annex 2 contains the Procedures. |
1.7.1 Job Function (JF) Procedures

These procedures describe core job functions that contribute to the provision of our products and services. Each one specifies the skills required to do the procedure.

**NOTE**  
Appendix 3 provides details of our processes.

1.7.2 Business Management (BM) Procedures

These procedures satisfy general business requirements and requirements of ISO 27001 and ISO 22301.

1.7.3 Information Security (IS) Procedures

These procedures satisfy requirements of ISO 27001.

<table>
<thead>
<tr>
<th>NOTES</th>
<th>(1) Procedures in other sub-sub-sections cover requirements of ISO 27001.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(2) The Employee’s Handbook contains a Disciplinary Procedure.</td>
</tr>
</tbody>
</table>

1.7.4 Business Continuity (BC) Procedures

These procedures satisfy general business continuity requirements and requirements of ISO 27001, Control A.17.1.

1.7.5 Anti-Corruption (AC) Procedure

This procedures addresses requirements of the UK Bribery Act 2010 and customer contractual requirements to implement arrangements to respond to (potential) bribery and any other form of corruption.

1.7.6 Management System (MS) Procedures

These procedures cover requirements of ISO 9001, ISO 27001 and ISO 22301. Procedures MS1 to MS-4 cover explicit requirements for procedures. Procedure MS-5 covers requirements for the inputs, outputs and records of management reviews.

1.8 Approved Suppliers

The Stock and Purchases Database can assign one of four categories to each supplier.

- **ON Trial**
- **Approved**
- **Do Not Use**
- **In Use**

Initially, new suppliers are assigned the category **On Trial** and if found to be satisfactory are then assigned the category **Approved**. The Technical Director authorises the assignment of a category to a supplier in the Stock and Purchases Database. The database can output a List of Approved Suppliers, which is a list of those suppliers, assigned the category **Approved**, as described above.
1.9 Work Instructions

Where appropriate, procedures are supplemented by Work Instructions. The following table lists the owner of each Work Instruction (usually the relevant team manager), who authorises each issue of it.

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VC1 Build Notes (DOS)</td>
<td>Operations Director</td>
</tr>
<tr>
<td>2</td>
<td>System Reboot Process</td>
<td>Operations Director</td>
</tr>
<tr>
<td>3</td>
<td>Ghost Instructions – Patient Partner</td>
<td>Operations Director</td>
</tr>
<tr>
<td>4</td>
<td>Guidelines for Appraisals</td>
<td>Operations Director</td>
</tr>
<tr>
<td>5</td>
<td>121 Guidelines</td>
<td>Operations Director</td>
</tr>
<tr>
<td>6</td>
<td>VC II Build Notes – Windows 2000</td>
<td>Operations Director</td>
</tr>
<tr>
<td>7</td>
<td>Customer Service Database – Guidance, Categories and Owners</td>
<td>Operations Director</td>
</tr>
<tr>
<td>8</td>
<td>(Brooktrout) Tone Tables</td>
<td>Operations Director</td>
</tr>
<tr>
<td>9</td>
<td>VC II Build Notes – Windows NT4</td>
<td>Operations Director</td>
</tr>
<tr>
<td>10</td>
<td>Manage Customer Hosted Installation</td>
<td>Operations Director</td>
</tr>
<tr>
<td>11</td>
<td>Installation</td>
<td>Operations Director</td>
</tr>
<tr>
<td>12</td>
<td>Processing Voicemail Retrieval Requests for the Met Police</td>
<td>Operations Director</td>
</tr>
<tr>
<td>13</td>
<td>Customer Maintenance or Product Specific Contract Cancellation</td>
<td>Operations Director</td>
</tr>
<tr>
<td>15</td>
<td>Termination of Use of Medical Messenger with EMIS software</td>
<td>Accounts</td>
</tr>
<tr>
<td>16</td>
<td>Moves and Changes – Patient Partner</td>
<td>Commercial Director</td>
</tr>
<tr>
<td>18</td>
<td>TV and Internet Rules</td>
<td>Technical Director</td>
</tr>
<tr>
<td>21</td>
<td>Build SMS Gateway</td>
<td>Technical Director</td>
</tr>
<tr>
<td>22</td>
<td>Helpdesk Monitoring</td>
<td>Operations Director</td>
</tr>
<tr>
<td>24</td>
<td>Change a Customer’s Details on All Databases</td>
<td>IMS Manager</td>
</tr>
<tr>
<td>26</td>
<td>Sending and Responding to Emails</td>
<td>Operations Director</td>
</tr>
<tr>
<td>27</td>
<td>Upgrade Advice</td>
<td>Operations Director</td>
</tr>
<tr>
<td>28</td>
<td>Being OnCall and Managing a Call Out</td>
<td>Operations Director</td>
</tr>
<tr>
<td>29</td>
<td>Supporting VC Alarm Receiving Centre</td>
<td>Operations Director</td>
</tr>
<tr>
<td>30</td>
<td>How to change the URLs of the ARC servers</td>
<td>Network Manager</td>
</tr>
<tr>
<td>32</td>
<td>Alarm Receiving Centre – Admin Process</td>
<td>Technical Director</td>
</tr>
<tr>
<td>33</td>
<td>Handover and System Check Instructions</td>
<td>Technical Director</td>
</tr>
<tr>
<td>34</td>
<td>Customer Campaigns in CRM</td>
<td>Commercial Director</td>
</tr>
<tr>
<td>36</td>
<td>Alarm Receiving Centre - Preparing User Reports</td>
<td>Technical Director</td>
</tr>
<tr>
<td>39</td>
<td>Processing a New User Request - Hosted Voicemail</td>
<td>Operations Director</td>
</tr>
<tr>
<td>40</td>
<td>ARC Cooperation</td>
<td>Technical Director</td>
</tr>
</tbody>
</table>

**NOTE** Italics indicate that the Work Instruction applies to a specific customer.
Integrated Management System (IMS) – Essentials

3 April 2019

The Integrated Management System (IMS) includes the following documents, which are available on both our network and implementation of Microsoft SharePoint, in separate shared folders.

(1) Organisation Chart. (The Telephone List, which is not part of the IMS, is in the same folder.)

(2) IMS Manual. This includes the following components that apply to all workers.

- Summary sheets (including this one)
- Acceptable ICT Use and Information Security Agreement
- Information Security Guides (1, 2 and 3)
- Job Descriptions (in Annex 1)
- Procedures (in Annex 2)

(3) Work Instructions

(4) Numbered documents (such as forms etc.)

The IMS provides the documentation, which you require, to fulfil your role, as follows.

(1) The Organisation Chart specifies your Job Title.

(2) IMS Manual - Annex 1 contains the Job Description that corresponds to your Job Title.

(3) IMS Manual - Annex 2 contains the Procedures specified on your Job Description.

(4) Each Procedure specifies, at the start, any Work Instructions that supplement it.

(5) Procedures and Work Instructions specify, at appropriate points, any required numbered documents.

Nonconformities, Complaints and (Information Security) Incidents

It is important that any detected non-conformity, (customer or third party) complaint or incident is raised, investigated and recorded to determine, implement and record any appropriate correction and corrective action, in accordance with Procedure MS-4 - Response to Non-conformity or Incident.

NOTE A failure to do this may result in the issue being detected and raised as a non-conformity or incident during an external (certification) audit. Furthermore, the failure to raise and manage the issue in accordance with Procedure MS-4, as required by ISO 9001, ISO 27001 and ISO 22301, may unnecessarily lead to one or more further non-conformities being raised.

Definitions from ISO 9000, ISO 27000 and ISO 22301

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>nonconformity</td>
<td>non-fulfilment of a requirement</td>
</tr>
<tr>
<td>correction</td>
<td>action to eliminate a detected non-conformity</td>
</tr>
<tr>
<td>corrective action</td>
<td>action to eliminate the cause of a non-conformity and to prevent recurrence</td>
</tr>
</tbody>
</table>
Properties and Classifications of Information

Integrity
Completeness and accuracy of information.

Availability
Ability to access information (by people that require access to it).

Confidentiality
Prevention of access to information by those that must not access it.

CIA
Confidentiality, Integrity, Availability

VC-Confidential
Information that must only be disclosed to people that require it.

VC-Restricted
Information, not proprietary or sensitive, intended for specific people.

VC-Unclassified
Information that can be disclosed to anyone.

Documents

<table>
<thead>
<tr>
<th>Information Asset Register</th>
<th>An inventory of all of our information assets. This document is VC-Restricted, in the IMS Manual, Annex 3.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context and Interested Parties</td>
<td>Context is what we do. Interested Parties is what other people want us to do. This document is VC-Unclassified, in the IMS Manual, Appendix 2.</td>
</tr>
<tr>
<td>Business Impact Analysis</td>
<td>Analysis of how scenarios of disruption would affect business operations and required periods of resumption. This is a separate VC-Confidential document (compiled according to IMS Manual, Appendix 6).</td>
</tr>
<tr>
<td>Risks and Opportunities</td>
<td>Risks and opportunities arising from the Context and Interested Parties, and what we do in response to them. This is a separate VC-Restricted document (compiled according to IMS Manual, Appendix 4).</td>
</tr>
<tr>
<td>Risk Register</td>
<td>Threats to information security and business continuity, our vulnerabilities to them, what we do to manage them and references to any applicable ISO 27001 Annex A controls. This is a separate VC-Confidential document (compiled according to IMS Manual, Appendix 5).</td>
</tr>
<tr>
<td>Information Security, Business Continuity and other Policies</td>
<td>The main policies governing our implementation of information security, business continuity and quality etc. (See also Policies and Procedures below.) These documents are VC-Unclassified, in the IMS Manual.</td>
</tr>
<tr>
<td>Policies and Procedures</td>
<td>Procedures IS-1 to IS-8 and DP-1 to DP-3 apply specifically to information security and Procedures BM-1 to BM-3 apply specifically to business continuity. Other procedures may contain provisions to implement aspects of information security and/or business continuity, in addition to implementation of other aspects, such as quality. These documents are VC-Restricted, in the IMS Manual, Annex 2.</td>
</tr>
<tr>
<td>Statement of Applicability</td>
<td>A list of all ISO 27001 Annex A controls, those that we select and why, and those that we do not select and why. The required version with inclusions and exclusions is VC-Restricted. The version with full details is a separate VC-Confidential document.</td>
</tr>
</tbody>
</table>
Information Security Policy and IMS Requirements

In this agreement WE, US and OUR refer to Voice Connect Limited and all workers (employees, agency workers and contractors) that work for Voice Connect Limited.

We operate an Integrated Management System (IMS), which manages quality, information security, business continuity and anti-corruption. The IMS is governed by the following five principal policies. You must comply with these and other policies, all procedures, and other requirements, of the IMS.

- Quality Policy
- Information Security Policy
- Business Continuity
- Anti-Corruption Policy
- Data Protection Policy

Acceptable ICT (Information and Communications Technology) Use

The purpose of this section is to secure the resources that Voice Connect Limited provides to its workers. All workers must use these resources responsibly, professionally, ethically, and lawfully.

Voice Connect Limited provides portable computing and communication devices (including laptops, tablets and smart-phones) and portable storage devices, to some workers, to enable them to work. All portable devices must be used securely, and as specified by Procedure IS-2 – Mobile Computing.

1. You receive access to our network to enable you to do your work. You should not have any expectation of privacy in anything you create, store, send or receive. The computer system belongs to Voice Connect Limited and may only be used for business purposes.

2. You MUST ONLY connect to our network, directly or through VPN, devices provided by Voice Connect Limited or devices approved by the Technical Director.

3. You MUST NOT disclose your network password to anyone, including other workers. If you suspect that anyone else knows your password, you MUST immediately notify the Network Manager or Technical Director and change it. Failure to safeguard your network password may result in disciplinary action.

4. Visitors MUST NOT connect to our network. Visitors that require internet access may use our wireless broadband (which is entirely separate from our network).

5. You MUST take appropriate care to manage your emails. If you receive any unsolicited email that you suspect MAY be harmful or malicious:
   
   (a) Do NOT click on any links;
   (b) Report it to the Network Manager and/or Technical Director.

6. You MUST NOT use our network and/or resources to do any of the following activities. If you become aware of anyone using computer resources for any of these activities, you must report the incident immediately to your line manager.
   
   (a) Knowingly visit websites that may contain unlawful or offensive material, or malware.
   (b) Send, receive, download, display, print or disseminate material that is unlawful, sexually explicit, profane, obscene, harassing, fraudulent, defamatory or offensive.
(c) Knowingly disseminate or store malware, or any other unauthorised material.

(d) Waste computer resources through non-business activities: for example; spend excessive amounts of time on the Internet, play games, send mass mailings or chain mailings or chain letters or any other activity that creates unnecessary network traffic.

(e) Use or copy software in violation of a license agreement or copyright.

**NOTE** Violation of a software licence agreement constitutes a violation of copyright law.

---

**Client, Information and Data, Confidentiality and Security**

The purpose of this section is to ensure that all information about clients, and their data, which we acquire, record and use, is correct and secure.

(A) You must obtain, from a client, any information about the client that we do not already have, which you require to fulfil your duties.

(B) You must record the information accurately, in the appropriate database or elsewhere, as appropriate, in accordance with any relevant job function procedures.

(C) You must NOT record any personal data, other than names and work contact details. (If you access any personal data that you do not require you breach data protection law.)

(D) You must ONLY disclose to a third party (such as a dealer), any information about a client, which the third party reasonably requires, to fulfil any contractual obligations. You must otherwise NOT disclose any information about a client to anyone else, whilst you work for Voice Connect Limited.

(E) You must ONLY lawfully access or retrieve any data, from a client or that the client controls, which you require, to fulfil your duties, and if the client expressly permits you to do so.

(F) You must NEVER disclose any information about a client to anyone, if you leave Voice Connect Limited.

---

**Law**

We must comply with all applicable UK and international law, including the following:

- European Union (EU) General Data Protection Regulation (GDPR);
- UK Data Protection Act 2018;
- Privacy and Electronic Communications (EC Directive) Regulations 2003;

---

**Breaches of this Agreement**

Violations of this agreement will be taken seriously and may result in disciplinary action, including possible termination of employment, and civil and criminal liability.

Name…………………………………………………………………………………
I have read and agree to comply with the terms of this agreement.

Signature…………………………………………………………………………

Date………………………………………………………………………………
Quality Policy

3 April 2019

Voice Connect design, develop, supply and support the following:

Integrated telephony and multiple media computer messaging products and services;  
An Alarm Receiving Centre (ARC) that provides a lone worker monitoring service;  
A Payment Portal that enables a cardholder to make secure payments.

Voice Connect operates an Integrated Management System (IMS) that implements the following:

Quality Management, certified to ISO 9001;  
Information Security Management, certified to ISO 27001;  
Business Continuity Management;  
Anti-Corruption Management.

Voice Connect will do the following:

Comply with all applicable legal, contractual and other requirements and obligations;  
Continually improve the effectiveness of the IMS.

Our quality objectives are as follows.

(1) To reduce, over each financial year, the number of customers lost, as a percentage of the total number of customers (at the start of the financial year), by 1% [of the total number of customers (at the start of the financial year)].

(2) To reduce, over each financial year, the number of 90 day debtors, as a percentage of the total number of debtors, by 1% [of the total number of debtors].

(3) To reduce, over each financial year, the number of Active Support Jobs, as a percentage of the total number of customers, by 0.5% [of the total number of customers].

The management will review the following, at least once each year:

The suitability of this policy;  
The objectives of this policy;  
Legal requirements and how we comply with them.

_______________________________ Stefan Olsberg, Managing Director
Information Security Policy
3 April 2019

Voice Connect design, develop, supply and support the following:

Integrated telephony and multiple media computer messaging products and services;
An Alarm Receiving Centre (ARC) that provides a lone worker monitoring service;
A Payment Portal that enables a cardholder to make secure payments.

Voice Connect operates an Integrated Management System (IMS) that implements the following:

Quality Management, certified to ISO 9001;
Information Security Management, certified to ISO 27001;
Business Continuity Management;
Anti-Corruption Management.

The scope of our information security management covers all of our operations.

Voice Connect will do the following:

Comply with all applicable legal, contractual and other requirements and obligations;
Continually improve the effectiveness of the IMS.

Our information security objectives are as follows.

(1) To annually provide information security awareness training to all staff, to ensure that they
can fulfil the information security requirements of their roles.

(2) To ensure that the details of all lone workers of our ARC customers, which we record on our
VC LoneWorker ARC database, completely and accurately, correspond to the details of the
lone workers that our ARC customers supply to us.

(3) To ensure that our ARC achieves 99.5% availability to our customers as defined by Annex A

(4) To ensure that hardware and software products and services that we provide maintain
availability, confidentiality, integrity, legal and contractual compliance of customers’
information that the hardware and software products and services process.

(5) To maintain availability, confidentiality, integrity, legal and contractual compliance of
customers’ information stored by hardware and software products and services that we
provide, when we do remote or on-site maintenance.

The management will review the following, at least once each year:

The suitability of this policy;
The objectives of this policy;
Legal requirements and how we comply with them.

_________________________________________ Stefan Olsberg, Managing Director
Business Continuity Policy

3 April 2019

Voice Connect design, develop, supply and support the following:

- Integrated telephony and multiple media computer messaging products and services;
- An Alarm Receiving Centre (ARC) that provides a lone worker monitoring service;
- A Payment Portal that enables a cardholder to make secure payments.

Voice Connect operates an Integrated Management System (IMS) that implements the following:

- Quality Management, certified to ISO 9001;
- Information Security Management, certified to ISO 27001;
- Business Continuity Management;
- Anti-Corruption Management.

The scope of our business continuity management covers all of our operations.

Voice Connect will do the following:

- Comply with all applicable legal, contractual and other requirements and obligations;
- Continually improve the effectiveness of the IMS.

Our business continuity objectives are that following disruption, we can recover, within:

1. 5 minutes - Alarm Receiving Centre (ARC) lone worker protection service and On-Call Technical Support;
2. 1 hour - main number telephone communication and access to our off-site hosted services (SMS Gateway, Hosted Voicemail and Payment Portal);
3. 3 days - Microsoft Exchange and Outlook, auto-attendant and voicemail, accounts, Customer Service Database and normal hours (8am-6pm) Technical Support;
4. 1 week - Microsoft SharePoint, CRM, partial operation of telemarketing, sales, and provision of products and services.

The management will review the following, at least once each year:

- The suitability of this policy;
- The objectives of this policy;
- Legal requirements and how we comply with them.

______________________________ Stefan Olsberg, Managing Director
Anti-Corruption Policy
3 April 2019

Voice Connect will do the following:

Comply with all applicable legal, contractual and other requirements and obligations.

We will not, either directly or through a third party:

Give or receive bribes or improper advantages;

Give or receive facilitation payments;

Give or receive any gift, hospitality, donation or benefit that may improperly influence a decision or impair independence or judgement.

We will not participate in any cartel.

We will not defraud or deceive anyone or act dishonestly.

We will not participate in any criminal activity, such as extortion, collusion, breach of trust, abuse of power, embezzlement, trading in influence or money laundering.

Conflicts of interest: We will avoid, or deal appropriately with, situations in which our own interests could conflict with our obligations or duties.

Personnel and controlled organisations: We will ensure that our workers, and organisations that we control, comply with this policy.

Business associates: We only work with organisations and people that conform to standards consistent with our own.

Implementation

Overall responsibility for implementation and review of this policy rests with senior management. However, all workers must adhere to and support this policy. We will inform all current and future workers about this policy and their role in its implementation.

The management will review the following, at least once each year:

The suitability of this policy;
Legal requirements and how we comply with them.

______________________________  Stefan Olsberg, Managing Director
Voice Connect will do the following.

(1) We will comply with all applicable legal, contractual and other requirements and obligations (including the following principal data protection legislation).

   European Union – Regulation 2016/679 (GDPR)
   United Kingdom – Data Protection Act 2018

(2) We will ONLY transfer personal data, if necessary (to fulfil a contract), to any of the following:

   (a) A member of the European Economic Area (EEA) [EU plus Norway, Iceland and Liechtenstein];

   (b) A country or state approved by the European Commission of the EU as having equivalent protection to the EU. Those currently approved are as follows.

   Isle of Man  
   Jersey  
   Guernsey  
   Andorra  
   Faroe Islands  
   Switzerland  
   Israel  
   Japan  
   Argentina  
   Uruguay  
   New Zealand  
   Canada (commercial organisations)  
   United States of America (limited to the Privacy Shield framework)

*Note*  The process of approval involves an opinion by the European Data Protection Board (EDPB) [https://edpb.europa.eu].

We will NOT transfer personal data to any other country or state.

The management will review the following, at least once each year:

The suitability of this policy;
Legal requirements and how we comply with them.

________________________________________  Stefan Olsberg, Managing Director
Voice Connect will:

(1) Comply with all applicable legal, contractual and other environmental requirements and obligations;

(2) Reuse materials where possible;

(3) Recycle materials and consumables where possible;

(4) Minimise our consumption of materials, utilities and fuel where possible.

_______________________________ Stefan Olsberg, Managing Director
Voice Connect Limited does not currently fall within the scope of the Modern Slavery Act 2015. (This is because its turnover is substantially below the present threshold of £ 36 million. However this threshold may be revised.)

We recognise the importance of measures to combat modern slavery, which we acknowledge is a serious problem that governments and international organisations must address and have decided to voluntarily provide a statement in accordance with the Modern Slavery Act 2015.

(1) We unequivocally oppose any manifestation of slavery.

(2) If we become aware of any practice of slavery, we will report it to the police.

(3) We shall terminate as soon as possible any relationship with an organisation or individual that practices, or intentionally and directly benefits from, the practice of any form of slavery.

Our business is a small enterprise (with approximately 30 employees) and we believe that there is no risk of slavery within our organisation.

We perceive the risk of modern slavery to be insignificant amongst the majority of our providers, such as those that can be categorised with one or more of the following attributes:

(a) Suppliers and partners that provide technological products and services, and which employ skilled staff;

(b) Small enterprises with very few employees, which are also generally composed of skilled staff;

(c) Suppliers and partners with which we have a close working relationship and/or are in regular personal contact.

Where we consider that there is a conceivable risk of slavery with respect to a provider we shall endeavour to obtain an Anti-Slavery Statement from the provider, to ensure that we know that the provider is aware of the existence and requirements of the Modern Slavery Act 2015:

(i) Either because the provider falls within the scope of the Modern Slavery Act 2015 and must provide the statement;

(ii) Or the provider does not fall within its scope, but is nevertheless willing to voluntarily provide a statement in accordance with the Modern Slavery Act 2015.
Appendix 1 – Legal and Regulatory Compliance

This appendix details how we comply with the legal and regulatory requirements that are relevant to aspects of operations that our Integrated Management System (IMS) manages.

It covers ISO 27001, Control A.18.1.1 (which requires details relevant to information security).

Legislation

GDPR (General Data Protection Regulation) and Data Protection Act 2018

<table>
<thead>
<tr>
<th>NOTES</th>
<th>(1) The GDPR is European Union (EU) Regulation 2016/679.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(2) The United Kingdom (UK) Data Protection Act 2018 implements qualifications to the GDPR and also European Union (EU) Directive 2016/680, which governs processing of personal data for purposes of law enforcement.</td>
</tr>
</tbody>
</table>

(1) All employees receive information security training, which includes an overview of data protection.

(2) Several of our products communicate with other software based information systems, as a result of collaborative software development with our partners. The following are the principal products.

- Informer
- Patient Partner
- Medical Messenger

To install, configure and maintain systems based on these and other products, we require a username and password to enable our software to log in to our partners' information systems, and access student or patient data. The following procedures contain instructions that require us to request a username and password that provides access to personal (contact) data, which our product requires, but forbids access to sensitive personal data (educational or medical information), which our product does not require.

- JF-7 Project Management
- JF-11 Installation
- JF-12 Training
- JF-13 Help Desk Support
- JF-14 Remote Service and Maintenance
- JF-15 On-Site Service and Maintenance

(3) Since the end of 2012 we have operated a hosted lone worker protection facility, provided by our Alarm Receiving Centre (ARC), which now requires us to hold personal data, namely contact details, and in some cases, sensitive personal data, namely medical details, such as required regular medication, epilepsy etc.

Our customer supplies the details of their lone workers to us and it is their responsibility to ensure the accuracy of the details they supply to us. We record these details in our system and may supply a copy to our customer, to verify. If an ARC customer informs us that a person is no longer a lone worker, we remove the person's details.
(4) The Technical Director and Operations Director can access paper personnel files, which are stored in a locked filing cabinet. The paper personnel files are being scanned and uploaded to an online HR management facility. The Technical Director, Operations Director and Commercial Director will have full access to this.

We use an Internet facility to process some of our personnel data. We are the Data Controller and the agency is the Data Processor. The processing of our employee’s personal data is covered by a Data Processing Agreement to ensure that the processing complies with the requirements of data protection law (as if we were processing the data).

(5) Only Accounts staff have access to details of salary payments.

Subject Access Request

The customers of our hosted lone worker protection facility provide details of their lone workers to us. We could receive a Subject Access Request from a lone worker for the details we hold about/him/her and would respond in accordance with the GDPR.

Privacy & Electronic Communications (EC Directive) Regulations 2003

We use email and postal mail to market our products and services but we only market to organisations, we do not market to private individuals.

Freedom of Information Act 2000

We do not consider that we hold any information that this act could require us to disclose, and have never received any such request under the provisions of this act.

If we received a request to disclose information, under the provisions of this act, we would evaluate the validity of and justification for, the request, and if necessary seek legal advice, and respond appropriately.

Computer Misuse Act 1990

We require all employees to sign our Acceptable ICT Use and Information Security Agreement.

Copyright, Designs and Patents Act 1988

Procedure IS-8 – Intellectual Property.

WEEE Directive

We produce some waste electrical and electronic equipment, as a result of supplying the following:

- New computers to new customers;
- Maintenance or upgrade replacement computers to existing customers.

We dispose of this waste through a registered provider of WEEE compliant waste disposal services.
Occupational Health and Safety Legislation and Regulations

The following document lists all applicable occupational health and safety legislation and regulations.

HSC13

This can be downloaded from the website of the UK Government – Health and Safety Executive.

www.hse.gov.uk

Contractual Requirements

Software Development Partners

The Technical Director and Chief Design Engineer manage implementation of these.

Our software development team have collaborative partnerships with other companies.

These are listed above in GDPR and Data Protection Act, Item (2).

These partnerships are governed by commercial agreements including mutual non-disclosure and confidentiality clauses.

Commercial – Partners and Customers

The Technical, Sales and Commercial Directors manage implementation of these.

Our Premier Plus customers require us to respond to helpdesk calls 24/7/365 within 2 hours.

We always have an On-Call Engineer on duty.

Our LoneWorker Alarm Receiving Centre (ARC) customers require us to maintain uninterrupted 24/7/365 operation.

Our ARC has dual geographically separated computers (that replicate data) and dual SIP phone lines to enable us to maintain continuous uninterrupted operation of the service from any location.

Contractors

The Technical, Sales and Operations Directors manage implementation of these.

Employees

The Technical, Sales, Commercial and Operations Directors manage implementation of these.
Appendix 2 – Context and Interested Parties

Our Organisation and its Context

Purpose, Activities and Functions

Voice Connect Limited is a software company that provides messaging products and services.

Background

Voice Connect Limited was founded in 1990 to provide add-on voicemail and auto-attendant facilities for telephone systems, which at that time did not include those features. This first product was called the Voice Connector. It was a standard computer, running Microsoft DOS, fitted with one or more telephony cards and connected to a telephone system. Its replacement, the VCII, offered a more sophisticated voicemail and auto-attendant facility. It was a messaging platform that also enabled modules to be added, which provide supplementary facilities and features. This has evolved into our current offering, the VC3, which can now operate with SIP (internet telephony) as well as conventional analogue and digital telephony. As telephone systems became more sophisticated and included a voicemail and auto-attendant facility as a standard feature this effectively eliminated most, but not all, of our initial market. This compelled us to develop and market alternative products and services.

External Issues

Political

The following two categories of our customers may be affected by political developments that influence policies, priorities and budgets.

NHS The NHS is subject to contradictory pressures. An increasing number of elderly people, due to the success of the NHS in improving health and prolonging life, require progressively more medical care as they age. This means that the NHS must provide an ever increasing quantity of care. However, it is funded from taxation so the government is faced with demands for a budget that invariably exceeds inflation and/or growth of the national economy. This pressure can build up, prompting the government to initiate a review.

The NHS is currently stable following a substantial reorganisation in 2013 to 2014. The abolition of Primary Care Trusts (PCTs), on 31 March 2013, which controlled approximately 80% of the NHS budget, and their replacement with Clinical Commissioning Groups (CCGs) and Commissioning Support Units (CSUs) caused significant disruption to the healthcare market, with a reduction in orders to suppliers as personnel and budgets were reassigned.

Government Obliged to provide services, and strictly comply with legal requirements, but invariably under budgetary pressure.

Economic

A significant proportion of our customers are public sector entities (predominantly medical practices), which operate with annual budgets that correspond to Her Majesty’s Revenue and Customs (HMRC), April to March, financial year. Many retain a proportion of their budget to cover contingencies and then release it towards the end of the financial year. This means that we must plan to receive a significant proportion of our revenue in the last quarter (January to March) of the financial year.
Social

The principal social issue that concerns us is demographic related to technological; specifically, how different age groups use communications technology. The use of mobile device (smartphone and tablet) apps is now routine amongst younger people and increasingly common amongst middle aged people. There is now an expectation that organisations provide apps to access their products and services. Older people increasingly possess smartphones and utilise SMS text messaging and email. Where appropriate, we must consider the provision of mobile device apps, as an alternative method of communication, in addition to voice calls, SMS text messaging and email in our products and services.

Technological

Changes and advances in information and communications technology predominantly influence how we provide our products and services. The following are some of the issues that we must consider:

- Increasing use of mobile devices (smartphones and tablets) and mobile device apps;
- Increasing use, acceptance and expectations of cloud products and services;
- Increasing use of internet telephony;
- Replacement in the (BT) national communication infrastructure of ISDN with SIP services;
- Upgrades of Microsoft Windows server and client operating systems;
- Upgrades of Microsoft applications (such as Microsoft Dynamics CRM).

National Health Service medical practices (and hospitals) constitute a significant proportion of our customers. Commissioning Support Units (CSUs) [that manage Information and Communications Technology (ICT) for Clinical Commissioning Groups (CCGs) and individual medical practices] may impose technical requirements, with the result that implementation of some of our products and services becomes uneconomic.

Legal

Refer to Appendix 1 for details of our legal requirements and how we comply with them.

NOTE Appendix 1 covers ISO 27001, Annex A, Control A.18.1.1, which requires an organisation to specify how it complies with legal requirements that apply to information security.

Environmental

There are two principal environmental issues that concern us. The first of these, the WEEE Regulations, is also a legal issue.

WEEE The WEEE Regulations 2006 require us to dispose of Waste Electrical and Electronic Equipment through a registered provider of WEEE compliant waste disposal services. (See Appendix 1.)

Weather Severe weather could adversely affect our operations.

We are increasingly able to implement our products and services remotely. Also, we now utilise remote presentation to sell software. Therefore, we increasingly rely upon communications utilities. Although less than in the past, we continue to rely upon the ability to physically visit, potential customers (to be able to sell our products and services) and existing customers to provide after sales support.
Internal Issues

Infrastructure

We must maintain and develop our ICT infrastructure so that it:

(1) Can provide our hosted (cloud) services:
(2) Remains secure;
(3) Provides resilience in the event of disruption.

Human Resources

We provide a broad range of products and services with relatively few staff. Also, the products and services that we provide, utilise progressively less hardware and progressively more software, internet telephony and hosted (cloud) services. Consequently we must do the following.

(1) Ensure that our staff possess or acquire the required knowledge and skills to be able to effectively, market, sell, provide and support our products and services, so that customers’ expectations are met or exceeded.
(2) Allocate roles to staff to optimally utilise their knowledge, skills and abilities.
(3) Ensure that information is effectively communicated to, by and between staff, to reinforce (2).

Financial Resources

We wish to increase the proportion of recurring revenue sales (such as services that customers pay for by monthly or annual subscription) with respect to capital expenditure sales (such as products based upon a physical or virtual computer that customers pay for with a substantial initial payment).

If recurring revenue sales increase faster than total sales, this may temporarily reduce revenue and adversely impact cash-flow, which may constrain us to defer some spending on investment, training and recruitment etcetera.

NOTE The remainder of this section Our Organisation and its Context addresses requirements of ISO 22301.

Products and Services

The following are some of our principal products and services.

Service - Payment Portal

This service enables a cardholder to use a touch tone phone (or a web interface) to make secure card payments.

Product - LoneWorker

One product we developed was VC LoneWorker, based upon our messaging platform, the VCII. This provides an organisation with a powerful lone worker protection facility, able to handle large numbers of lone workers, in addition to the sophisticated voicemail and auto-attendant facility. It enables a lone worker to record a message and set an expiry time before starting a task. If the lone worker does not clear the message before the expiry time or extend the expiry time, it issues an alert.
**Service - Alarm Receiving Centre (ARC) Lone Worker Protection**

We also now offer operation of VC LoneWorker as a hosted service, paid for by subscription, based on the number of lone workers. This is a cost effective alternative to an in-house system, for organisations with many lone workers, but it also offers a service that is affordable to many other organisations regardless of their numbers of lone workers.

**Product - Patient Partner**

A current successful product is Patient Partner. This is an automated system that enables a patient to use a telephone keypad to book, change and cancel an appointment at any time of the day or night, every day of the year. It is the result of collaborative software development with five other companies that provide information systems for medical practices. Medical information systems increasingly provide the ability to manage appointments online, but we are the only company to enable patients to manage appointments by phone.

**Service - SMS Gateway**

This SMS text message service enables subscribers to send single or multiple SMS text messages, and is provided through the following website. The website also provides access to another service called SmartMail that enables subscribers to send single or multiple (automated) traditional mail.

[www.vcsms.co.uk](http://www.vcsms.co.uk)

**Product - Medical Messenger**

This is a licensed software product that operates cooperatively with Patient Partner, the SMS Gateway and SmartMail to send a variety of SMS, email and traditional mail communications such as the following.

- Confirmations of appointments
- Reminders of appointments
- Prompts for tests and reviews
- Notifications of inoculation clinics

**Partnerships, Supply Chains, and Relationships with other Interested Parties**

Refer to the section on Interested Parties in this appendix for details relating to the following.

- Software Development Partners;
- Reseller Partners;
- Suppliers;
- Other parties.

**Impact of Disruptive Incidents**

Refer to our current Business Impact Analysis.

**Policies and Objectives**

The following policies all explicitly stipulate associated objectives.

- Quality Policy
- Information Security Policy
- Business Continuity Policy
Risk Management Strategy

(1) Appendix 4 specifies how we manage quality, information security and business continuity opportunities and risks.

(2) Appendix 5 specifies how we manage information security and business continuity risks, including risk criteria. The risk register contains identified threats and vulnerabilities.

Business Continuity Management - Risk Appetite and Purpose

<table>
<thead>
<tr>
<th>IMPORTANT</th>
<th>The following lists of facilities and data, grouped according to four different required recovery times, provide a guide to treatment of business continuity (and associated information security) risks and our required ability to recover from disruption.</th>
</tr>
</thead>
</table>

Following disruption, we can recover the following activities and functions, within the following times.

(1) 5 minutes:
  (a) ARC lone worker protection service;
  (b) On-Call Technical Support.

(2) 1 hour:
  (a) Main number telephone communication;
  (b) Access to our off-site hosted services (SMS Gateway, Hosted Voicemail and Payment Portal).

(3) 2 days:
  (a) Microsoft Exchange and Outlook;
  (b) Auto-attendant and voicemail;
  (c) Accounts;
  (d) Customer Service Database;
  (e) Normal hours (8am-6pm) technical support.

(4) 1 week:
  (a) Microsoft SharePoint;
  (b) Microsoft CRM;
  (c) Partial operation of telemarketing, sales, and provision of products and services.
Interested Parties – Their and Our, Needs and Expectations

The following sub-sections, each containing two tables, list interested parties, their interests, our interests with respect to them, and the aspects of operations (quality, information security and business continuity etcetera) that correspond to each of their and our interests.

Customers

<table>
<thead>
<tr>
<th>Their interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>We provide products, services and maintenance support that add value.</td>
<td>Quality</td>
</tr>
<tr>
<td>We provide products, services and maintenance support in accordance with contractual requirements.</td>
<td>Quality Information Security</td>
</tr>
<tr>
<td>We provide products, services and maintenance support in accordance with applicable legal requirements.</td>
<td>Quality</td>
</tr>
<tr>
<td>We can provide products, services and maintenance support at any time (24/7/365).</td>
<td>Quality</td>
</tr>
<tr>
<td>We continue to provide products, services and maintenance support in the event of any disruption.</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>We provide products, services and maintenance support in accordance with any additional, applicable industry, third party or end user requirements (e.g. NHS Digital, IGSoC approval).</td>
<td>Information Security Business Continuity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Our interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>We provide products and services that potential customers want to buy.</td>
<td>Quality</td>
</tr>
<tr>
<td>Our products and services add value, and meet or exceed customers' expectations, so that they continue to, use them and renew maintenance and/or licences.</td>
<td>Quality</td>
</tr>
<tr>
<td>We provide products and services, and maintain appropriate certifications and approvals, which enable us to successfully participate in tenders and framework agreements.</td>
<td>Quality Information Security Business Continuity</td>
</tr>
</tbody>
</table>
End Users

Our products and services interact with various groups of end users including, but not limited to, the following.

- Staff that work alone employed by customers that use our Alarm Receiving Centre (ARC) lone worker protection service.
- Staff that work alone employed by customers that possess a VC Lone Worker system.
- Patients registered at medical practices that possess one or more of Patient Partner, Repeat Prescriptions and Medical Messenger.
- Public and staff that utilise auto-attendant and voicemail systems.
- Police and other groups that utilise VC Relay systems.

<table>
<thead>
<tr>
<th>Their interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our products and services are reliable and simple (to use).</td>
<td>Quality</td>
</tr>
<tr>
<td>Products and services that we directly provide, and those that our customers provide (using our systems), are available when required.</td>
<td>Quality, Information Security</td>
</tr>
<tr>
<td>There is a simple and effective process to enable lone workers to specify accurate, complete and up-to-date personal details.</td>
<td>Quality, Information Security</td>
</tr>
<tr>
<td>Our products and services adequately protect personal data (contact details) and sensitive personal data (medical details).</td>
<td>Information Security</td>
</tr>
<tr>
<td>We can support our products and services at all times.</td>
<td>Quality</td>
</tr>
<tr>
<td>In the event of disruption, we can continue operation of products and services that we directly provide, and continue to provide support for those that customers provide (using our systems).</td>
<td>Business Continuity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Our interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Many end users utilise our products and services.</td>
<td>Quality</td>
</tr>
<tr>
<td>Customers of our ARC supply us with accurate, complete and up-to-date personal details of their lone workers.</td>
<td>Information Security</td>
</tr>
</tbody>
</table>
**Software Development Partners**

Our product Informer reads data from a scholastic information system as a result of a software development partnership with another software company.

Our product Patient Partner reads from, and writes data to, various medical information systems as a result of software development partnerships with other software companies.

<table>
<thead>
<tr>
<th>Their Interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>We provide any correct and complete technical information that they require, to enable them to amend, enhance, and rectify any faults in, their Application Programming Interface (API), in order to enable us to develop software that communicates and exchanges data with their API, in accordance with our requirements.</td>
<td>Quality Information Security</td>
</tr>
<tr>
<td>We develop software in accordance with any mutually agreed schedule.</td>
<td>Quality</td>
</tr>
<tr>
<td>We comply with any confidentiality and non-disclosure agreements.</td>
<td>Quality Information Security</td>
</tr>
<tr>
<td>Our relationship is not adversely affected by the departure or absence of any of our workers.</td>
<td>Business Continuity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Our interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Their software has an API with which our software can communicate and exchange data, in accordance with our requirements.</td>
<td>Quality</td>
</tr>
<tr>
<td>They develop any amendments, enhancements and corrections to, their API, in accordance with any mutually agreed schedule.</td>
<td>Quality</td>
</tr>
<tr>
<td>They comply with any confidentiality and non-disclosure agreements.</td>
<td>Quality Information Security</td>
</tr>
<tr>
<td>Our relationship is not adversely affected by the departure or absence of any of their workers.</td>
<td>Business Continuity</td>
</tr>
</tbody>
</table>
Reseller Partners

We have several partners that resell our products and services.

A number of these are telephone maintainers.

They may sell our products and services to their customers possibly in conjunction with their telephone products and services.

For example, a telephone maintainer may win a contract to supply a telephone system to a medical practice and at the same time sells our product Patient Partner, together with the telephone system, to the medical practice as a package.

Alternatively, a telephone maintainer may have supplied a telephone system to a medical practice in the past, is contracted to provide maintenance for it and subsequently sells Patient Partner to the medical practice.

We have a reciprocal reseller relationship with some of these telephone maintainers, so that we may also sell their products and services.

For example we may sell Patient Partner to a medical practice and at the same time purchase a new telephone system to replace an old one, possibly with additional telephone lines, to which we will connect the Patient Partner system.

Alternatively, we may sell to a medical practice an upgrade of a Patient Partner system from four ports (lines) to eight ports (lines), for which we require the telephone maintainer to install an extra four telephone lines.

<table>
<thead>
<tr>
<th>Their interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>We provide required training, to enable the reseller to sell our products and services.</td>
<td>Quality</td>
</tr>
<tr>
<td>We efficiently expedite orders.</td>
<td>Quality</td>
</tr>
<tr>
<td>We comply with any confidentiality and non-disclosure agreements.</td>
<td>Quality and Information Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Our interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>They appropriately sell our products and services.</td>
<td>Quality</td>
</tr>
<tr>
<td>They provide correct and complete, required information and documentation, to enable us to expedite orders.</td>
<td>Quality and Information Security</td>
</tr>
<tr>
<td>They comply with any confidentiality and non-disclosure agreements.</td>
<td>Quality and Information Security</td>
</tr>
</tbody>
</table>
**Suppliers**

The products and services that we procure include the following (which is not an exhaustive list).

- Telephony resource cards.

- Communications networks:
  - Landline telephone network(s), with multiple lines;
  - SIP telephone network(s), with multiple lines;
  - Mobile phone network(s);
  - Broadband link(s).

- Payment gateway.

- Hosted computer services.

- Other products and services including:
  - SMS Messaging;
  - Computer components;
  - Laptops;
  - Mobile phones;
  - Cars.

<table>
<thead>
<tr>
<th>Their interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>We purchase their products and/or services.</td>
<td>Quality</td>
</tr>
<tr>
<td>Where applicable, we subscribe to their technical support.</td>
<td>Quality</td>
</tr>
<tr>
<td>Where applicable, we provide complete and accurate information when we require their technical support.</td>
<td>Quality Information Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Our interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>They provide products and/or services that meet our requirements.</td>
<td>Quality</td>
</tr>
<tr>
<td>Where applicable, they supply stable and reliable (driver / interface) software to support the product or service, which is compatible with current server and client versions of Microsoft Windows that are under Microsoft mainstream or extended support.</td>
<td>Quality</td>
</tr>
<tr>
<td>Where applicable, they provide continuous, uninterrupted service.</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Where applicable, they provide responsive and effective technical support.</td>
<td>Quality Information Security</td>
</tr>
</tbody>
</table>
Workers (Employees and Contractors)

We currently have approximately 30 employees, in roles of management, software development, computer and telephony engineering, sales, telemarketing, account management, finance and administration. Also, we use two contractors that provide the following services.

Prompts  Professionally recorded voice prompts for the menu options and announcements of our voicemail, and other products and services based upon our messaging platform.

Office Cleaning  The offices are cleaned on Friday evening.

<table>
<thead>
<tr>
<th>Workers' Interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>The company is profitable and provides secure (employment and subcontract) work.</td>
<td>Quality Business Continuity</td>
</tr>
<tr>
<td>The company provides a safe and appropriate work environment.</td>
<td>Quality Occupational Health &amp; Safety</td>
</tr>
<tr>
<td>The company provides required training and support.</td>
<td>Quality</td>
</tr>
<tr>
<td>The company clearly specifies its requirements and expectations of workers.</td>
<td>Quality</td>
</tr>
<tr>
<td>Workers believe that they can positively contribute to the success of the company.</td>
<td>Quality</td>
</tr>
<tr>
<td>The company facilitates dialogue with workers so that they are aware of their contribution.</td>
<td>Quality</td>
</tr>
<tr>
<td>The company protects their personal information.</td>
<td>Information Security</td>
</tr>
<tr>
<td>The company pays fairly for work and as scheduled.</td>
<td>Quality Business Continuity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The Company's Interests</th>
<th>Aspects of Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workers fulfil their duties effectively and add value to the company.</td>
<td>Quality</td>
</tr>
<tr>
<td>Workers remain with the company (so that the company retains their knowledge and skills).</td>
<td>Quality</td>
</tr>
<tr>
<td>Workers can, and feel able to, suggest opportunities and improvements.</td>
<td>Quality</td>
</tr>
</tbody>
</table>
Lone Working

Over half of our staff at varying times work alone.

Sales and senior engineers routinely work away from the office.

Other engineers regularly, and other staff occasionally, work away from the office.

A few staff work in our Alarm Receiving Centre (ARC) providing lone worker protection, which operates permanently, around the clock, every day. Therefore they are alone in the building outside normal office hours.

| NOTE | All staff that work alone, in our ARC, and out of the office, use our ARC lone worker protection system. |

Regulators

We are not directly subject to any industry specific regulatory authority, but we are subject to various legal requirements from applicable legislation.
Applicability of ISO Management Standards

ISO international management standards are undergoing transition to align them all to a common structure. This is known as the High Level Structure (HLS). The following major management system standards are aligned to the HLS.

- **ISO 9001**: Quality Management
- **ISO 14001**: Environmental Management
- **ISO 22301**: Business Continuity Management
- **ISO 27001**: Information Security Management
- **ISO 37001**: Anti-Bribery Management
- **ISO 45001**: Occupational Health and Safety Management

We are currently certified to ISO 9001 and ISO 27001.

We have implemented substantial business continuity measures to support our hosted lone worker protection service. We may implement further business continuity measures in the foreseeable future to support other existing and planned services. Also a potentially catastrophic fire on 9 June 2014 at an adjacent site has highlighted the need to consider additional contingency measures. We intend to implement business continuity management and pursue certification to ISO 22301.
Appendix 3 – Processes

ISO management system standards aligned to the Annex SL High Level Structure (HLS), and ISO 9001 in particular, require you to describe the operations of your organisation as a sequence of processes, each of which transforms inputs into outputs, as illustrated in the following diagram.

A typical example of a process would be sales for which the:

- **Input** is **Appointments (with Potential and Existing Customers)**;
- **Process** is to **Sell**;
- **Output** is **Orders**.

ISO 9001 explicitly requires you to do the following.

1. Determine the processes that your organisation requires to manage quality of delivery of products and/or services.
2. Determine the sequence and interaction of the processes.
3. Determine the inputs that each process requires.
4. Determine the outputs expected from each process.
5. Determine the resources that each process requires and ensure that they are available.
6. Assign responsibilities and authorities for each process.
7. Address risks and opportunities associated with the processes.
8. Determine and apply the criteria and methods required to ensure the effective operation of each process. This includes monitoring, measurements and performance indicators.
9. Evaluate (the operation of) the processes and implement any changes required to ensure that they achieve their intended results.
10. Improve (the operation of) the processes.
11. Maintain documented information required for the operation of the processes.
12. Retain documented information required to show that the processes operate as planned.
Sequence and Interaction of Processes

Develop Software
Products and Services

Market

Sell

Fulfil Orders

Manage Accounts
Support

Purchase
Invoice
# Processes

<table>
<thead>
<tr>
<th>Process (verb) and component procedures</th>
<th>Inputs (nouns)</th>
<th>Outputs (nouns)</th>
<th>Resources (nouns)</th>
<th>Evaluation [Measurement or Monitoring (method)]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop Software Products and Services</td>
<td>Requests and requirements for changes and additions to existing products and services. Requests and ideas for new products and services.</td>
<td>Changes and additions to existing products and services. New products and services.</td>
<td>Staff. ICT equipment. Development software. Test environment. Authoring software.</td>
<td>Progress against schedule.</td>
</tr>
<tr>
<td>JF-1 JF-17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JF-2 JF-3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sell</td>
<td>Appointments.</td>
<td>Orders.</td>
<td>Staff. ICT equipment. Office software. Vehicles.</td>
<td>Sales of: Products; Software licences; Subscription services; SMS Credits.</td>
</tr>
<tr>
<td>JF-4 JF-6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JF-7 JF-9 JF-10 JF-11 JF-12 JF-19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process (verb) and component procedures</td>
<td>Inputs (nouns)</td>
<td>Outputs (nouns)</td>
<td>Resources (nouns)</td>
<td>Evaluation [Measurement or Monitoring (method)]</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Purchase JF-8</td>
<td>Requirements for goods and services.</td>
<td>Procured goods and services.</td>
<td>Staff. ICT equipment. Office software. Accounts software.</td>
<td>Approved suppliers (assessment and monitoring).</td>
</tr>
<tr>
<td>Invoice No procedure</td>
<td>Fulfilled orders.</td>
<td>Received payments.</td>
<td>Staff. ICT equipment. Office software. Accounts software.</td>
<td>Debtors List</td>
</tr>
<tr>
<td>Manage Accounts JF-5 JF-12</td>
<td>Fulfilled orders.</td>
<td>Renewals of maintenance and subscription service contracts. Sales of changes to configurations Sales of additional products, software licences, subscription services and SMS credits. Cancellations of contracts and licences.</td>
<td>Staff. ICT equipment. Office software. Vehicles.</td>
<td>Maintenance revenue Lost Customers</td>
</tr>
<tr>
<td>Support JF-13 JF-14 JF-15 JF-16 JF-18</td>
<td>Requests from customers. Requests from Account Managers. Requests from our staff.</td>
<td>Resolutions of problems encountered by customers. Changes to installed hardware and/or software. Resolutions of problems encountered by our staff.</td>
<td>Staff. ICT equipment. Office software. Vehicles. Component hardware and software. Build area.</td>
<td>Number of Active Support Jobs (ASJs) Number of ASJs as percentage of total number of customers Average time to answer a support call</td>
</tr>
</tbody>
</table>

**NOTE** In the above table, each Procedure specifies the Job Descriptions to which it applies and each Job Description specifies the Procedures that apply to it.
Appendix 4 – Guide to Opportunities and Risks

Annex SL

ISO is imposing a common structure on its management standards known as the High Level Structure (HLS) defined in Annex SL (an annex in an ISO specification document for management standards). This now applies to several management standards including the following major standards.

- ISO 9001 Quality Management System (QMS)
- ISO 14001 Environmental Management System (EMS)
- ISO 22301 Business Continuity Management System (BCMS)
- ISO/IEC 27001 Information Security Management System (ISMS)
- ISO 37001 Anti-Bribery Management System (ABMS)
- ISO 45001 Occupational Health and Safety Management System (OHSMS)

The alignment of ISO management standards to Annex SL includes requirements to consider risks but these differ between standards. ISO 27001 requires formal risk management that links to a set of controls specified in its Annex A. ISO 9001 requires a much simpler arrangement.

Annex SL introduces other new components.

Section 4 requires you to identify the context of your organisation and interested parties, with respect to the management system and determine its scope. These will be different, for example, for a Quality Management System (QMS) and an Environmental Management System (EMS), but if you operate an Integrated Management System (IMS) you include everything relevant to the aspects of your operations that your IMS manages.

Sub-Section 6.1 requires an organisation to consider risks and opportunities that arise from Section 4.

Opportunities and Risks - Are Separate

One problem that arises from the introduction to ISO management standards, of consideration of risks and opportunities, is confusion caused by the definition of risk. The standards define risk and state that it can be positive as well as negative. This concept is also known and referred to as upside risk and downside risk. This conflicts with the common understanding that risk is a negative phenomenon. Also, the standards do not define opportunity. This has had the unfortunate consequence that some guidance on how to address risks and opportunities erroneously equates opportunity to positive risk.

The concept of positive risk exists because in some situations it is appropriate to evaluate the possibility of associated positive and negative outcomes in a consistent manner. A typical example is a financial investment, where it is appropriate to evaluate, in a consistent manner, the probabilities that an investor will make or lose money. The term positive risk may seem counterintuitive and a contradiction in terms but it arises from a mathematical need. One way to accommodate the concept is to use the word outcome instead of risk, with the understanding that the possibility of a negative outcome is what is commonly understood as a risk.

You can analyse opportunities more easily, if you utilise the concept of the possibility of a positive outcome (positive risk), and consider it as separate from, and different to, an opportunity.

(1) A (negative) risk is the possibility of a negative outcome.
A positive risk is the possibility of a positive outcome.
(2) A (negative) risk (possibility of a negative outcome) or positive risk (possibility of a positive outcome) is something to which you are subject, without choice.

You may be subject to a risk as a consequence of a choice that you made.

(3) An opportunity is something that you can choose to pursue.

(4) An opportunity has an associated possibility of at least one positive outcome.

(5) An opportunity may have associated possibilities of both positive outcomes and negative outcomes (risks).

(6) After you choose to pursue an opportunity, you are then subject to its associated possibilities of negative outcomes (risks) and positive outcomes.

(7) You may have to take or increase (negative) risks to pursue an opportunity.

(8) An opportunity may be something that you can pursue, to mitigate a (negative) risk.

(9) If you choose to pursue an opportunity, you must review your assessments of possibilities of positive and negative outcomes (risks), and opportunities, to determine:

(a) Additional possibilities of positive and negative outcomes (risks), which arise because you now pursue the opportunity;

(b) Additional opportunities that arise because you now pursue the opportunity.

For example, the sale of lottery tickets provides an opportunity, to buy a lottery ticket. If you choose to buy a lottery ticket, you pursue an opportunity. This opportunity has an associated possibility of a positive outcome and an associated possibility of a negative outcome (risk).

The possibility of a positive outcome is that you win the lottery. This has a very low likelihood.

The possibility of a negative outcome (risk) is that you lose your stake, i.e. the ticket price. This has a very high likelihood.

A (negative) risk usually consists of a threat and a vulnerability (a weakness that makes you susceptible to the threat). To assess the risk you must evaluate the threat and the vulnerability. To assess the possibility of a positive outcome, you must evaluate the nature of its positive influence and the extent to which it would affect the subject. The impacts of the above example are as follows.

Low Wage Worker  
The possibility of a positive outcome would have a very high impact.  
The possibility of a negative outcome (risk) would have a low impact.

Professional  
The possibility of a positive outcome would have a high impact.  
The possibility of a negative outcome (risk) would have a very low impact.

Head of Multinational  
The possibility of a positive outcome would have a medium (or low) impact.  
The possibility of a negative outcome (risk) would have a very low impact.

How to Address Opportunities and Risks

Section 6.1 Actions to address risks and opportunities of an ISO management standard aligned to Annex SL requires an organisation to consider risks and opportunities that arise from Section 4 of the ISO management standard. An opportunity may have associated risks (of both pursuing it and not pursuing it) so it is more convenient to itemise opportunities first and then risks.
Simple Opportunity Assessment

The following table provides a simple method to assess and manage opportunities.

<table>
<thead>
<tr>
<th>Opportunity</th>
<th>Associated Risks</th>
<th>Decision</th>
<th>Outcome</th>
<th>Who</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>What we could Choose to Pursue and What would be the Advantages.</td>
<td>Risks of Pursuing Opportunity and / or Risks of Not Pursuing it.</td>
<td>Pursue Defer Ignore</td>
<td>Actions to Pursue Opportunity or Reasons Not to Pursue it.</td>
<td>Persons that do actions</td>
<td>Date actions begun</td>
<td>Date actions done</td>
</tr>
</tbody>
</table>

Simple Risk Assessment

The following table provides a simple method to assess and manage risks.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Vulnerability</th>
<th>Current Counter-measures</th>
<th>Risk Treatment</th>
<th>Who</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>(What you cannot change.) What can happen and its consequences.</td>
<td>(Elements under your control.) Weaknesses that make you susceptible to the Threat.</td>
<td>Existing arrangements or components that mitigate or eliminate the Vulnerability.</td>
<td>Type (Accept, Control, Avoid, Transfer) and Details of actions.</td>
<td>Persons that do actions</td>
<td>Date actions begun</td>
<td>Date actions done</td>
</tr>
</tbody>
</table>

NOTE  
This method complies with the requirements of ISO 9001 and ISO 14001.

It does NOT comply with the risk assessment requirements of ISO 22301 – Business Continuity, ISO 27001 – Information Security or ISO 37001 – Anti-Bribery.

IMPORTANT  
For ISO 22301, ISO 27001 or ISO 37001 (or any other management system standard that requires formal risk management) you can use this simple risk assessment table to list actual and potential risks as part of your identification of both opportunities and risks. When you have determined which opportunities you will pursue and therefore, which risks you will actually be subject to, you must manage the risks in accordance with the requirements of ISO 22301, ISO 27001 or ISO 37001 (etcetera): i.e. you must then add the (actual) risks to your risk register to manage them appropriately.
Appendix 5 – How to Maintain a Risk Register

Management of (negative) risks is fundamentally a simple process that consists of identifying something that can happen, what its consequences are, what your vulnerability is to it, what you already do, and what else you can do, to prevent or mitigate it.

People to Involve in Risk Assessment and Management

The correct people to involve in risk assessment and management are people with a good knowledge and understanding of the product, service, system or organisation, for which you must identify, assess and treat the risks. The most important aspect of risk management is risk identification. You can only assess and treat risks that you identify. Risk assessment and management is essentially a simple process that you and your colleagues can and should do yourselves, without outside help.

Risk Priority is Treatment Priority, not Risk Seriousness

If you must manage a substantial number of risks, it is advantageous to use a method in which you quantify the Consequence and estimate the Likelihood of each risk, from which you calculate a Risk Priority, to rank the risks. The most common method requires you to assign a value of 1 (Low), 2 (Medium) or 3 (High) to the Consequence and Likelihood, from which you calculate a Risk Priority using the following formula.

\[
\text{Risk Priority} = \text{Consequence} \times \text{Likelihood}
\]

Alternatively, you can use the formula below, which assigns greater weight to the Consequence. This may be more suitable for Health and Safety risks, to ensure that you assess and appropriately treat risks in order of severity of injury or illness. The formula is also more suitable if it is difficult to reliably estimate the likelihood, which is frequently the case.

\[
\text{Risk Priority} = (10 \times \text{Consequence}) + \text{Likelihood}
\]

The most important aspects of risk management are risk identification and risk treatment. If you identify 67 risks you must decide how to treat all 67 of the risks, irrespective of the order in which you list them, and even if the treatment for several is simply to accept the risk.

(1) The Risk Priority is not a measure of the seriousness of a risk. It is not expressed in any units and is based on the Consequence and Likelihood, which may only be rough estimates.

(2) The Risk Priority is a number that ranks risks, to assist you to assess and manage them. The Risk Priority puts risks in an appropriate order of priority, so that when you have a meeting to decide how to treat the risks, you have them in a list with the highest priority at the top and lowest priority at the bottom.

NOTES

(A) Only categorise Consequence and Likelihood on a scale of 1 to 3. If you categorise them on a scale of 1 to 5 or 1 to 10 it has little effect on the order and no effect on the treatment, so it is a waste of time.

(B) You should review the risks as you apply treatments, so the order in which you rank them will change.

(C) It is more productive and effective to use your time and devote your thinking, to identify the risks and decide how to treat them (than how to rank them).
Standard Risk Assessment

This describes how to do risk assessments, which satisfy the requirements of the following:

- ISO 27001 – Information Security Management;

Risk Methodology

A variety of risk scenarios are identified and linked to specific assets. In each case the threats and vulnerabilities are identified and linked to an appropriate assessment of the consequences of the risk.

**NOTE**

For information security risk assessments, the assessment of the consequences of the risk is based on identification of whether confidentiality, integrity, or availability would be compromised in the scenario.

Consequence and Likelihood Grading

The **Consequence** and **Likelihood** of every risk are each assigned a value of 1 to 3, and multiplied together to give a **Risk Priority** from 1 to 9. This represents the current residual risk within the IMS.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Information Security</th>
<th>Business Continuity</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 High</td>
<td>Public exposure of confidential or personal, sensitive information leading to significant embarrassment for the company, or its customers.</td>
<td>Severe and/or long term disruption. For example: fire or structural damage to building; severe weather for a long period; serious epidemic.</td>
</tr>
<tr>
<td>2 Medium</td>
<td>Exposure of confidential or personal sensitive information to a non-authorised third-party, system downtime or data corruption, with undesirable consequences upon operations and with potential consequences upon customer(s).</td>
<td>Temporary, substantial disruption. For example: a loss of electrical power, for several hours; severe weather for a short period, minor epidemic.</td>
</tr>
<tr>
<td>1 Low</td>
<td>Internal exposure of internally restricted information beyond authorised individuals, system downtime or data corruption, with only minor disruption to operations.</td>
<td>Temporary, minor disruption. For example: a loss of electrical power, which resumes before our UPSs (Uninterruptible Power Supplies) cease to provide emergency power to our phone system and principal servers.</td>
</tr>
</tbody>
</table>
### Likelihood

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Likely to happen within the next 2 months</td>
<td>Likely to happen within the next 12 months</td>
<td>Unlikely to happen within the next 12 months</td>
</tr>
</tbody>
</table>

### Risk Treatment Criteria

The following table gives a recommended risk treatment plan that specifies who has the authority to accept risks at varying levels.

### Risk Treatment

<table>
<thead>
<tr>
<th>Risk Priority</th>
<th>Risk Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>$6 \text{ or } 9$ High</td>
<td>Director reduces or accepts risk.</td>
</tr>
<tr>
<td>$3 \text{ or } 4$ Medium</td>
<td>Management Review Meeting reduces or accepts risk.</td>
</tr>
<tr>
<td>$1 \text{ or } 2$ Low</td>
<td>Acceptable – Review annually.</td>
</tr>
</tbody>
</table>

### Documentation

The risk assessments are documented in a table with the following columns.

1. Date Logged
2. Process
3. Asset
   - The asset, such as the following examples.
     - IT Infrastructure
     - Sage Payroll data
     - Personnel (paper) files
     - Cisco certified staff
4. Type (of the Asset)
   - One or more of the following five categories.
     - Information
     - Hardware
     - Software
     - Services
     - People
(5) **Risk Owner**

The person or entity with the accountability and authority to manage the **Risk**.

(6) **Threat (what you cannot change)**

A description of what may happen to the **Asset** (such as loss, corruption, damage, attack), how it may happen and the possible consequences.

(7) **Property (of the information Asset)**

One or more of the following three aspects of the information **Asset** that the **Threat** could influence.

- Confidentiality
- Integrity
- Availability

Refer to the Terms and definitions in the following.

ISO 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary

<table>
<thead>
<tr>
<th>NOTE</th>
<th>This column applies to an information security risk assessment.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>It does NOT apply to a business continuity risk assessment.</td>
</tr>
</tbody>
</table>

(8) **Consequence (1 to 3)**

A number, ONE, TWO or THREE, that represents the severity of the effect that the **Threat** could have on the **Asset**.

Refer to the **Consequence** table above.

(9) **Vulnerability (elements under your control)**

A description of one or more weakness(es) that make the **Asset** susceptible to the **Threat**.

(10) **Current Countermeasure(s)**

Any organisational arrangement(s) and / or component(s) of infrastructure that mitigate or negate the **Vulnerability**.

(11) **ISO 27001, Annex A, Reference(s)**

Any controls that correspond to the **Existing Countermeasure(s)**.

<table>
<thead>
<tr>
<th>NOTE</th>
<th>This column applies to an information security risk assessment.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>It does NOT apply to a business continuity risk assessment.</td>
</tr>
</tbody>
</table>

(12) **Likelihood (1 to 3)**

A number ONE, TWO or THREE that represents the likelihood that the **Threat** will occur.

Refer to the **Likelihood** table above.
(13) **Risk Priority (= Consequence x Likelihood)**

Multiply the **Consequence** and **Likelihood** together to give the **Risk Priority** that represents the current residual risk within the ISMS.

Refer to the **Risk Treatment** table above.

(14) **Risk Treatment Plan**

A description of the planned treatment(s), in response to the **Risk Priority**, based on the **Risk Treatment Criteria**.

Refer to the **Risk Treatment** table above.

(15) **Treatment Type**

One or more of the following four categories of treatment that comprise the **Risk Treatment Plan**.

- Accept
- Control
- Avoid
- Transfer

(16) **Treatment Owner**

The person or entity that is responsible for the implementation of the **Risk Treatment Plan**.

(17) **Review Date**

The planned date of review of the implementation of the **Risk Treatment Plan**.

(18) **Desired Risk Priority (1 to 3)**

A number ONE, TWO or THREE that is an estimate of the likely long-term residual risk following the planned treatment(s).
Health and Safety

This describes a modification to the risk methodology described in the previous pages, to assess risks to health and safety. The formula \( \text{Risk Priority} = \text{Consequence} \times \text{Likelihood} \) is appropriate for the management of information security and business continuity risks. This modification uses the following formula that assigns a higher Risk Priority to deaths and serious injuries than minor injuries, which is appropriate for the management of health and safety risks. You may also choose to use this formula for other types of risk assessment if it is difficult to reliably estimate the likelihood.

\[
\text{Risk Priority} = (10 \times \text{Consequence}) + \text{Likelihood}
\]

**NOTE** The Risk Priority that this formula assigns is a two-digit number with the Consequence as the first digit and the Likelihood as the second digit.

**NOTE** Use appropriate descriptions of consequences. Those listed below are suggestions.

### Consequence

<table>
<thead>
<tr>
<th>3</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Death; Permanent disablement; Loss of a limb, eye, sight, hearing; Serious or critical injury with permanent after effects.</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Serious recoverable injury with no or superficial permanent after effects.</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
</tr>
<tr>
<td>1</td>
<td>Minor injury.</td>
</tr>
</tbody>
</table>

**NOTE** Use appropriate periods (that make it simple) to estimate likelihood. The three combinations of periods (1 & 10 or 2 & 15 or 5 & 25 years) shown in the following table are suggestions.

### Likelihood

<table>
<thead>
<tr>
<th>3</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Likely to happen within the 1 (or 2 or 5) year(s).</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>2</td>
<td>Likely to happen within the next 10 (or 15 or 25) years.</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
</tr>
<tr>
<td>1</td>
<td>Unlikely to happen within the next 10 (or 15 or 25) years.</td>
</tr>
</tbody>
</table>

**NOTE** Group the Risk Priority numbers appropriately. The groupings shown below are suggestions.

### Risk Treatment

<table>
<thead>
<tr>
<th>Risk Priority = (10 x Consequence) + Likelihood</th>
<th>Risk Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>22, 23, 31, 32 or 33 High</td>
<td>Director reduces or accepts risk.</td>
</tr>
<tr>
<td>12, 13 or 21 Medium</td>
<td>Management Meeting reduces or accepts risk.</td>
</tr>
<tr>
<td>1 Low</td>
<td>Acceptable – Review annually.</td>
</tr>
</tbody>
</table>
Appendix 6 – Maintain a Business Impact Analysis

This specifies how to compile and maintain a business impact analysis. It restates requirements from ISO 22301 but specifies additional details, including the following:

- Periods of disruption of activities;
- Levels of resumption of activities;
- Things that activities depend upon.

Activities

Identify the following:

- Activities that support the provision of products and/or services;
- Any other activities that you wish to include in this analysis.

**NOTE** Categorise the Activities according to Processes.

Disruption

Assess the impacts of not performing the identified activities for the following periods;

- Five minutes;
- One Hour;
- Half a day;
- One day;
- Three days;
- One week;
- One month;
- Three months.

Identify the period, after which it would become unacceptable to not perform each activity.

Resumption

Specify intervals, after which, it would be imperative to resume each activity, to contribute towards, or to achieve, production of products and/or services, at the following levels:

- Minimal - very incomplete and/or very infrequent;
- Partial - incomplete and/or infrequent;
- Normal - complete and uninterrupted.

Dependencies

Identify any of the following that must be present and/or functional for each activity:

- Other activities;
- Resources (people, equipment, money etcetera);
- Utility services (water, sanitation, electricity, telephony, broadband etcetera);
- Other providers (suppliers and partners etcetera);
- Customers' facilities (communication links etcetera).
Abbreviations

BCMS  Business Continuity Management System

The part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

NOTE The management system includes organizational structure, policies, planning activities, responsibilities, procedures, processes and resources.

MTPD  Maximum Tolerable Period of Disruption

The time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.

MBCO  Minimum Business Continuity Objective

The minimum level of services and/or products that is acceptable to the organization to achieve its business objectives during a disruption.

RTO  Recovery Time Objective

The period of time following an incident within which:

- product or service must be resumed, or;
- activity must be resumed, or;
- resources must be recovered.

NOTE For products, services and activities, the recovery time objective must be less than the time it would take for the adverse impacts that would arise as a result of not providing a product/service or performing an activity to become unacceptable.

RPO  Recovery Point Objective

The point to which information used by an activity must be restored to enable the activity to operate on resumption.

NOTE Can also be referred to as “Maximum Data Loss”. 

Appendix 7 – Information Security Guide
Part 1 – Overview

Introduction

We currently operate an Integrated Management System (IMS) that manages quality and information security certified to ISO 9001 and ISO 27001, with additional components that satisfy requirements of the NHS Data Security and Protection Toolkit.

What – is Information Security Management?

There are three, equally important, aspects, which management of information security must control:

- **Integrity**: Ensuring that data is complete and accurate;
- **Availability**: Ensuring that data is available to people that require access to it;
- **Confidentiality**: Ensuring that data is NOT available to people that do not require access to it.

When discussing *Information Security* most people immediately think of confidentiality, i.e. making sure that there is no unauthorised disclosure of data, as has happened in many high profile breaches.

> *Information Security Management must effectively control all three aspects. All three aspects are equally important.*

The following acronym summarises the three aspects that Information Security Management controls.

**CIA – Confidentiality, Integrity, Availability**

Why – implement Information Security Management

We implement Information Security Management for the following reasons.

1. Our entire business is based on information.
2. Many of our customers must operate stringent information security.
3. We must ensure that our arrangements for secure remote working are effective.
4. We must ensure that our arrangements for business continuity are effective.
5. We must comply with legal requirements, such as data protection law (see Guide 3).
6. We must satisfy the NHS Data Security and Protection Toolkit requirements, to maintain access to NHS digital services, including the NHS (broadband) wide area network.
7. Organisations increasingly require that suppliers are certified to ISO 27001, either in general, for provision of ICT services, or for specific contracts and/or framework agreements.
   
   It is conceivable that part or all of the NHS might make this a universal requirement.
8. We compete with companies that are certified to ISO 27001, as well as ISO 9001.
Incidents – Actual or Potential and How to Report Them

An important part of management of information security is that any actual or potential incident (threat to security of information) is identified, reported, recorded and, where possible, mitigated.

**IMPORTANT**

A threat to any of the three aspects, **Integrity**, **Availability** and **Confidentiality**, of security of information or an information asset, is an incident.

A violation of a relevant legal requirement (such as data protection law) or contractual requirement (such as a non-disclosure clause) is also an incident.

The following are some typical examples of actual or potential incidents.

**Integrity**

Changes of details of contact information of a customer, received by the Helpdesk and recorded in the Customer Service Database, are not communicated to (a) the Account Manager and recorded in CRM, and (b) Accounts and recorded in Sage.

**Availability**

The CRM server fails, so that CRM is unavailable.

**Confidentiality**

Contact details of a patient, relating to a Patient Partner support call, are emailed by an engineer to Toni Mason instead of Tony Bicker.

_This would also constitute a violation of data protection law._

**Legal Requirement**

Contact details of a patient, relating to a Patient Partner support call, are included in the details of the support call recorded in the Customer Service Database.

_The Customer Service Database does not enable you to delete these contact details when the support call has been resolved and closed. The details could also be viewed by anyone looking at the recorded details of the support call. This would violate data protection law, because it would not be necessary for anyone else to view that personal information._

**Contractual Requirement**

An employee discloses to a customer, details of licence payments for access to a medical practice database, in contravention of a non-disclosure agreement.

_This does not involve any personal data._

_This would also constitute a violation of Confidentiality._

**IMPORTANT**

If you become aware of any actual or potential incident, in which there is a threat to security of information, report it to any of the following people. If you are not sure whether a situation is an actual or potential incident, report it anyway.

IMS Manager  
Line Manager  
Director

**How – Classification, Labelling and Handling**

Refer to Procedure IS-6. If you require any clarification of this, please contact the IMS Manager.
Appendix 8 – Information Security Guide
Part 2 – Legislation

Introduction

This document provides an overview of relevant legislation and how it applies to our operations. It also contains the most important parts of data protection law. You should refer to this and be aware of its provisions if you need to process personal data and especially if you must access a medical practice or scholastic database.

Legislation

The principal, but not only, pieces of legislation that apply to the issue of Information Security are the following. These are all available for download from either of the following European Union (EU) or United Kingdom (UK) Government legislation websites as appropriate.

http://eur-lex.europa.eu
http://www.opsi.gov.uk.

General Data Protection Regulation (GDPR) and Data Protection Act 2018

(1) The GDPR is European Union (EU) Regulation 2016/679.


All staff should be aware of the following:

- Chapter 1 - General Principles (Articles 1 to 4);
- Chapter 2 - Principles (Articles 5 to 11);
- Chapter 3 - Rights of the Data Subject (Articles 12 to 23).

All staff should be aware of the CONTENTS of the following:

- Chapter 2 - Principles (Articles 5 to 11).
- Article 5 - Principles relating to processing of personal data
- Article 6 - Lawfulness of processing
- Article 7 - Conditions for consent
- Article 8 - Conditions applicable to child's consent in relation to information society services
- Article 9 - Processing of special categories of personal data
- Article 10 - Processing of personal data relating to criminal convictions and offences
- Article 11 - Processing which does not require identification

(2) The United Kingdom (UK) Data Protection Act 2018 implements qualifications to the GDPR and also European Union (EU) Directive 2016/680, which governs processing of personal data for purposes of law enforcement.


The EU provides the following free handbook on European data protection law.

The practical restriction that data protection imposes is that if you require access, for example, to a medical practice or scholastic database, you must, if possible, use a login that provides access to contact information but forbids access to medical or educational details etc. The following procedures contain instructions that cover this requirement.

IMS Procedure JF-7 – Project Management
IMS Procedure JF-11 – Installation
IMS Procedure JF-13 – Help Desk Support
IMS Procedure JF-14 – Remote Service and Maintenance
IMS Procedure JF-15 – On-Site Service and Maintenance

Privacy and Electronic Communications (EC Directive) Regulations 2003

These regulations essentially augment the Data Protection Act, and cover electronic communications including telephone calls, SMS text messages and emails. They address issues such as marketing etc.

Freedom of Information Act 2000

An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and for connected purposes.

This act is closely associated with data protection law. However, it principally applies to disclosure of information held by public authorities.

Computer Misuse Act 1990

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

This legislation makes it an offence to access a computer system or data without the owner’s authorisation. For example, if you use remote access software to access someone’s computer system, and they don’t want you to do so, you contravene this law.

Copyright, Designs and Patents Act 1988

An Act to restate the law of copyright, with amendments; to make fresh provision as to the rights of performers and others in performances; to confer a design right in original designs; to amend the Registered Designs Act 1949; to make provision with respect to patent agents and trade mark agents; to confer patents and designs jurisdiction on certain county courts; to amend the law of patents; to make provision with respect to devices designed to circumvent copy-protection of works in electronic form; to make fresh provision penalising the fraudulent reception of transmissions; to make the fraudulent application or use of a trade mark an offence; to make provision for the benefit of the Hospital for Sick Children, Great Ormond Street, London; to enable financial assistance to be given to certain international bodies; and for connected purposes.

This act is not primarily concerned with information security. However, any instance of copying or installation of software that is not legally owned constitutes a breach of this act, which is basically considered as theft. An information security audit could uncover occurrences of this, if present.
Appendix 9 – Information Security Guide
Part 3 – Encryption

Introduction

There are various methods to encrypt documents and data.

(1) Use Microsoft Windows Encrypting Filing System (EFS) to encrypt the contents of a folder (directory) or a file.

This method of encryption does not require you to remember a password, because the encryption relates to your network login.

Use this to encrypt documents on your computer and on the network, such as in your UserFolder.

(2) Use Microsoft Windows BitLocker to encrypt a USB storage device, if you must do either of the following.

(a) Backup VC-Confidential files on a Windows computer or device;
(b) Transfer VC-Confidential files between two or more Windows computers or devices.

(3) Password protect a Microsoft Office document, through the Save As option.

Installable versions of Microsoft Office are available for Windows and Mac. Office 365 is a suite of web applications available to all operating environments.

(4) Use an encryption utility, such as the open source application AESCrypt, which encrypts individual files, and is available for Windows (XP, Vista, 7, 8), Apple (Mac OSX, iPad/iPhone iOS), Linux and Android, if you must do either of the following:

(a) Transfer VC-Confidential files between devices running different operating environments;
(b) Send VC-Confidential files(s) as attachments to emails.

Alternatively, use an archive utility, such as the commercial utility WinZip (Windows and Mac), or open source utility PeaZip, (Windows and Linux), which provides encryption through password protection.
Microsoft Windows – Encrypting Filing System (EFS)

To set a folder (directory) to use the Encrypting Filing System (EFS), do the following procedure.

**NOTE** The encryption is specific to the log in profile you use to encrypt the folder. Another user, logging in with a different user name will NOT be able to access the encrypted files. All encryption must be accessible to at least two people. Before you use this facility, speak to the Network Manager, to ensure that he has a domain recovery agent, to be able to access the encrypted files.

1. Right click on the folder. (This example use the folder TEMP.)

   Windows displays a menu similar to the following.

   ![Menu](image)

2. Select the option *Properties*.
(3) Windows displays a **Properties** window for the selected folder, similar to the following.

(4) Click the **Advanced** button.

(5) Windows displays the **Advanced Attributes** window, similar to the following.
(6) Click the **Encrypt contents to secure data** check box, to select it, so that it contains a tick.

(7) Click the **OK** button.

(8) Windows sets the **Properties** window for the selected folder as the currently active window.

(9) Click the **OK** button.
Windows displays the name and details of the encrypted folder **TEMP** in **green**.
IMPORTANT

(1) Windows encrypts (i.e. applies EFS encryption to) any file that you create in, move into, or copy into, the encrypted directory.

(2) If you move or copy a file from this encrypted directory to another directory on a NTFS drive on your computer, the file remains encrypted.

(3) If you move or copy a file from this encrypted directory to another directory on a NTFS drive on the network, the file remains encrypted, provided the correct attributes are set on the network drive.

If the correct attributes are not set, you will not be able to move or copy the file.

(4) If you try to move or copy a file from this encrypted directory to another directory on a FAT, FAT32 or exFAT drive, Windows informs you that the destination does not support encryption and prompts you to confirm the operation.

If you agree and continue with the operation, Windows decrypts (i.e. removes EFS encryption from) the file and moves or copies it.

(5) You can use this method to encrypt a (single) file but Windows asks you if you want to encrypt the folder that contains the file.

If you encrypt the folder and subsequently edit the file, then any ancillary or temporary work files etcetera will be encrypted.

If you only encrypt the file, any ancillary or temporary work files will not be encrypted.

---

Microsoft Windows – BitLocker Encryption

Windows BitLocker encryption enables you to encrypt (all folders and files on) a USB storage device formatted as FAT, FAT32, exFAT or NTFS. Windows 7 Enterprise, Windows 7 Ultimate and all editions of Windows 8 provide full BitLocker capability. Windows 7 Professional does not enable you to set up BitLocker encryption on a USB storage device, but it does enable you to access and utilise a USB storage device that has BitLocker encryption set up on it.

IMPORTANT

Use a USB storage device formatted as FAT32 or exFAT.

If you attempt to copy a file encrypted by EFS from your computer to the USB storage device, this forces Windows to remove the EFS encryption as you copy or move the file from your computer to the USB storage device.

This ensures that you can transfer it to the destination.

WARNING

Do NOT use a USB storage device formatted as NTFS.

If you use a USB storage device formatted as NTFS you could copy or move a file already encrypted by EFS to the USB storage device.

You may then be unable to copy or move the file from the USB storage device to the destination.
Set Up BitLocker encryption on a USB storage device

To set up BitLocker encryption on a USB storage device, do the following procedure.

(1) Attach the USB storage device.
(2) Right click on the USB storage device and select the popup menu option **Turn on BitLocker**.
(3) Windows initially displays the following view.

![Screenshot of BitLocker Drive Encryption](image1.png)

(4) Windows then displays the following prompt.

![Screenshot of BitLocker Drive Encryption](image2.png)
(5) Click in the **Use a password to unlock the drive** check box, so that it contains a tick.

(6) Key in the password twice and click the **Next** button.
Windows BitLocker displays the following Recovery Key view.

---

IMPORTANT

You only require the recovery key if it is possible that you may forget or lose the password. If you do require the recovery key, you must manage this securely under the same arrangements as for passwords.

The following is an example of a BitLocker recovery key. It is a text file with a file name and contents similar to the following.

**BitLocker Recovery Key F05BBAB0-1DBB-4EA2-BEC8-1F0CF60823B0.txt**

*BitLocker Drive Encryption Recovery Key*

The recovery key is used to recover the data on a BitLocker protected drive.

To verify that this is the correct recovery key compare the identification with what is presented on the recovery screen.

*Recovery key identification: F05BBAB0-1DBB-4E*

*Full recovery key identification: F05BBAB0-1DBB-4EA2-BEC8-1F0CF60823B0*

*BitLocker Recovery Key:*

250382-294580-074679-170511-488070-315876-646173-624767

Click the **Cancel** button [and continue from Step (8)] or do the following if you require the recovery key.
(a) Select one (or both) of the recovery key options. If you select **Save the recovery key to a file**, Windows displays the following view.

![Save BitLocker Recovery Key as](image)

(b) After you save and/or print the recovery key, click the **Next** button.

![BitLocker Drive Encryption](image)
(8) Click the **Start Encrypting** button.

(9) Windows encrypts the USB storage device.
Access a USB storage device encrypted by BitLocker

To access a USB storage device that is encrypted by BitLocker, do the following procedure.

(1) Attach the USB storage device. Windows Explorer shows it with the BitLocker Icon (Drive I).
(2) Windows displays the following prompt.

![Image of BitLocker Drive Encryption dialog box]

(3) Key in the password and click the **Unlock** button.
(4) Windows unlocks the USB storage device.
Manage BitLocker

You can manage the BitLocker attributes of the USB storage device, as follows.

1. Right click on the USB storage device and select the popup menu option **Manage BitLocker**.
(2) Windows displays the following menu.

![BitLocker Drive Encryption menu](image)

**Select options to manage**

- Change password to unlock the drive
- Remove password from this drive
- Add a smart card to unlock the drive
- Save or print recovery key again
- Automatically unlock this drive on this computer

[Close button]
Appendix 10 – Information Security Guide
Part 4 – Guidance and Good Practice

Passwords and Passphrases

(1) DO change any initial (default) password assigned to you, such as a network or local computer (administrator) password.

(2) DO NOT create an unnecessarily simple Password.
   For example, DO NOT create a password such as Jklmn0pqr.

(3) DO NOT create a password that someone else may be able to guess.
   For example, if Anastasia is the name of your cat, DO NOT create the password Anastas1a.

(4) DO NOT use the same password for two or more accounts.
   ONLY use a password for one account.

(5) If appropriate, use a password manager.

PINs

(1) DO change any initial (default) PIN assigned to you, such as a telephone mailbox PIN.

(2) DO NOT create an unnecessarily simple PIN.
   For example, DO NOT create a pin such as 6789.

(3) DO NOT create a PIN that someone else may be able to guess.
   For example, if your birthday is 25 December 2001, DO NOT create the PIN 2512 or 251201.

Emails

(1) ONLY click on any links in an email if:
   (a) You are sure who sent it;
   (b) You are certain that it does not contain, or link to, any malicious software or website.

(2) If you suspect that an email may contain, or link to, any malicious software or website:
   (a) DO NOT click on any link;
   (b) DO notify the Network Manager and/or Technical Director.
Internet

(1) DO notify the Network Manager and/or Technical Director, if you visit a website that you believe and expect to be legitimate, but it behaves in an unexpected, suspicious or apparently dangerous manner (indicating that it may have been hacked and/or infected with malware).

(2) DO configure and use your web browser(s) to operate as securely as practicable.

Consider the following.

(a) ONLY allow popups from trusted websites.

(b) DO configure your web browser to delete browsing history and temporary files when you close the browser.

(c) DO NOT allow third party cookies.

(d) DO NOT configure or use your web browser to retain (username and password) authentication information.

NOTE
Consider the use of an established, reliable password manager to manage a substantial quantity of (username and password) authentication information.

(e) DO TAKE CARE if and when you use any browser extensions.

(i) Some browser extensions, such as those provided by established, reliable password managers, can improve security.

(ii) Other browser extensions, which may provide, convenience (e.g. toolbars), media functionality (e.g. Adobe Flash) or other functionality (e.g. Java Runtime), can compromise security (e.g. by introducing vulnerabilities).

Procedures

Note the following procedures, which contain components that substantially impact the effectiveness of our implementation of information security and business continuity, and routinely apply to all staff and/or the provision of our products and services.

Provisions for data protection
- JF-7 - Project Management
- JF-11 - Installation
- JF-12 - Training
- JF-13 - Help Desk Support
- JF-14 - Remote Service and Maintenance
- JF-15 - On Site Service and Maintenance

ICT Information Security
- IS-1 - Computer Data Backups
- IS-2 - Mobile Computing
- IS-3 - Network Management

Organisational Info. Security
- IS-6 - Information Classification, Handling, Clear Desk & Screen

Business Continuity
- BC-1 – Business Continuity
- BC-3 – Disruption of the ARC
Appendix 11 – Company Information

Voice Connect Limited

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Registration Number</td>
<td>02689638</td>
</tr>
<tr>
<td>VAT Number</td>
<td>GB 558 7440 08</td>
</tr>
<tr>
<td>ICO Registration Number</td>
<td>Z7735602</td>
</tr>
<tr>
<td>Dun &amp; Bradstreet DUNS Number</td>
<td>771171204</td>
</tr>
<tr>
<td>NHS ODS Code</td>
<td>8HC51</td>
</tr>
<tr>
<td>NHS (PASA) SID Number</td>
<td>SID 002 432</td>
</tr>
</tbody>
</table>
# Appendix 12 – Important Dates

## Microsoft End of Support

<table>
<thead>
<tr>
<th>Product</th>
<th>End of Mainstream Support</th>
<th>End of Extended Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP SP3</td>
<td>14 April 2009</td>
<td>8 April 2014</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>10 April 2012</td>
<td>11 April 2017</td>
</tr>
<tr>
<td>Windows 7 and Windows Server 2008</td>
<td>13 January 2015</td>
<td>14 January 2020</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>9 January 2018</td>
<td>10 January 2023</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>9 October 2018</td>
<td>10 October 2023</td>
</tr>
<tr>
<td>Windows 10</td>
<td>13 October 2020</td>
<td>14 October 2025</td>
</tr>
<tr>
<td>Windows Server 2016</td>
<td>11 January 2022</td>
<td>11 January 2027</td>
</tr>
<tr>
<td>Office 2003 SP3</td>
<td>14 April 2009</td>
<td>8 April 2014</td>
</tr>
<tr>
<td>Office 2007 SP3</td>
<td>9 October 2012</td>
<td>30 October 2017</td>
</tr>
<tr>
<td>Office 2010 SP2</td>
<td>13 October 2015</td>
<td>13 October 2020</td>
</tr>
<tr>
<td>Office 2013 SP1</td>
<td>10 April 2018</td>
<td>11 April 2023</td>
</tr>
<tr>
<td>Office 2016</td>
<td>13 October 2020</td>
<td>14 October 2025</td>
</tr>
<tr>
<td>Exchange Server 2003 SP2</td>
<td>14 April 2009</td>
<td>8 April 2014</td>
</tr>
<tr>
<td>Exchange Server 2007 SP3</td>
<td>10 April 2012</td>
<td>11 April 2017</td>
</tr>
<tr>
<td>Exchange Server 2010 SP3</td>
<td>13 January 2015</td>
<td>14 January 2020</td>
</tr>
<tr>
<td>Exchange Server 2013 SP1</td>
<td>10 April 2018</td>
<td>11 April 2023</td>
</tr>
<tr>
<td>Exchange Server 2016</td>
<td>13 October 2020</td>
<td>14 October 2025</td>
</tr>
<tr>
<td>Dynamics CRM 4.0</td>
<td>9 April 2013</td>
<td>10 April 2018</td>
</tr>
<tr>
<td>Dynamics CRM 2011</td>
<td>12 July 2016</td>
<td>13 July 2021</td>
</tr>
<tr>
<td>Dynamics CRM 2013 SP1</td>
<td>8 January 2019</td>
<td>9 January 2024</td>
</tr>
<tr>
<td>Dynamics CRM 2015</td>
<td>14 January 2020</td>
<td>14 January 2025</td>
</tr>
<tr>
<td>Dynamics CRM 2016 SP1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SharePoint Server 2003 SP3</td>
<td>14 April 2009</td>
<td>8 April 2014</td>
</tr>
<tr>
<td>SharePoint Server 2007 SP3</td>
<td>9 October 2012</td>
<td>10 October 2017</td>
</tr>
<tr>
<td>SharePoint Server 2010 SP2</td>
<td>13 October 2015</td>
<td>13 October 2020</td>
</tr>
<tr>
<td>SharePoint Server 2013 SP1</td>
<td>10 April 2018</td>
<td>11 April 2023</td>
</tr>
<tr>
<td>SharePoint Server 2016</td>
<td>13 July 2021</td>
<td>14 July 2026</td>
</tr>
<tr>
<td>SQL Server 2005 SP4</td>
<td>12 April 2011</td>
<td>12 April 2016</td>
</tr>
<tr>
<td>SQL Server 2008 R2 SP3</td>
<td>8 July 2014</td>
<td>9 July 2019</td>
</tr>
<tr>
<td>SQL Server 2012 SP3</td>
<td>20 July 2017</td>
<td>12 July 2022</td>
</tr>
<tr>
<td>SQL Server 2014 SP2</td>
<td>9 July 2019</td>
<td>9 July 2024</td>
</tr>
<tr>
<td>SQL Server 2016 SP1</td>
<td>13 July 2021</td>
<td>14 July 2026</td>
</tr>
</tbody>
</table>

## Microsoft Internet Explorer

Since 12 January 2016 Microsoft only provides technical support and security updates for the most current version of Internet Explorer available for a supported operating system. The following link provides a list of supported operating systems and browser combinations.

http://support.microsoft.com/gp/Microsoft-Internet-Explorer
Appendix 13 – How to Maintain this Manual

Overview

This manual contains almost all the documentation of our Integrated Management System (IMS). The only other separate standalone documents are as follows.

- Contain people's names
- Organisation Chart
- Classified as VC-Confidential
- Risk Register
- Internal Statement of Applicability

Dated Documents

This manual contains the following documents.

- Integrated Management System (IMS) – Essentials
- Information Security and Business Continuity Management - Essentials
- Acceptable ICT Use and Information Security Agreement
- Quality Policy
- Information Security Policy
- Business Continuity Policy
- Environmental Policy
- Anti-Corruption Policy
- Data Protection Policy
- Data Protection – Privacy Notice
- Anti-Slavery Statement

These each have their own date of issue, immediately underneath the title. This is separate from, and independent of, the date of the entire document, shown on the front (title) page and in the footer of all other pages. The Managing Director signs printed copies of the policies and each employee must agree to, and sign, the agreement, which is current at the time that the employee joins the company.

Paragraph Styles and Heading Levels

The first part of this manual (classified as VC-Unclassified and containing the Overview, Context and Interested Parties, Risk Methodology and the Training Guides) uses the standard auto-numbered heading styles Heading 1, Heading 2, Heading 3 etcetera. Additionally, to generate the contents list, the following three heading styles are assigned as Level 1 and Level 2 headings.

Level 1

Heading – Title Page

Heading – Centred Medium

Level 2

Heading – Centred Large

To create centred headings with similar (font) weights that are NOT assigned as Level 1 and Level 2 heading, left aligned un-numbered heading styles are used and then additionally centred.
Appendix 14 – Data Protection Privacy Notice

Overview

(1) Our lawful basis for processing personal data is principally to perform contracts.
   (a) We process the personal data of employees to perform contracts of employment.
   (b) We process the personal data of other individuals to perform commercial contracts.

(2) We do NOT sell our data to, or share our data with, any other organisation or people.

Alarm Receiving Centre (ARC) - Customers and Lone Workers

(1) We hold the following details of people who work for customers of our ARC:

   Names and phone numbers of lone workers;
   Where contract requires Addresses of lone workers;
   Name and phone numbers of line managers;
   Customers’ escalation phone numbers;
   Relevant medical details (i.e. sensitive personal data);
   Names and contact details of partners and/or family.

(2) We process this data to perform a contract, to provide a lone worker protection service.

(3) Our customers provide (to us) the details of the lone workers that work for them.

(4) We do not disclose the details of any lone worker to any other organisation or person, unless contractually required to do so, e.g., to escalate an alert to one or more emergency service.

(5) We remove the details of a lone worker when a customer informs us that the person no longer works for them.

(6) We remove the details of the lone workers that work for a customer after our contract with the customer ends. We may retain some or all of the details for an interim period to enable reporting and/or invoicing etc.
Payment Portal

(1) Payment Portal retains and stores the following information:

- Order number;
- Amount;
- Transaction Reference;
- Payment result;
- Card expiry date, where needed for notification of subscription expiry.

(2) Payment Portal does not retain or store the following information:

- Name;
- Postal address;
- Email address;
- Telephone number;
- Partial payment card number.

Patient Partner and Repeat Prescriptions, Voicemail and Auto-attendant

(1) Patient Partner and Repeat Prescriptions are products that we provide to medical practices. Voicemail and Auto-attendant are products that we provide to a diverse range of customers. These process personal data but belong to the customer. Patient Partner processes telephone numbers and dates of birth. Repeat Prescriptions also processes details of medication. Voicemail records voice messages that callers leave. It is impossible to control the content of these. The owners of these products are legally responsible for the processing of personal data that these products perform.

(2) We must sometimes process personal data to perform a (maintenance) contract to provide technical support.

(3) We do not record any personal data in our permanent records of technical support.

(4) We delete any required personal data after a technical support issue is resolved and closed.

Voice Connect Communications Portal and Medical Messenger

(1) The Voice Connect Communications Portal can send single and bulk SMS text messages, and single and bulk postal messages through VC SmartMail.

(2) Medical Messenger communicates with a medical practice information system, and the Voice Connect Communications Portal, to enable a medical practice to send single and bulk SMS text, email and postal messages, via the cheapest type of message, to patients.

(3) The Voice Connect Communications Portal retains records of messages for the following periods.

- Email 14 days (default - this can be changed);
- SMS 2 months if sent via NHS.net, 6 months if sent via the Voice Connect Communications Portal;
- Post 3 months.

(4) After a customer cancels the service, we delete all of the customer’s data within 30 days.
## Appendix 15 – Data Processing Register

<table>
<thead>
<tr>
<th>DIGITAL</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange</td>
<td>Emails and Appointments</td>
</tr>
<tr>
<td>Microsoft CRM</td>
<td>Communications and Appointments</td>
</tr>
<tr>
<td>Microsoft SharePoint</td>
<td>Documents – Quotes, Specifications, Contracts etc.</td>
</tr>
<tr>
<td>Sage</td>
<td>Accounts records of purchases and sales</td>
</tr>
<tr>
<td>Customer Service Database</td>
<td>Records of:</td>
</tr>
<tr>
<td></td>
<td>(1) Delivery of products and services;</td>
</tr>
<tr>
<td></td>
<td>(2) Technical support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PAPER</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts records</td>
<td>Accounts records of purchases and sales</td>
</tr>
<tr>
<td>Lost Customers</td>
<td>Communications with customers that do not renew maintenance</td>
</tr>
<tr>
<td>Customer Complaints</td>
<td>Historical communications with customers that complain</td>
</tr>
</tbody>
</table>

### Purpose of processing

To purchase from, sell to, fulfill sales (orders and contracts) for, provide after sales support to and collaborate with, various organisations, including, but not limited to, the following:

1. Private commercial organisations (similarly funded by sales);
2. Public organisations (funded by taxes);
3. Non-profit organisations, such as charities.

### Categories of individuals

1. Our employees;
2. Employees of customers, suppliers and partners.

### Categories of personal data

Standard professional contact information, including, but not limited to, some or all, of the details below. Note that for some organisations, such as the NHS, contact information may be publicly available on a website.

1. Name and Job Title;
2. Department or Team;
3. Telephone number(s);
4. Email addresses;
5. Content of communications.

### Categories of recipients

We share contact information with another (partner) organisation, if required to fulfill a contract. A common example of this is when we implement Patient Partner together with a telephone provider.

### Reason(s) for processing

1. Legitimate interests
2. Performance of a contract

### Retention

We retain all relevant information associated with a customer.

We retain all relevant financial information associated with a customer for six years, in accordance with legal requirements.

We may further retain relevant information, associated with an organisation, after it ceases to be a customer if we believe that it is in our legitimate interest to retain the information.
### DIGITAL Voicemail

<table>
<thead>
<tr>
<th><strong>Purpose of processing</strong></th>
<th>Business communication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Categories of individuals</strong></td>
<td>(1) Our employees; (2) Employees of customers, suppliers and partners.</td>
</tr>
<tr>
<td><strong>Categories of personal data</strong></td>
<td>(1) Name; (2) Telephone number(s); (3) Content of communications.</td>
</tr>
<tr>
<td><strong>Categories of recipients</strong></td>
<td>N/A – This data is not shared.</td>
</tr>
<tr>
<td><strong>Reason(s) for processing</strong></td>
<td>(1) Legitimate interests (2) Performance of a contract</td>
</tr>
<tr>
<td><strong>Retention</strong></td>
<td>The voicemail retains recordings for 31 days after they have been listened to. Additionally a user may have a long storage facility and opt to archive a message, which will be retained until the user chooses to delete it.</td>
</tr>
</tbody>
</table>

### DIGITAL Management System

<table>
<thead>
<tr>
<th><strong>Purpose of processing</strong></th>
<th>To record that we control, our operations, to ensure that we: Meet or exceed our customers’ expectations; Maintain integrity, availability and confidentiality of information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Categories of individuals</strong></td>
<td>(1) Our employees; (2) Employees of customers, suppliers and partners.</td>
</tr>
<tr>
<td><strong>Categories of personal data</strong></td>
<td>Standard professional contact information, including, but not limited to, some or all, of the details below. (1) Name and Job Title; (2) Department or Team; (3) Telephone number(s); (4) Email addresses; (5) Content of communications.</td>
</tr>
<tr>
<td><strong>Categories of recipients</strong></td>
<td>Auditors</td>
</tr>
<tr>
<td><strong>Reason(s) for processing</strong></td>
<td>Legitimate interests – Certification to ISO 9001 and ISO 27001.</td>
</tr>
<tr>
<td><strong>Retention</strong></td>
<td>We retain all documents and records for at least four years. The re-certification audits are every three years, so the minimum four year retention ensures that all documented information is available for the period that it is subject to audit.</td>
</tr>
</tbody>
</table>
| **PAPER**  
| **Visitor’s Book**  
| --- | ---  
| Purpose of processing | Safety and security  
| Categories of individuals | Employees of customers, suppliers and partners.  
| Categories of personal data | Standard professional contact information, including, but not limited to, some or all, of the details below.  
|  | (1) Name;  
|  | (2) Company;  
|  | (3) Car Reg.  
| Categories of recipients | N/A  
| Reason(s) for processing | (1) Legitimate interests – (information) security  
|  | (2) Legal compliance – with health and safety at work  
| Retention | We retain each completed visitors’ book until it is used up.  

| **DIGITAL and PAPER**  
| **Personnel (Human Resource) Information**  
| --- | ---  
| Purpose of processing | Recruitment and employment  
| Categories of individuals | Our employees  
| Categories of personal data | Any relevant information including, but not limited to:  
|  | Name  
|  | Address  
|  | Telephone Numbers(s)  
|  | Email Address(es)  
|  | Education  
|  | Employment history  
| Categories of recipients | N/A – This data is not shared.  
| Reason(s) for processing | Performance of contracts (of employment)  
| Retention | We may retain any information whilst an employee is employed.  
|  | We retain the following information after an employee leaves:  
|  | (1) Information required to comply with statutory requirements;  
|  | (2) Information required to comply with regulatory requirements;  
|  | (3) Information we require as a consequence of the employment;  
|  | (4) Information retained by agreement with the employee.  

### DIGITAL Sage Payroll

<table>
<thead>
<tr>
<th>Purpose of processing</th>
<th>To pay employees’ salaries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of individuals</td>
<td>Our employees</td>
</tr>
<tr>
<td>Categories of personal data</td>
<td>Any relevant information including, but not limited to:</td>
</tr>
<tr>
<td></td>
<td>Name</td>
</tr>
<tr>
<td></td>
<td>Address</td>
</tr>
<tr>
<td></td>
<td>National Insurance number</td>
</tr>
<tr>
<td></td>
<td>HMRC Tax code</td>
</tr>
<tr>
<td></td>
<td>Salary payments</td>
</tr>
<tr>
<td>Categories of recipients</td>
<td>HMRC</td>
</tr>
<tr>
<td>Reason(s) for processing</td>
<td>Performance of contracts (of employment)</td>
</tr>
<tr>
<td></td>
<td>Legal requirement</td>
</tr>
<tr>
<td>Retention</td>
<td>6 years after employment ends.</td>
</tr>
</tbody>
</table>

### DIGITAL SMS Gateway

<table>
<thead>
<tr>
<th>Purpose of processing</th>
<th>To send (SMS) text messages.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of individuals</td>
<td>Patients (of medical practices) and employees (of customers)</td>
</tr>
<tr>
<td>Categories of personal data</td>
<td>This is a messaging service that we provide we have no control over the content of the messages.</td>
</tr>
<tr>
<td>Categories of recipients</td>
<td>N/A – This data is not shared.</td>
</tr>
<tr>
<td>Reason(s) for processing</td>
<td>Performance of contracts (to provide services)</td>
</tr>
<tr>
<td>Retention</td>
<td>The Voice Connect Communications Portal retains records of messages for the following periods.</td>
</tr>
<tr>
<td>Email</td>
<td>14 days (default - this can be changed);</td>
</tr>
<tr>
<td>SMS</td>
<td>2 months if sent via NHS.net, 6 months if sent via the VC Communications Portal;</td>
</tr>
<tr>
<td>Post</td>
<td>3 months.</td>
</tr>
</tbody>
</table>
### DIGITAL Hosted Voicemail

<table>
<thead>
<tr>
<th>Purpose of processing</th>
<th>To record, store and replay voice messages.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of individuals</td>
<td>Everyone</td>
</tr>
<tr>
<td>Categories of personal data</td>
<td>This is a messaging service that we provide we have no control over the content of the messages.</td>
</tr>
<tr>
<td>Categories of recipients</td>
<td>N/A – This data is not shared.</td>
</tr>
<tr>
<td>Reason(s) for processing</td>
<td>Performance of contracts (to provide services)</td>
</tr>
<tr>
<td>Retention</td>
<td>See Voicemail earlier.</td>
</tr>
</tbody>
</table>

### DIGITAL Alarm Receiving Centre (ARC)

<table>
<thead>
<tr>
<th>Purpose of processing</th>
<th>To provide a protection service for lone workers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of individuals</td>
<td>Employees of our customers that work alone.</td>
</tr>
<tr>
<td>Categories of personal data</td>
<td>This is a messaging service that we provide we have no control over the content of the messages.</td>
</tr>
<tr>
<td>Categories of recipients</td>
<td>Managers responsible for lone workers.</td>
</tr>
<tr>
<td>Reason(s) for processing</td>
<td>Performance of contracts (to provide services)</td>
</tr>
<tr>
<td>Retention</td>
<td>Data is retained for the duration of a contract and any necessary period after termination of a contract to enable billing &amp; reporting.</td>
</tr>
</tbody>
</table>

### DIGITAL Payment Portal

<table>
<thead>
<tr>
<th>Purpose of processing</th>
<th>To process card payments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categories of individuals</td>
<td>Everyone</td>
</tr>
<tr>
<td>Categories of personal data</td>
<td>Card payment details.</td>
</tr>
<tr>
<td>Categories of recipients</td>
<td>N/A – This data is not shared.</td>
</tr>
<tr>
<td>Reason(s) for processing</td>
<td>Performance of contracts (to provide services)</td>
</tr>
<tr>
<td>Retention</td>
<td>The details of cards are not retained but details of payments such as amounts and payment references (i.e. pseudonymised person identifiable data) are retained as required by contract.</td>
</tr>
</tbody>
</table>