This document is classified as **VC – Restricted** if the Annexes are attached.

VOICE CONNECT

Integrated Management System (IMS) Manual

20 July 2017

nqa
ISO 9001
Registered
Quality Management
UKAS MANAGEMENT SYSTEMS
015

SYSTEM CERTIFICATION
BMTRADA
ISO 27001
UKAS MANAGEMENT SYSTEMS
012

Contents

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 9001:2015 (and ISO 9001:2008);
(2) Information Security Management in accordance with ISO 27001:2013;
(3) The requirements of the NHS Information Governance Statement of Compliance (IGSoC);
(4) Business Continuity Management;
(5) Anti-Bribery Management.

1.2 Scope of the IMS (and Exclusions from ISO 9001:2008)

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 9001:2008.

Section 7.5.2	*Validation of processes for production and service provision* *All processes for the provision of products and services are verified by testing.* *(We test all of our software and built computer systems.)*
Section 7.6	*Control of monitoring and measuring equipment* *We do NOT use any monitoring or measuring equipment.*

1.3 Documents of the IMS

The IMS consists of the following documents.

IMS Manual	This document.
Organisation Chart	Refer to Section 1.5 (Page 8).
Business Impact Analysis	Refer to Appendix 6.
Risk Register	Refer to Appendix 5.
Statement of Applicability	This details how the IMS satisfies the requirements of the controls of ISO 27001:2013, Annex A.

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-Bribery Policy
Environmental Policy

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

Information Security and Computer Use 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 27001:2013 and ISO 22301:2012.

1.7.3 Information Security (IS) Procedures

These procedures satisfy requirements of ISO 27001:2013.

NOTES	(1)	Procedures in other sub-sub-sections cover requirements of ISO 27001.
	(2)	The Employee's Handbook contains a Disciplinary Procedure.

1.7.4 Business Continuity (BC) Procedures

These procedures satisfy general business continuity requirements and requirements of ISO 27001:2013, Control A.17.1.

1.7.5 Anti-Bribery (AB) Procedure

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

1.7.6 Management System (MS) Procedures

These procedures cover requirements of ISO 9001:2008, ISO 9001:2015, ISO 27001:2013 and ISO 22301:2012. Procedures MS1 to MS-4 and MS-6 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.

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

NOTE *Italics indicate that the Work Instruction applies to a specific customer.*

Integrated Management System (IMS) - Essentials

7 February 2017

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 staff and contractors:

Summary sheets (including this one);
Policies (Quality, Information Security, Business Continuity and Anti-Bribery);
Information Security and Computer Use 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 **nonconformity, (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 Nonconformity or Incident.*

NOTE A failure to do this may result in the issue being detected and raised as a nonconformity 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 nonconformities being raised.

Definitions from ISO 9000:2015, ISO 27000:2016 and ISO 22301:2012

nonconformity	non-fulfilment of a requirement
correction	action to eliminate a detected nonconformity
corrective action	action to eliminate the cause of a nonconformity and to prevent recurrence

Information Security Management - Essentials

25 August 2016

Fundamentals

Properties (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*

Classifications (of Information)

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

Information Security Policy	The main policy governing our implementation of information security. (See also Policies & Procedures below.) *This document is VC-Unclassified, and in the IMS Manual.*
Context & Interested Parties	This is in two parts (1) Context and (2) Interested Parties. Context is what we do. Interested Parties is what other people want us to do. *This document is VC-Unclassified, in the IMS Manual.*
Risks and Opportunities	Risks and opportunities that we identify arising from the Context and Interested Parties, and what we intend to do in response to them. *This is a separate VC-Restricted document.*
Policies & Procedures	Procedures IS-1 to IS-9 apply specifically to implementation of information security, some of which contain statements of policy. Other procedures contain provisions to implement aspects of information security, in addition to implementation of other requirements. *These documents are VC-Restricted, in the IMS Manual, Annex 2.*
Information Asset Register	An inventory of all of our information assets. *This document is VC-Restricted, in the IMS Manual, Annex 3.*
Risk Register	A list of information security threats, our vulnerabilities to them, what we do (in response) to treat them and references to any applicable ISO 27001:2013 Annex A controls. *This is a separate VC-Confidential document.*
Statement of Applicability	A list of all ISO 27001:2013 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.*

Voice Connect Ltd.

Information Security and Computer Use Agreement

28 February 2017

Information Security Policy and IMS Requirements

Voice Connect Limited operates an Integrated Management System (IMS), which manages quality, information security, business continuity and anti-bribery. The IMS is governed by the following four policies. You must comply with these policies, all procedures and other requirements of the IMS.

Quality Policy
Information Security Policy
Business Continuity Policy
Anti-Bribery Policy

Client, Information and Data, Confidentiality and Security

The purpose of this section of the agreement is to ensure that all information about clients, and their data, which Voice Connect Limited acquires, records and uses, is correct and secure.

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

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

(3) 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 the Data Protection Act 1998.)

(4) 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 remain an employee of Voice Connect.

(5) 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.

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

Computer Use

The purpose of this section of the agreement is to maximise the benefits of the computer resources that Voice Connect Limited provides to its employees. All employees must use these resources responsibly, professionally, ethically, and lawfully.

(1) You are given access to our computer network to assist you in performing your job. You should not have any expectation of privacy in anything you create, store, send or receive. The computer system belongs to the company and may only be used for business purposes.

(2) Use of computer resources for any of the following activities is strictly prohibited.

(a) Sending, receiving, downloading, displaying, printing or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful.

(b) Disseminating or storing commercial or personal advertisements, solicitations, promotions, destructive programs (that is viruses or self replicating code), political information or any other unauthorised material.

(c) Wasting computer resources through non-business activities by, for example, sending mass mailings or chain mailings or chain letters, spending excessive amounts of time on the Internet, playing games, or otherwise creating unnecessary network traffic.

(d) Using or copying software in violation of a license agreement or copyright.

(e) Violation of UK and International law.

If you become aware of anyone using computer resources for any of these activities, you must report the incident immediately to your line manager.

(3) Employees must ONLY connect to our network, directly or through VPN, devices provided by Voice Connect or devices approved by the Technical Director.

(4) You MUST NOT disclose your network password to anyone, including other employees. 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.

(5) Visitors that require internet access may use our wireless broadband. Visitors must NOT connect to our corporate network.

Laptops and Portable Storage Devices

Voice Connect Limited provides laptops to sales and technical support staff to enable them to perform their duties.

All laptops and portable storage devices must be used securely as specified by **Procedure IS-2 – Mobile Computing**.

Law

Voice Connect Limited and its employees must always comply with the law, including the following.

Data Protection Act 1998
Privacy and Electronic Communications (EC Directive) Regulations 2003
Computer Misuse Act 1990

NOTE *This legislation is available for download, free of charge, from www.legislation.gov.uk.*

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.

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

Date…….. Signature……..

Printed Name……..

VOICE CONNECT

Quality Policy

20 July 2017

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 9001:2008;
Information Security Management, certified to ISO 27001:2013;
Business Continuity Management;
Anti-Bribery 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 provide required training to our employees, to enable them to fulfil their roles.

(2) To design and develop software in accordance with planned schedules.

(3) To complete installations in one visit.

(4) To meet invoice targets (for installations and provision of products and services).

(5) To meet our Service Level Agreements (SLAs).

(6) To optimise customer satisfaction.

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

20 July 2017

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 9001:2008;
Information Security Management, certified to ISO 27001:2013;
Business Continuity Management;
Anti-Bribery 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 of the CENELEC standard EN 50518-2:2013.

(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

VOICE CONNECT

Business Continuity Policy

20 July 2017

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 9001:2008;
Information Security Management, certified to ISO 27001:2013;
Business Continuity Management;
Anti-Bribery 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

VOICE CONNECT

Environmental Policy

13 October 2016

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

Anti-Bribery Policy

28 February 2017

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 9001:2008;
Information Security Management certified to ISO 27001:2013;
Business Continuity Management;
Anti-Bribery 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.

IMPORTANT	Voice Connect is committed to implementing and enforcing effective systems to counter bribery. Therefore, it is Voice Connect's policy to conduct all aspects of its business in an honest and ethical manner at all times. Under UK law (UK Bribery Act 2010), bribery and corruption is punishable for individuals by up to ten years imprisonment. If Voice Connect is found to have taken part in the corruption or lacks adequate procedures to prevent Bribery, it could face an unlimited fine and be excluded from tendering for Government contracts.

The aim of this policy is to help Voice Connect act in accordance with the Bribery Act 2010, maintain the highest possible standards of business practice, and advise individuals of Voice Connect's 'zero-tolerance' to bribery. This policy applies to all permanent and fixed-term staff employed by Voice Connect, and any contractors, consultants or other persons acting under or on behalf of Voice Connect.

Voice Connect will not:

Make contributions of any kind with the purpose of gaining any commercial advantage.

Provide gifts or hospitality with the intention of persuading anyone to act improperly, or to influence a public official in the performance of their duties.

Make, or accept, "kickbacks" of any kind.

Company Responsibility

Voice Connect will:

Keep appropriate internal records that will evidence the business reason for making any payments to third parties.

Encourage employees to raise concerns about any issue or suspicion of malpractice at the earliest possible stage.

See that anyone raising a concern about bribery will not suffer any detriment as a result, even if they turn out to be mistaken.

Employee Responsibility

Employees must not:

Accept any financial or other reward from any person in return for providing some favour.

Request a financial or other reward from any person in return for providing some favour.

Offer any financial or other reward from any person in return for providing some favour.

Non Compliance

All employees have a role to play in enforcing the policy and are required to deal with any observed or reported breaches. Should employees feel apprehensive about their own safety in regard to addressing any breach, they should seek senior management support.

Failure to comply with this policy may lead to a lack of clarity over job role, learning needs or expected standards of performance, resulting in reduced effectiveness or efficiency, underperformance and putting service delivery at risk.

Any member of staff refusing to observe the policy will be liable to disciplinary action in accordance with Voice Connect's Disciplinary Procedure up to and including dismissal.

Implementation of the Policy

Overall responsibility for policy implementation and review rests with Voice Connect senior management. However, all employees are required to adhere to and support the implementation of the policy. Voice Connect will inform all existing employees about this policy and their role in the implementation of the policy. They will also notify all new employees of the policy on induction to Voice Connect.

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

VOICE CONNECT

Anti-Slavery Statement

7 February 2017

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 27001:2013, Control A.18.1.1 (which requires details relevant to information security).

Legislation

Data Protection Act 1998

IMPORTANT	This will need to be revised when the European Union (EU) General Data Protection Regulations (GDPR) replace the Data Protection Act 1998 in April 2018.

(1) All employees receive information security training, which includes an overview of the Data Protection Act.

(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 the Data Protection Act 1998 (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 our Work Instruction 25.

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 ***Information Security and Computer Use 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 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 ARC customers require us to maintain uninterrupted 24/7/365 operation.

Our ARC has dual remotely hosted computers and dual SIP phone lines to enable 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

Understanding the Organisation and its Context

Overview

Background, Activities and Functions

Voice Connect Limited is a software company that provides messaging products and services. It 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 Voice Connect to develop and market alternative products and services.

Constant Change

A constant and recurring influence throughout the life of Voice Connect, and with particular importance for our management system, has been the need to repeatedly change and adapt our products, services and the way that we work, to respond to technological advances and the consequential changes in the commercial environment in which we operate.

Compliance with Legal and Regulatory Requirements

As with all commercial enterprises, in addition to commercial, technological, and contractual influences, we are also subject to various legal requirements. Refer to Appendix 1, which specifies those that apply to us. Additionally, this appendix also describes how we comply with the legislation. It covers ISO 27001:2013, Annex A, Control A.18.1.1, which requires an organisation to specify how it complies with legal and regulatory requirements that apply to information security.

Products and Services

The following are some of our principal products and services.

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 continue to offer this product as an installed system for organisations with large numbers of lone workers, to operate as an in-house lone worker protection facility. 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.

www.vcsms.co.uk

The website also provides access to another service called SmartMail that enables subscribers to send single or multiple (automated) traditional mail.

Product - Medical Messenger

This is a licensed software product that can operate 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

Service - Payment Portal

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

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

IMPORTANT	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.

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.

Understanding the Needs & Expectations of Interested Parties

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

Their interests	Aspects of Operations
We provide products, services and maintenance support that add value.	Quality
We provide products, services and maintenance support in accordance with contractual requirements.	Quality Information Security
We provide products, services and maintenance support in accordance with applicable legal requirements.	Quality
We can provide products, services and maintenance support at any time (24/7/365).	Quality
We continue to provide products, services and maintenance support in the event of any disruption.	Business Continuity
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).	Information Security Business Continuity

Our interests	Aspects of Operations
We provide products and services that potential customers want to buy.	Quality
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.	Quality
We provide products and services, and maintain appropriate certifications and approvals, which enable us to successfully participate in tenders and framework agreements.	Quality Information Security Business Continuity

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.

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

Our interests	Aspects of Operations
Many end users utilise our products and services.	Quality
Customers of our ARC supply us with accurate, complete and up-to-date personal details of their lone workers.	Information Security

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.

Their Interests	Aspects of Operations
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.	Quality Information Security
We develop software in accordance with any mutually agreed schedule.	Quality
We comply with any confidentiality and non-disclosure agreements.	Quality Information Security
Our relationship is not adversely affected by the departure or absence of any of our workers.	Business Continuity

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

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.

Their interests	Aspects of Operations
We provide required training, to enable the reseller to sell our products and services.	Quality
We efficiently expedite orders.	Quality
We comply with any confidentiality and non-disclosure agreements.	Quality Information Security

Our interests	Aspects of Operations
They appropriately sell our products and services.	Quality
They provide correct and complete, required information and documentation, to enable us to expedite orders.	Quality Information Security
They comply with any confidentiality and non-disclosure agreements.	Quality Information Security

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.

Their interests	Aspects of Operations
We purchase their products and/or services.	Quality
Where applicable, we subscribe to their technical support.	Quality
Where applicable, we provide complete and accurate information when we require their technical support.	Quality Information Security

Our interests	Aspects of Operations
They provide products and/or services that meet our requirements.	Quality
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.	Quality
Where applicable, they provide continuous, uninterrupted service.	Business Continuity
Where applicable, they provide responsive and effective technical support.	Quality Information Security

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.

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

The Company's Interests	Aspects of Operations
Workers fulfil their duties effectively and add value to the company.	Quality
Workers remain with the company (so that the company retains their knowledge and skills).	Quality
Workers can, and feel able to, suggest opportunities and improvements.	Quality

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

We are currently certified to ISO 9001:2008 and ISO 27001:2013.

ISO 9001:2008 is one of several ISO international management standards that are undergoing transition to align them all to a common structure. This is known as the High Level Structure (HLS). At the end of 2016 the management system standards aligned to the HLS includes the following major standards.

ISO 9001:2015	Quality Management
ISO 27001:2013	Information Security Management
ISO 22301:2012	Business Continuity Management
ISO 14001:2015	Environmental Management
ISO 37001:2016	Anti-Bribery Management

ISO 9001 – Quality Management

The latest issue of this standard is ISO 9001:2015. This has a structure aligned to the HLS. Our Integrated Management System (IMS) is certified to the previous issue ISO 9001:2008. We will maintain certification to ISO 9001. We will adapt our IMS to comply with ISO 9001:2015.

ISO 27001 – Information Security Management

The current issue of this standard is ISO 27001:2013. This has a structure aligned to the HLS. Our IMS is certified to this standard.

ISO 22301 – Business Continuity Management

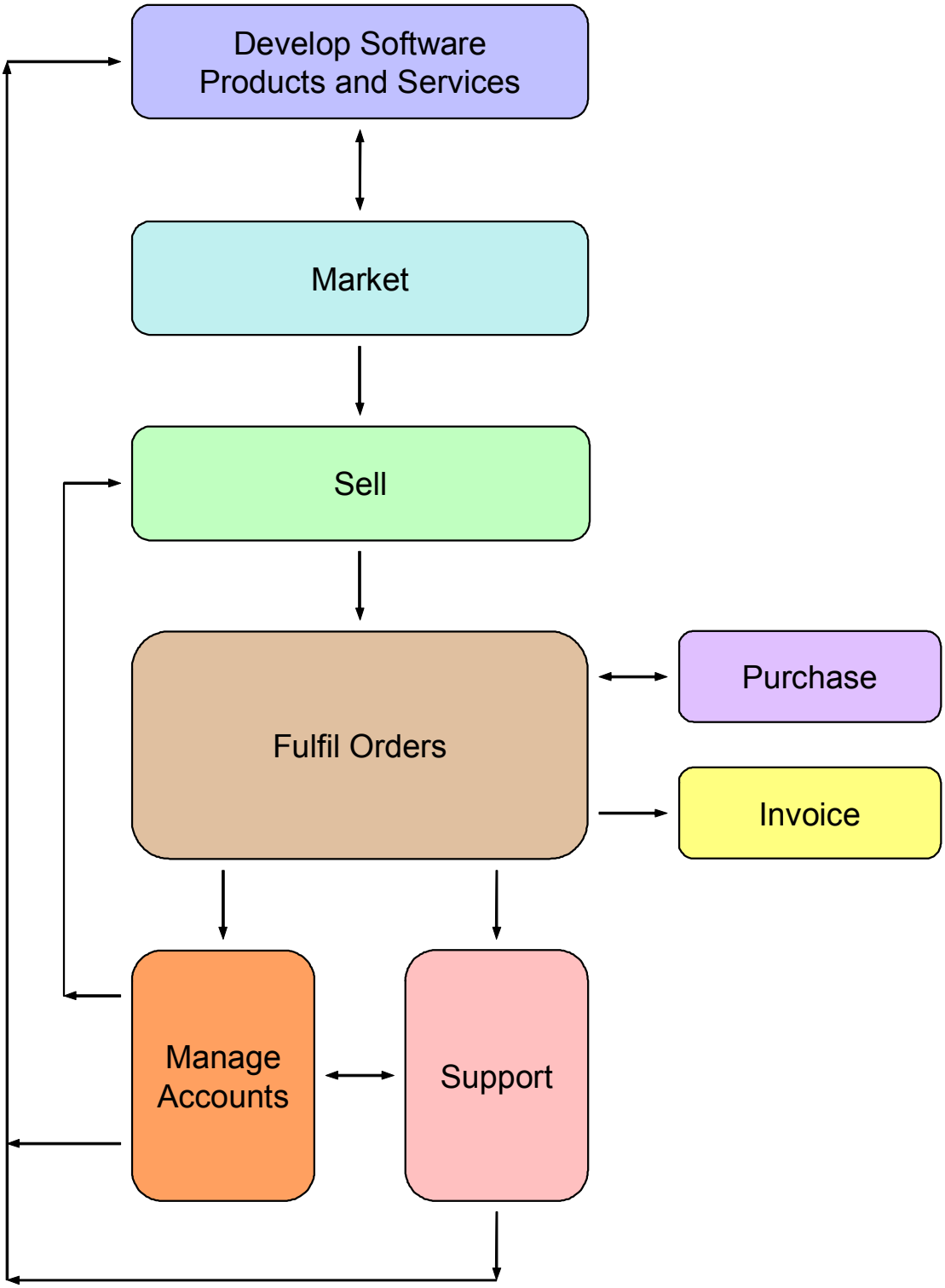
The current, and first, issue of this standard is ISO 22301:2012. It was the first ISO management standard released with a structure aligned to the HLS. We have implemented substantial business continuity measures to support our hosted lone worker protection service. We may implement further business 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

Process (Verb)	Inputs (Nouns)	Outputs (Nouns)	Resources (Nouns)	Procs.
Develop software products and services	(1) Requests and requirements for changes and additions to existing products and services. (2) Requests and ideas for new products and services.	(1) Changes and additions to existing products and services. (2) New products and services.	(1) Staff. (2) ICT equipment. (3) Development software. (4) Test environment. (5) Authoring software.	JF-1 JF-17
Market	(1) Details of products and services. (2) Details of existing customers. (3) Details of potential customers.	(1) Market awareness. (2) Appointments.	(1) Staff. (2) ICT equipment. (3) Office software. (4) Creative s/ware and resources.	JF-2 JF-3
Sell	(1) Appointments.	(1) Orders.	(1) Staff. (2) ICT equipment. (3) Office software. (4) Vehicles.	JF-4 JF-6
Fulfil Orders	(1) Orders.	(1) Operational installations of hardware and/or software. (2) Operational hosted services. (3) Operational lone worker protection services. (4) Changes and additions to configurations of operational products and services.	(1) Staff. (2) ICT equipment. (3) Office software. (4) Vehicles. (5) Component hardware and software. (6) Build area. (7) Operational hosted services. (8) Alarm Receiving Centre (ARC).	JF-7 JF-9 JF-10 JF-11 JF-12 JF-19

Process (Verb)	Inputs (Nouns)	Outputs (Nouns)	Resources (Nouns)	Procs.
Purchase	(1) Requirements for goods and services.	(1) Procured goods and services.	(1) Staff. (2) ICT equipment. (3) Office software. (4) Accounts software.	JF-8
Invoice	(1) Fulfilled orders.	(1) Received payments.	(1) Staff. (2) ICT equipment. (3) Office software. (4) Accounts software.	None
Manage Accounts	(1) Fulfilled orders.	(1) Renewals of contracts. (2) Orders for additional products and services. (3) SMS credits.	(1) Staff. (2) ICT equipment. (3) Office software. (4) Vehicles.	JF-5 JF-12
Support	(1) Requests from customers. (2) Requests from Account Managers. (3) Requests from our (ARC) staff.	(1) Resolutions of problems encountered by customers. (2) Changes to installed hardware and/or software. (3) Resolutions of problems encountered by our (ARC) staff.	(1) Staff. (2) ICT equipment. (3) Office software. (4) Vehicles. (5) Component hardware and software. (6) Build area.	JF-13 JF-14 JF-15 JF-16 JF-18

NOTES	(1)	Each Procedure specifies the Job Descriptions to which it applies.
	(2)	Each Job Description specifies the Procedures that apply to it.


Develop Software Products and Services
Market
Sell
Fulfil Orders
Purchase
Invoice
Manage Accounts
Support

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 9001:2015 – Quality Management System (QMS)
ISO 14001:2015 – Environmental Management System (EMS)
ISO 22301:2012 – Business Continuity Management System (BCMS)
ISO 27001:2013 – Information Security Management System (ISMS)
ISO 37001:2016 – Anti-Bribery Management System (ABMS)

The alignment of ISO management standards to Annex SL includes requirements to consider risks but these differ between standards. ISO 27001:2013 requires formal risk management that links to a set of controls specified in its Annex A. ISO 9001:2015 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.

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

Simple Risk Assessment

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

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

NOTE	***This method complies with the requirements of ISO 9001:2015 and ISO 14001:2015.*** It does NOT comply with the risk assessment requirements of ISO 22301:2012 – Business Continuity, ISO 27001:2013 – Information Security or ISO 37001:2016 – 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.

Risk Priority = Consequence x 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.

Risk Priority = (10 x Consequence) + 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 27001:2013 – Information Security Management;
ISO 22301:2012 – Business Continuity 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.

Consequence

3	High	**Information Security** Public exposure of confidential or personal, sensitive information leading to significant embarrassment for the company, or its customers. **Business Continuity** Severe and/or long term disruption. For example: fire or structural damage to building; severe weather for a long period; serious epidemic.
2	Medium	**Information Security** 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). **Business Continuity** Temporary, substantial disruption. For example: a loss of electrical power, for several hours; severe weather for a short period, minor epidemic.
1	Low	**Information Security** Internal exposure of internally restricted information beyond authorised individuals, system downtime or data corruption, with only minor disruption to operations. **Business Continuity** 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.

Likelihood

3	High	Likely to happen within the next 2 months
2	Medium	Likely to happen within the next 12 months
1	Low	Unlikely to happen within the next 12 months

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

Risk Priority = Consequence x Likelihood		Risk Treatment
6 or 9	***High***	***Director reduces or accepts risk.***
3 or 4	*Medium*	*Network and ICT Systems Security Review Meeting reduces or accepts Information Security Risk.* *IMS Review Meeting reduces or accepts Business Continuity Risk.*
1 or 2	Low	Acceptable – Review annually.

Documentation

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

(1) **Date Logged**

(2) **Asset**

The asset, such as the following examples.

IT Infrastructure
Sage Payroll data
Personnel (paper) files
Cisco certified staff

(3) **Type (of the Asset)**

One or more of the following five categories.

Information
Hardware
Software
Services
People

(4) **Risk Owner**

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

(5) **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.

(6) **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 following.

ISO 27000:2016, Section 2 – Terms and definitions

NOTE	This column applies to an information security risk assessment. It does NOT apply to a business continuity risk assessment.

(7) **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.

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

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

(9) **Current Countermeasure(s)**

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

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

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

NOTE	This column applies to an information security risk assessment. It does NOT apply to a business continuity risk assessment.

(11) **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.

(12) **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.

(13) **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.

(14) **Treatment Type**

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

Accept
Control
Avoid
Transfer

(15) **Treatment Owner**

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

(16) **Review Date**

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

(17) **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 **Risk Priority = Consequence x 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.*

Risk Priority = (10 x Consequence) + 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

3	High	Death; Permanent disablement; Loss of a limb, eye, sight, hearing; Serious or critical injury with permanent after effects.
2	Medium	Serious recoverable injury with no or superficial permanent after effects.
1	Low	Minor injury.

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

3	High	Likely to happen within the 1 (or 2 or 5) year(s).
2	Medium	Likely to happen within the next 10 (or 15 or 25) years.
1	Low	Unlikely to happen within the next 10 (or 15 or 25) years.

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

Risk Treatment

Risk Priority = (10 x Consequence) + Likelihood		Risk Treatment
22, 23, 31, 32 or 33	***High***	***Director reduces or accepts risk.***
12, 13 or 21	*Medium*	*Management Meeting reduces or accepts risk.*
1	Low	Acceptable – Review annually.

Appendix 6 - Maintain a Business Impact Analysis

This specifies how to compile and maintain a business impact analysis. It restates the requirements of ISO 22301, Section 8.2.2 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.

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).

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 9001:2008 and ISO 27001:2013, with additional components that satisfy the requirements of the NHS England, Information Governance Statement of Compliance (IGSoC) certification.

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 some embarrassing high profile incidents.

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 are implementing 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 (all aspects of) our arrangements for remote working are secure.

(4) We must improve our arrangements for Business Continuity, i.e. resilience.

(5) We must comply with legal requirements, such as the Data Protection Act (see Guide 3).

(6) We must satisfy the NHS England Information Governance process. (We already do this.)
This gives us access to NHS digital services, including the N3 broadband wide area network.

(7) Some organisations are beginning to require that suppliers are certified to ISO 27001.
NHS Wales effectively does.
It is conceivable that NHS England may make this a requirement.

(8) We now 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.

An incident is not just an unauthorised disclosure of personal data.

An incident may consist of a threat to one or more of the three aspects of security of information, Integrity, Availability and Confidentiality.

An incident may also be a contravention of a legal or contractual requirement.

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 be a contravention of the Data Protection Act.***
Data Protection Act	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 can also be viewed by anyone looking at the recorded details of the support call.***
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 also falls under the heading of Confidentiality.***

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.

IMS Manager
Line Manager
Director

If you are not sure whether a situation is an actual or potential incident, report it anyway.

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 the Data Protection Act 1998. 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 the Government's Office of Public Sector Information website www.opsi.gov.uk.

Data Protection Act 1998

IMPORTANT	This will need to be revised when the European Union (EU) General Data Protection Regulations (GDPR) replace the Data Protection Act 1998 in April 2018.

An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

This governs the use of personal information, and it is important to be aware of the provisions of this act, and in particular, the following.

Part 1, Item 1	This contains the definitions of terms used in the act.
Schedule 1	This specifies eight principles, ALL of which must be observed when you process any personal data.
Schedule 2	This specifies six conditions, AT LEAST ONE of which must be satisfied, in order to process personal data.
Schedule 3	This specifies ten conditions, AT LEAST ONE of which must be satisfied, in order to process sensitive personal data. The term sensitive personal data includes a person's medical information, educational information and details of criminal convictions etc.
Schedule 4	This specifies nine conditions, at least one of which must be satisfied, in order to transfer data outside of the European Economic Area (EEA = EU plus Norway, Iceland and Lichtenstein) and other states that offer equivalent protection. These are currently Andorra, Argentina, Australia, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay and also organisations in the USA subject to *Safe Harbor* or *Transfer of Air Passenger Name Record (PNR) Data*.

IMPORTANT	The practical restriction that the Data Protection Act 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 the Data Protection Act. 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.

Data Protection Act 1998

IMPORTANT	This will need to be revised when the European Union (EU) General Data Protection Regulations (GDPR) replace the Data Protection Act 1998 in April 2018.

Definitions

Data means information which -

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

i.e. a health record as defined by subsection (2),
an educational record as defined by Schedule 11, or
an accessible public record as defined by Schedule 12.

i.e. Local Authority – Housing
Local Authority – Social Services

(e) is recorded information held by a public authority and does not fall within categories (a) to (d).

Data Controller means subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Processor in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject means an individual who is the subject of personal data.

Personal Data means data which relate to a living individual who can be identified -

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including -

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

Relevant Filing System means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Sensitive Personal Data means personal data consisting of information as to -

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

(b) his political opinions,

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

(d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

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

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

Special Purposes means any one or more of the following -

(a) the purposes of journalism,

(b) artistic purposes, and

(c) literary purposes.

Schedule 1 – The Data Protection Principles

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedule 2 – Conditions for: Processing of Any Personal Data

Conditions relevant for purposes of the first principle: processing of any personal data

1 The data subject has given his consent to the processing.

2 The processing is necessary -

(a) for the performance of a contract to which the data subject is a party, or

(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary -

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or

(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Schedule 3 – Conditions for: Processing of Sensitive Data

Conditions relevant for purposes of the first principle: processing of sensitive personal data

1 The data subject has given his explicit consent to the processing of the personal data.

2 (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2) The Secretary of State may by order -

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3 The processing is necessary -

(a) in order to protect the vital interests of the data subject or another person, in a case where -

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing -

(a) is carried out in the course of its legitimate activities by any body or association which -

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6 The processing -

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7 (1) The processing is necessary -

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order -

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8 (1) The processing is necessary for medical purposes and is undertaken by -

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9 (1) The processing -

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

Schedule 4 – Cases where the Eighth Principle does NOT Apply

1 The data subject has given his consent to the transfer.

2 The transfer is necessary—

(a) for the performance of a contract between the data subject and the data controller, or

(b) for the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller.

3 The transfer is necessary—

(a) for the conclusion of a contract between the data controller and a person other than the data subject which—

(i) is entered into at the request of the data subject, or

(ii) is in the interests of the data subject, or

(b) for the performance of such a contract.

4 (1) The transfer is necessary for reasons of substantial public interest.

(2) The Secretary of State may by order specify—

(a) circumstances in which a transfer is to be taken for the purposes of sub-paragraph (1) to be necessary for reasons of substantial public interest, and

(b) circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of sub-paragraph (1) to be necessary for reasons of substantial public interest.

5 The transfer—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

6 The transfer is necessary in order to protect the vital interests of the data subject.

7 The transfer is of part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.

8 The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.

9 The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

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.

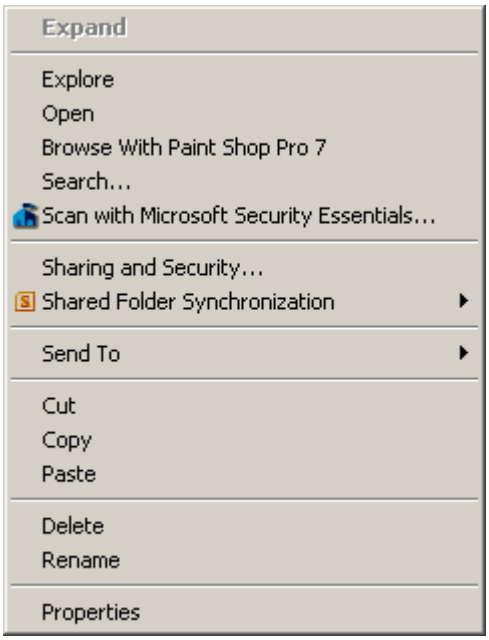
Microsoft Windows – Encrypting Filing System (EFS)

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

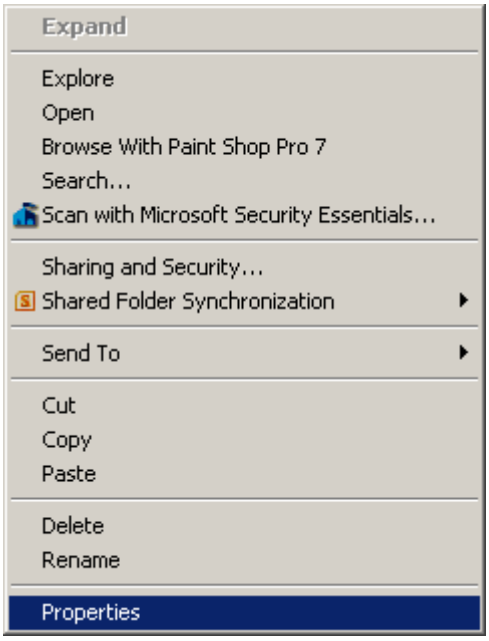
NOTE	The encryption is specific to the log in profile you use to encrypt the folder. Another user, logging in with a different user name will NOT be able to access the encrypted files. All encryption must be accessible to at least two people. Before you use this facility, speak to the Network Manager,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

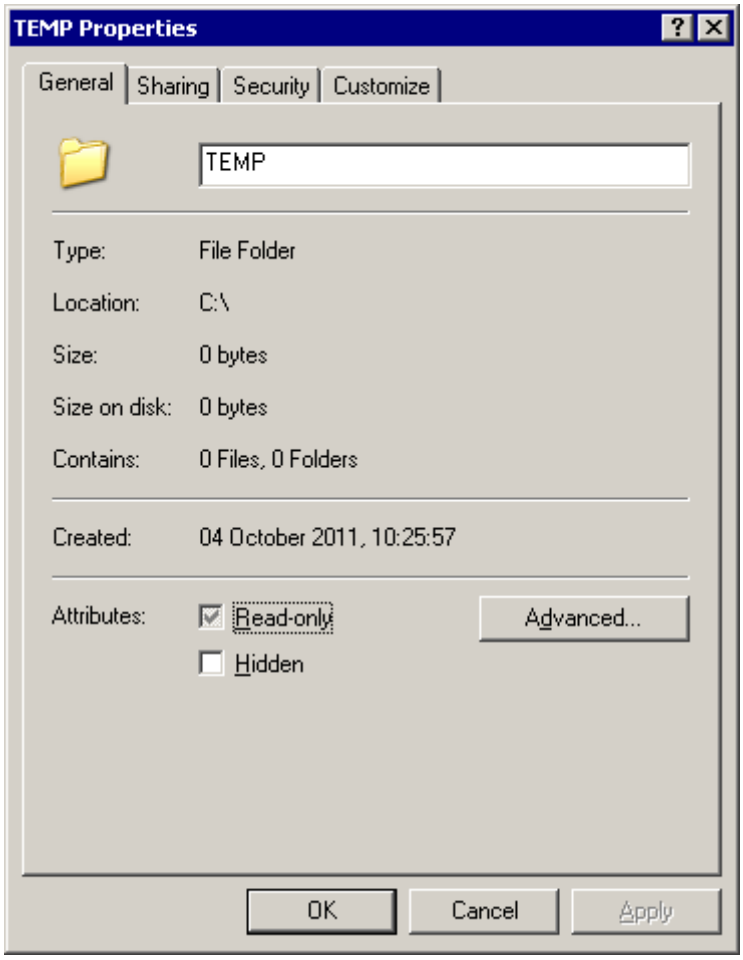
Windows displays a menu similar to the following.



(2) Select the option **Properties**.

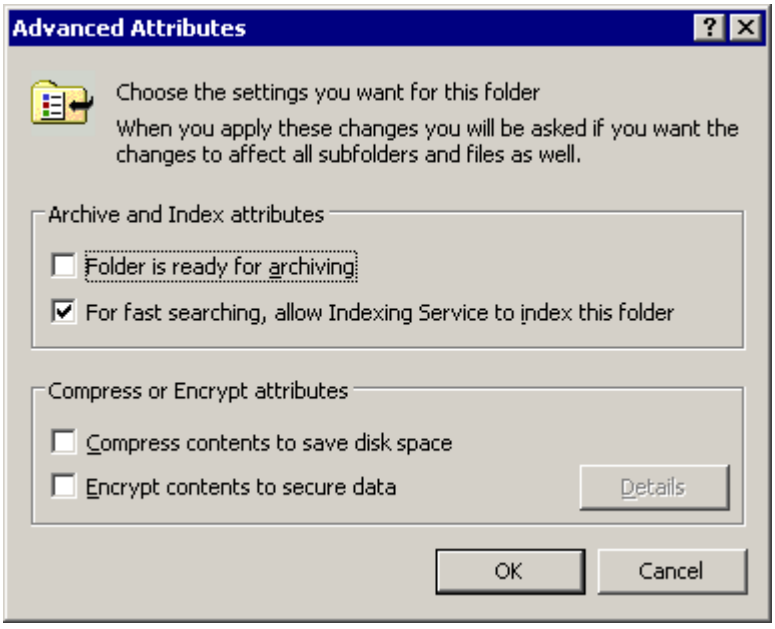


(3) Windows displays a **Properties** window for the selected folder, similar to the following.

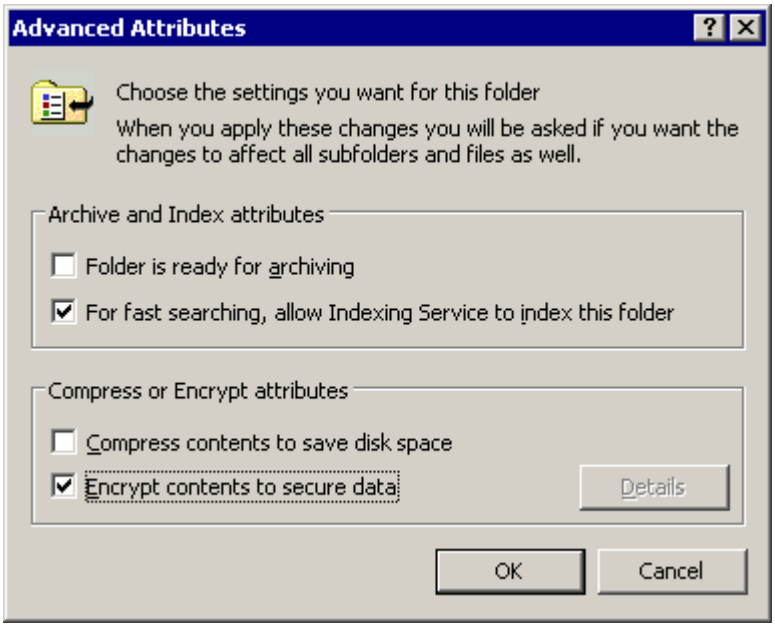


(4) Click the **Advanced** button.

(5) Windows displays the **Advanced Attributes** window, similar to the following.

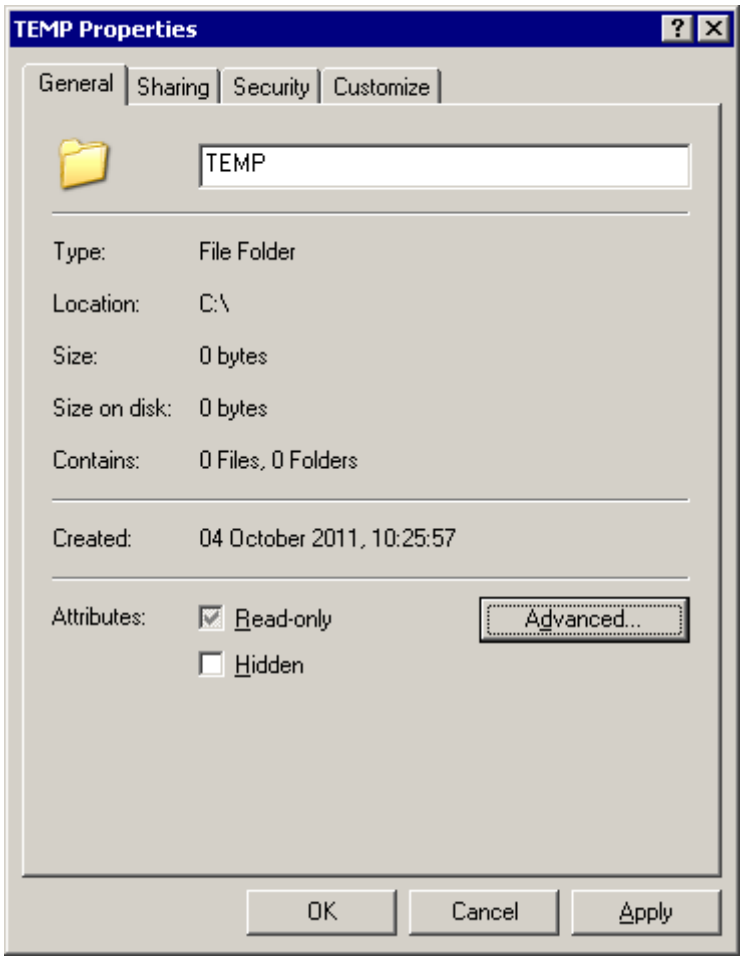


(6) Click the **Encrypt contents to secure data** check box, to select it, so that it contains a tick.



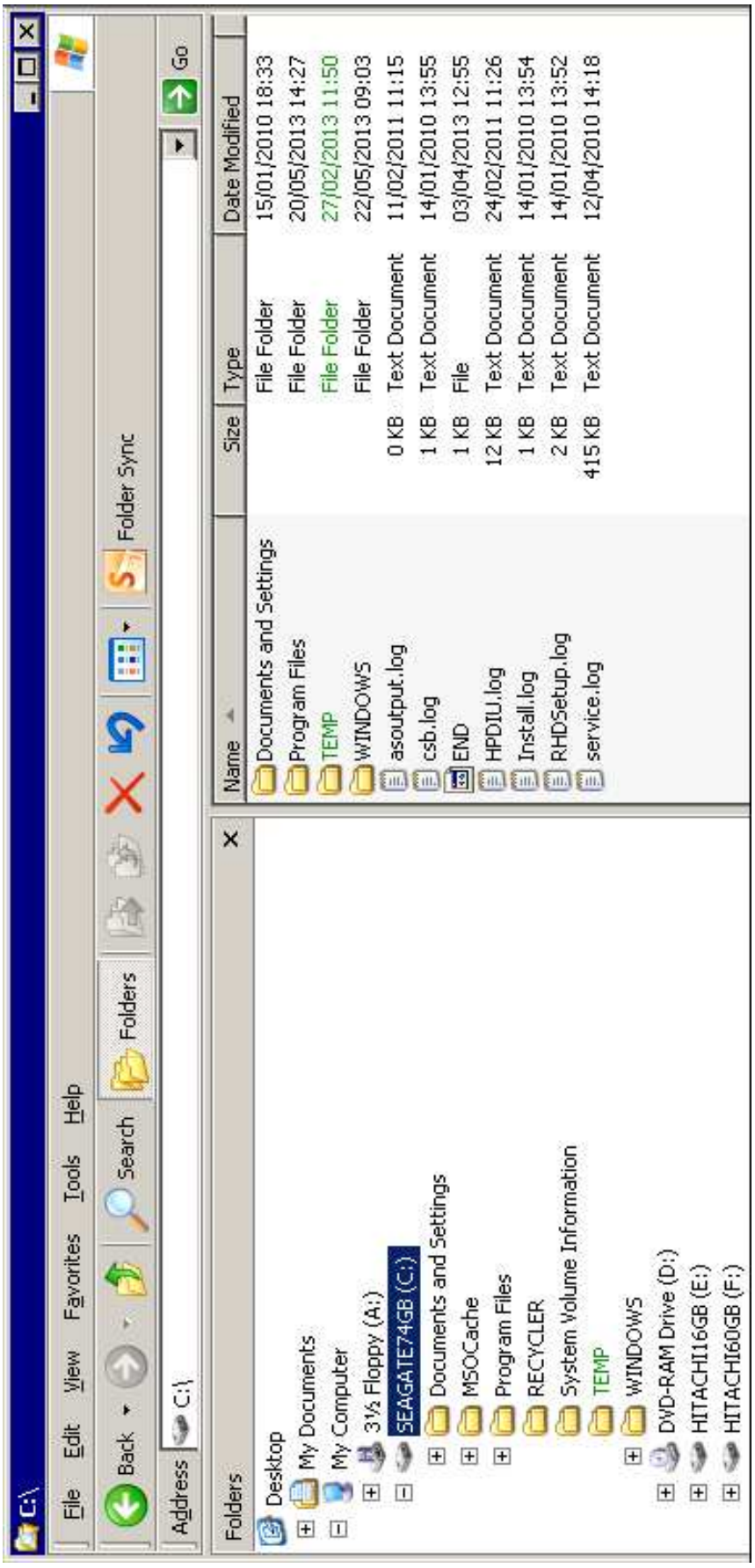
(7) Click the **OK** button.

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



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

(10) 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

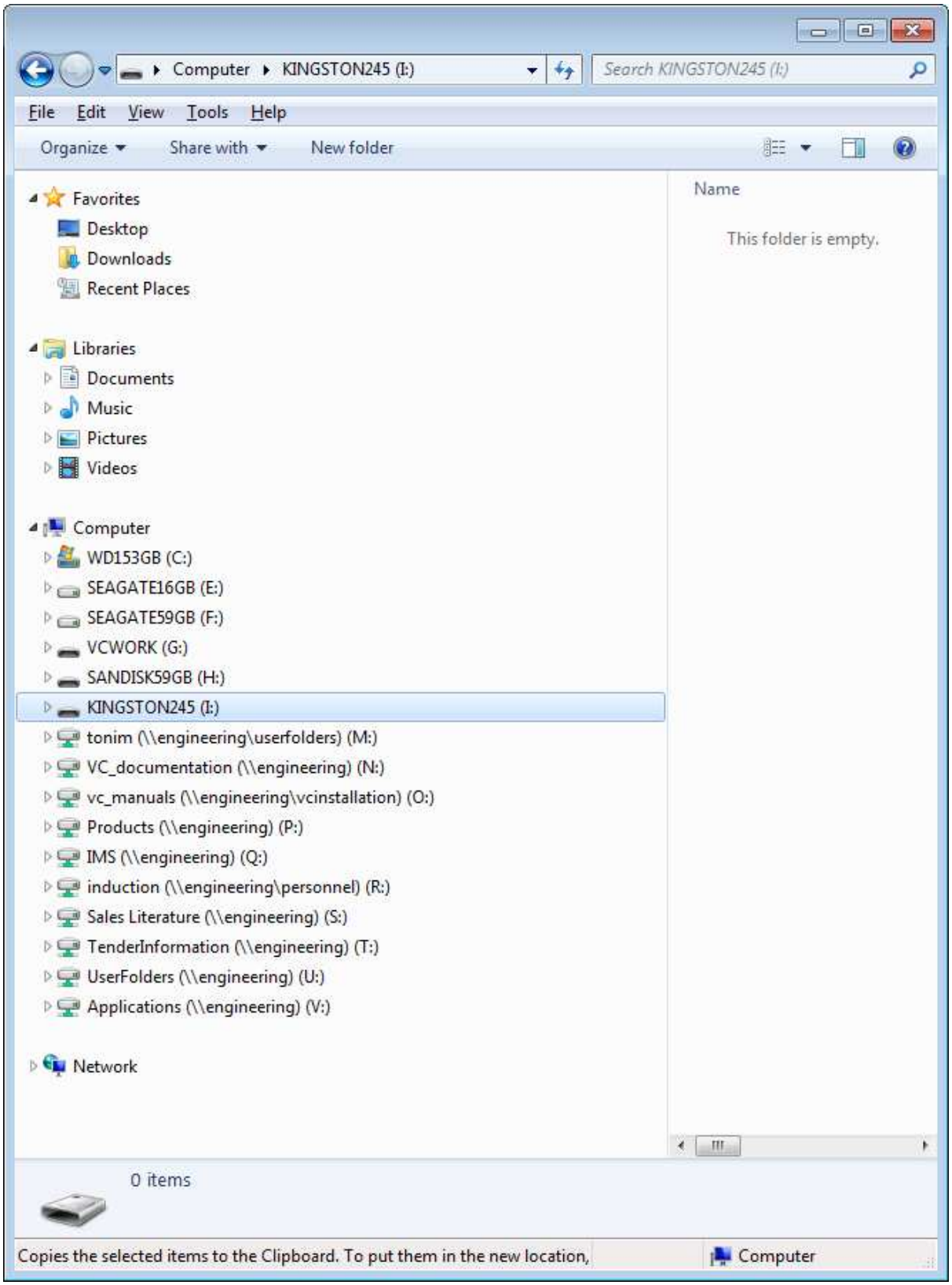
Windows BitLocker encryption enables you to encrypt (all folders and files on) a USB storage device formatted as FAT, FAT32, exFAT or NTFS. Windows 7 Enterprise, Windows 7 Ultimate and all editions of Windows 8 provide full BitLocker capability. Windows 7 Professional does not enable you to set up BitLocker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

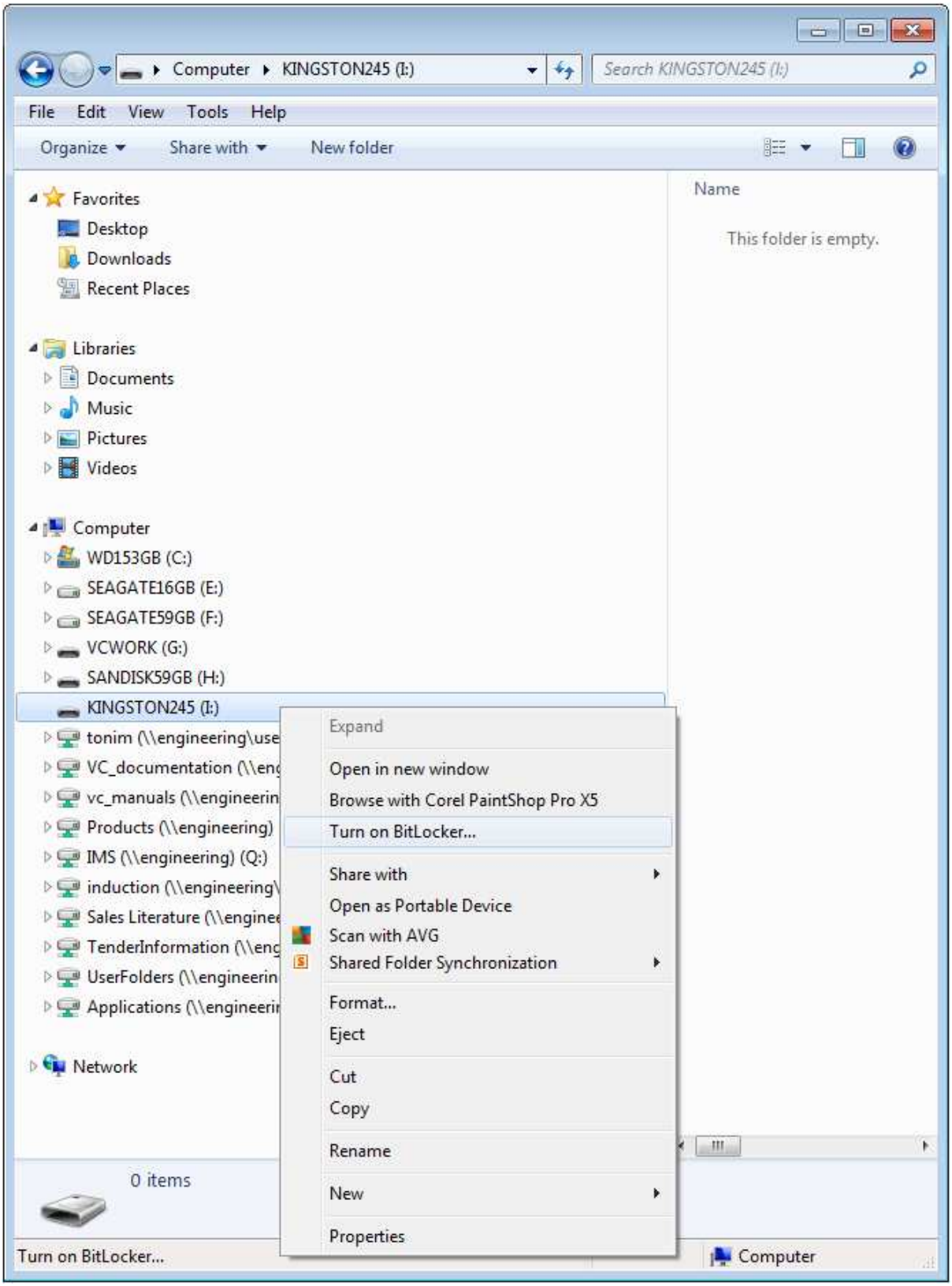
Set Up BitLocker encryption on a USB storage device

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

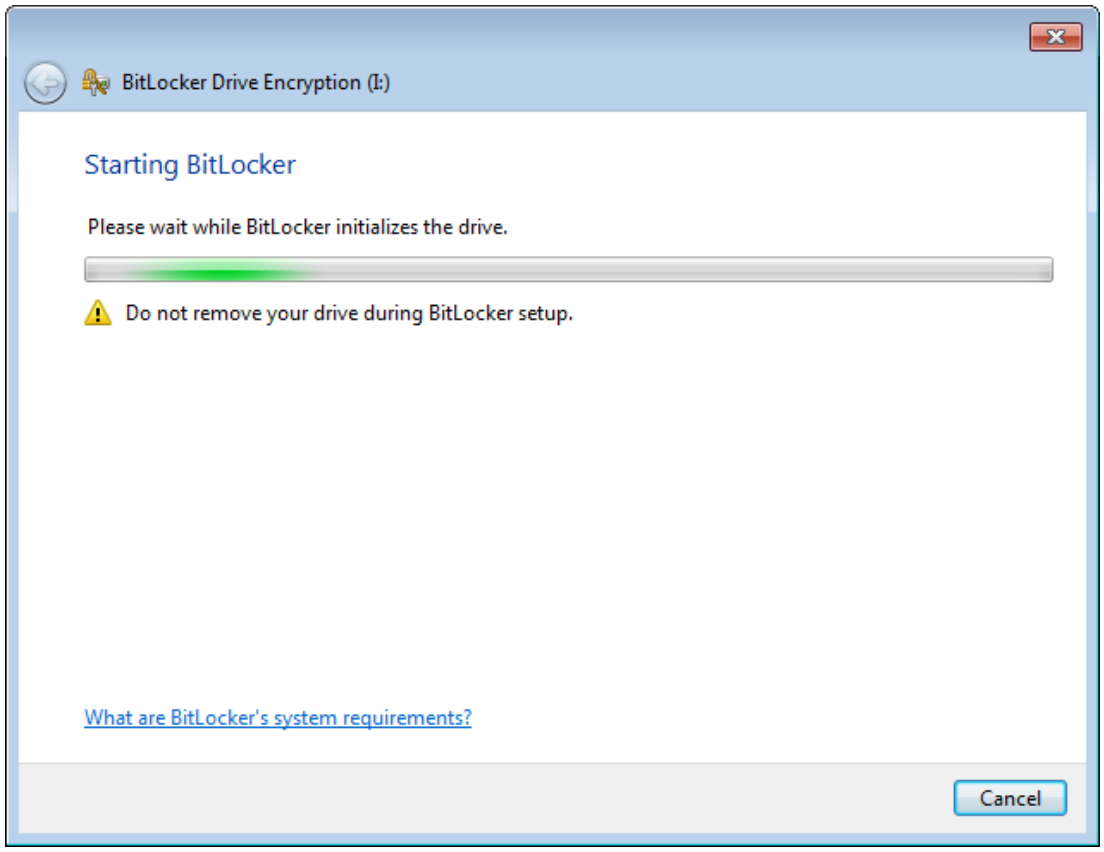
(1) Attach the USB storage device.



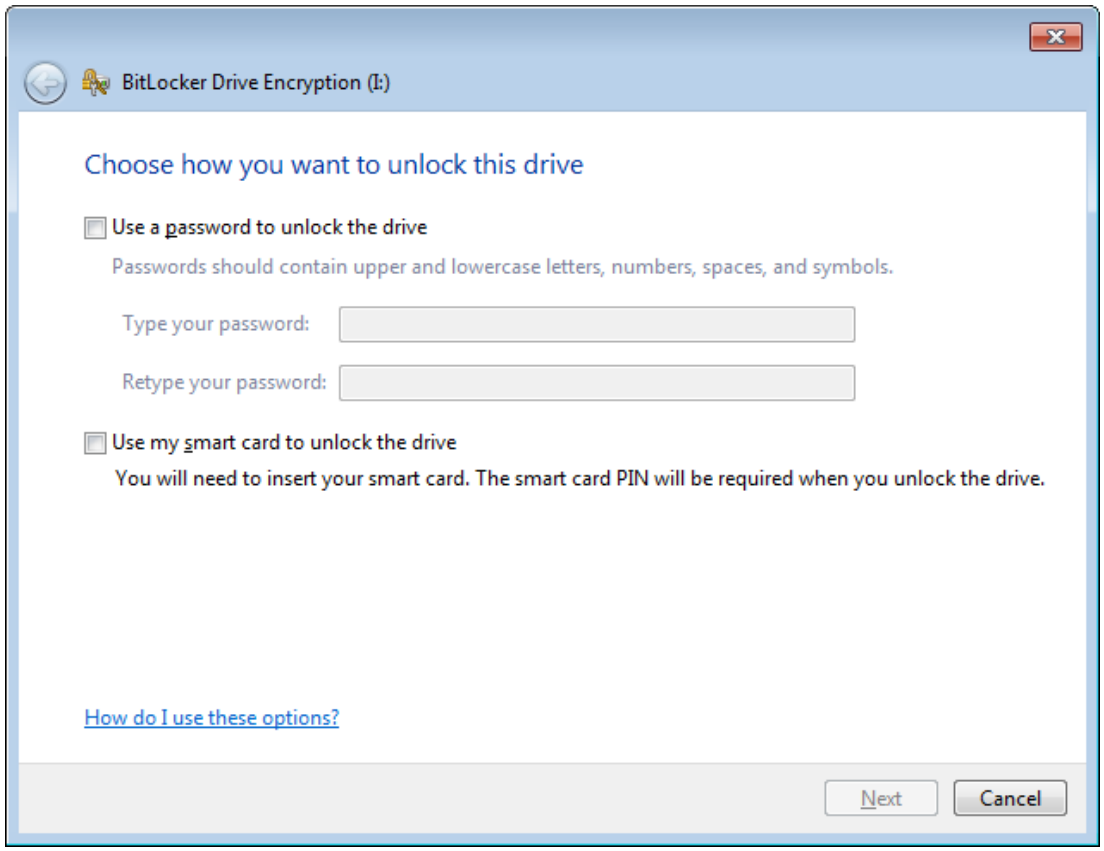
(2) Right click on the USB storage device and select the popup menu option **Turn on BitLocker**.



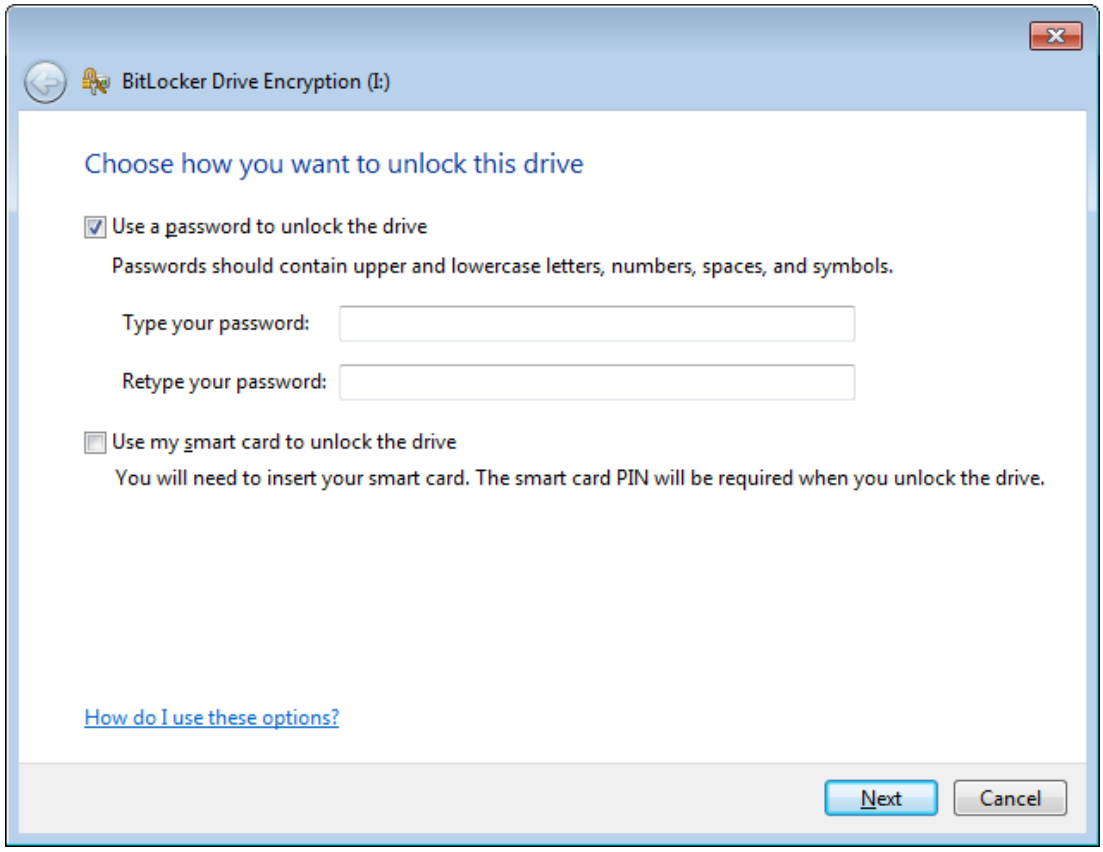
(3) Windows initially displays the following view.



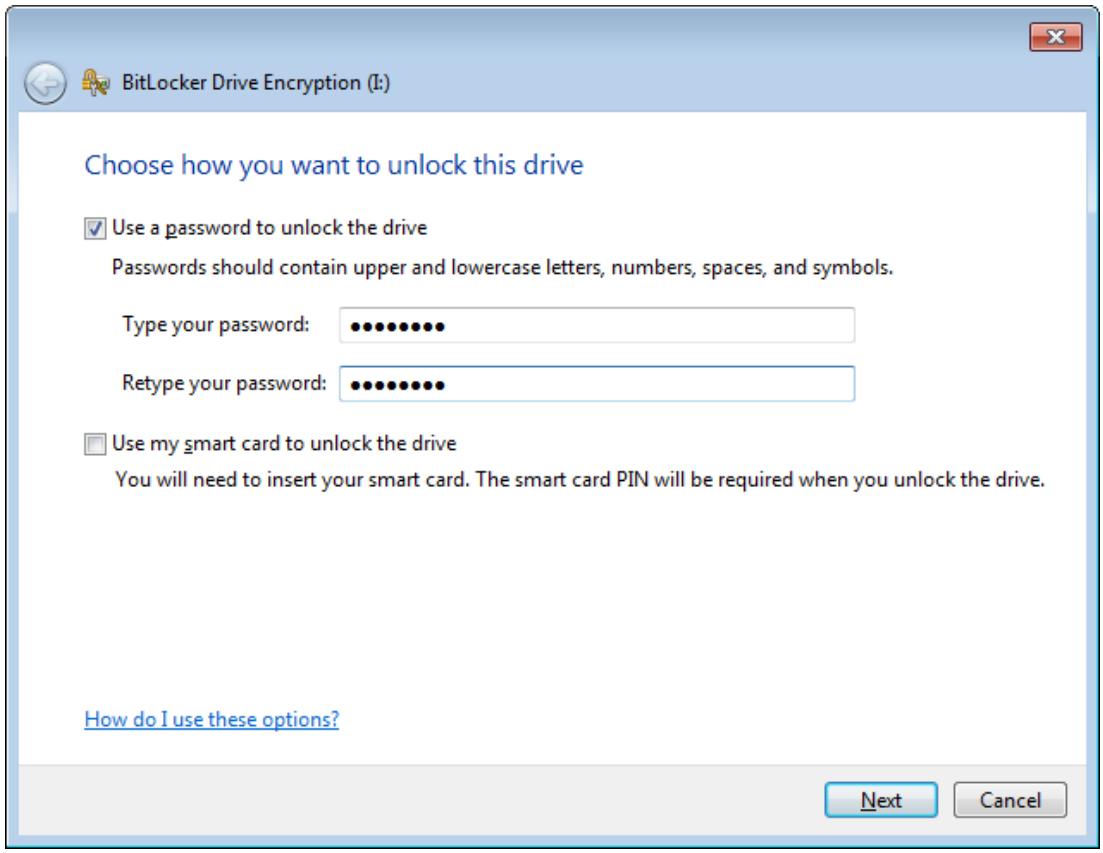
(4) Windows then displays the following prompt.



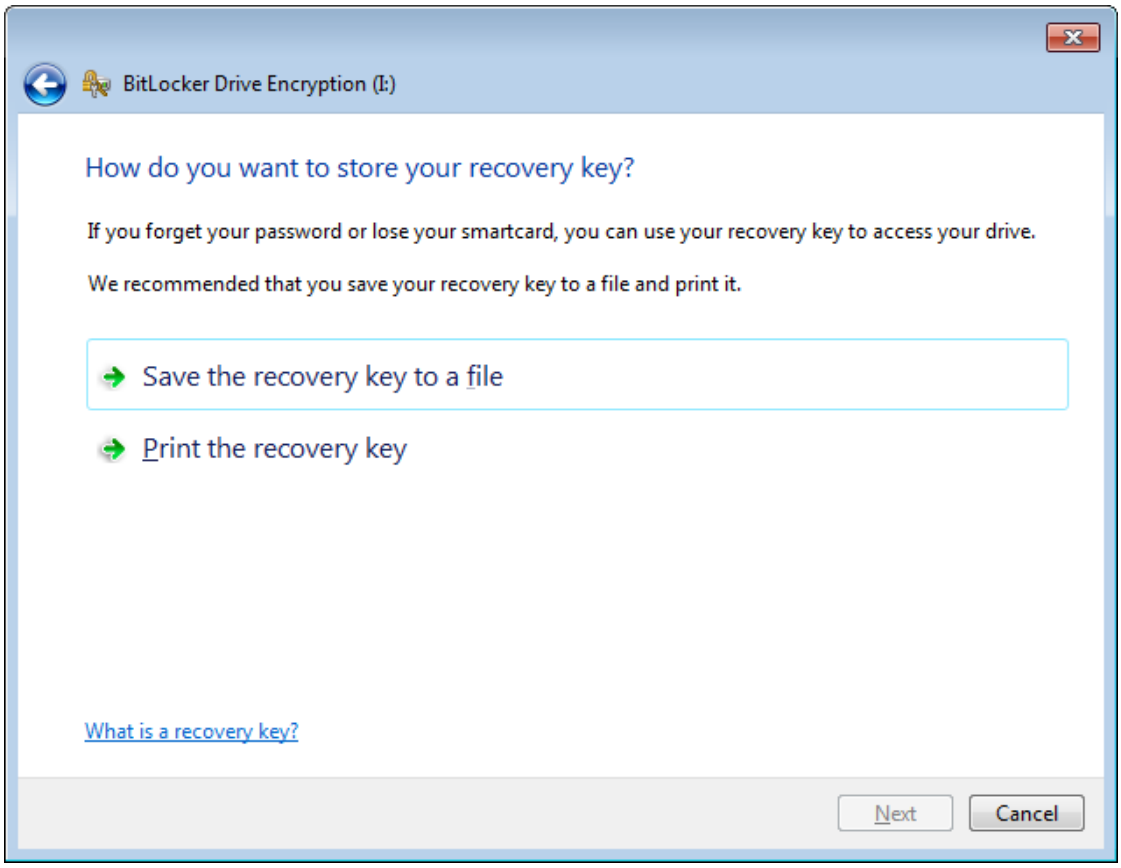
(5) Click in the **Use a password to unlock the drive** check box, so that it contains a tick.



(6) Key in the password twice and click the **Next** button.



(7) 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

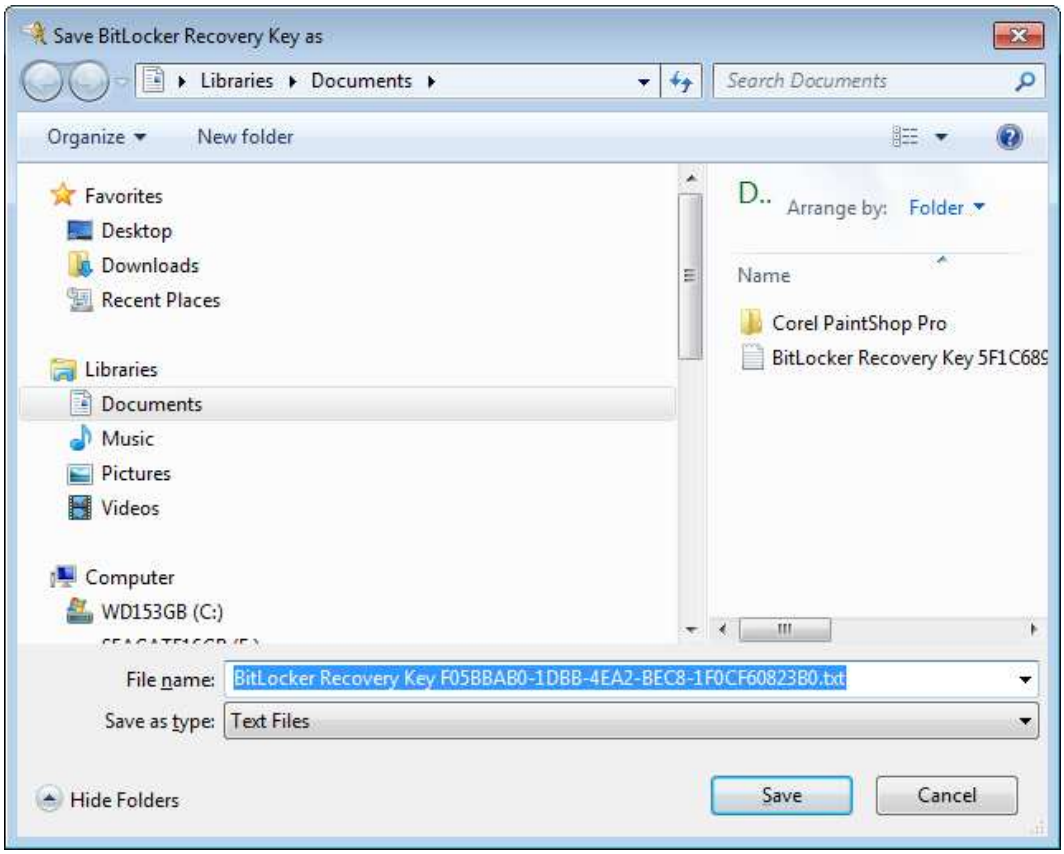
Full recovery key identification: F05BBAB0-1DBB-4EA2-BEC8-1F0CF60823B0

BitLocker Recovery Key:

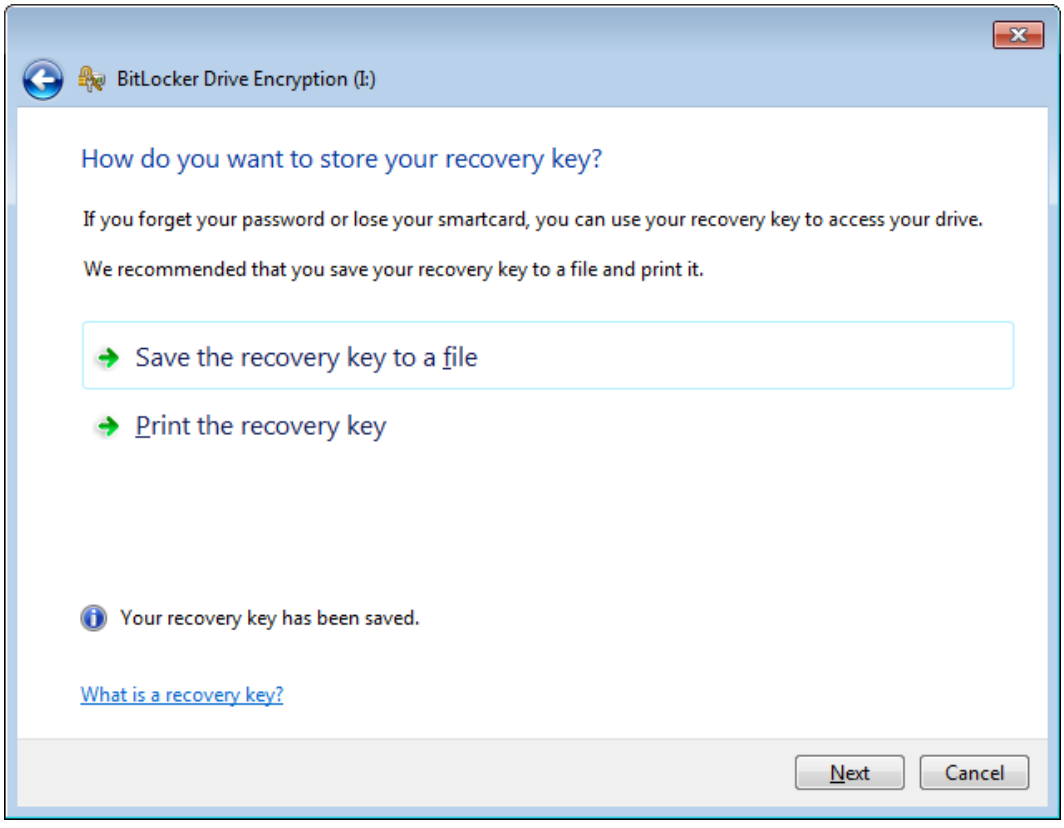
250382-294580-074679-170511-488070-315876-646173-624767

Click the **Cancel** button [and continue from Step (8)] or do the following if you require the recovery key.

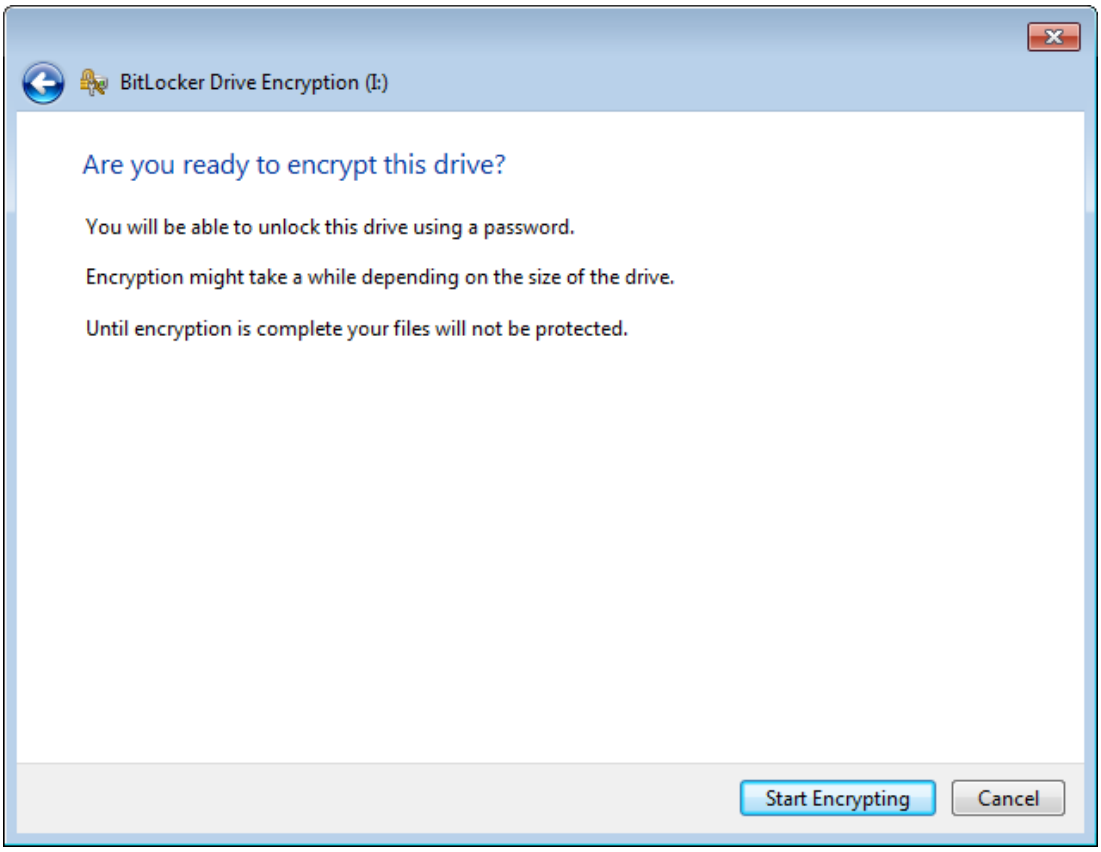
(a) Select one (or both) of the recovery key options. If you select **Save the recovery key to a file**, Windows displays the following view.



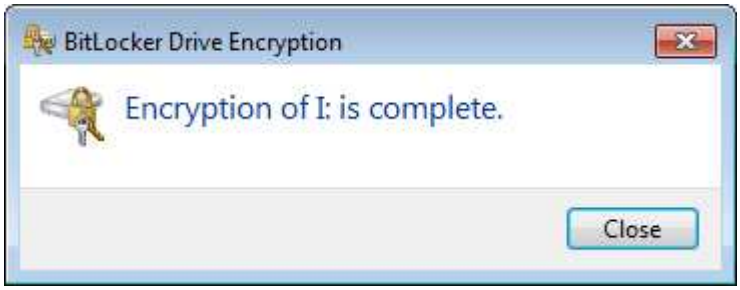
(b) After you save and/or print the recovery key, click the **Next** button.



(8) Click the **Start Encrypting** button.



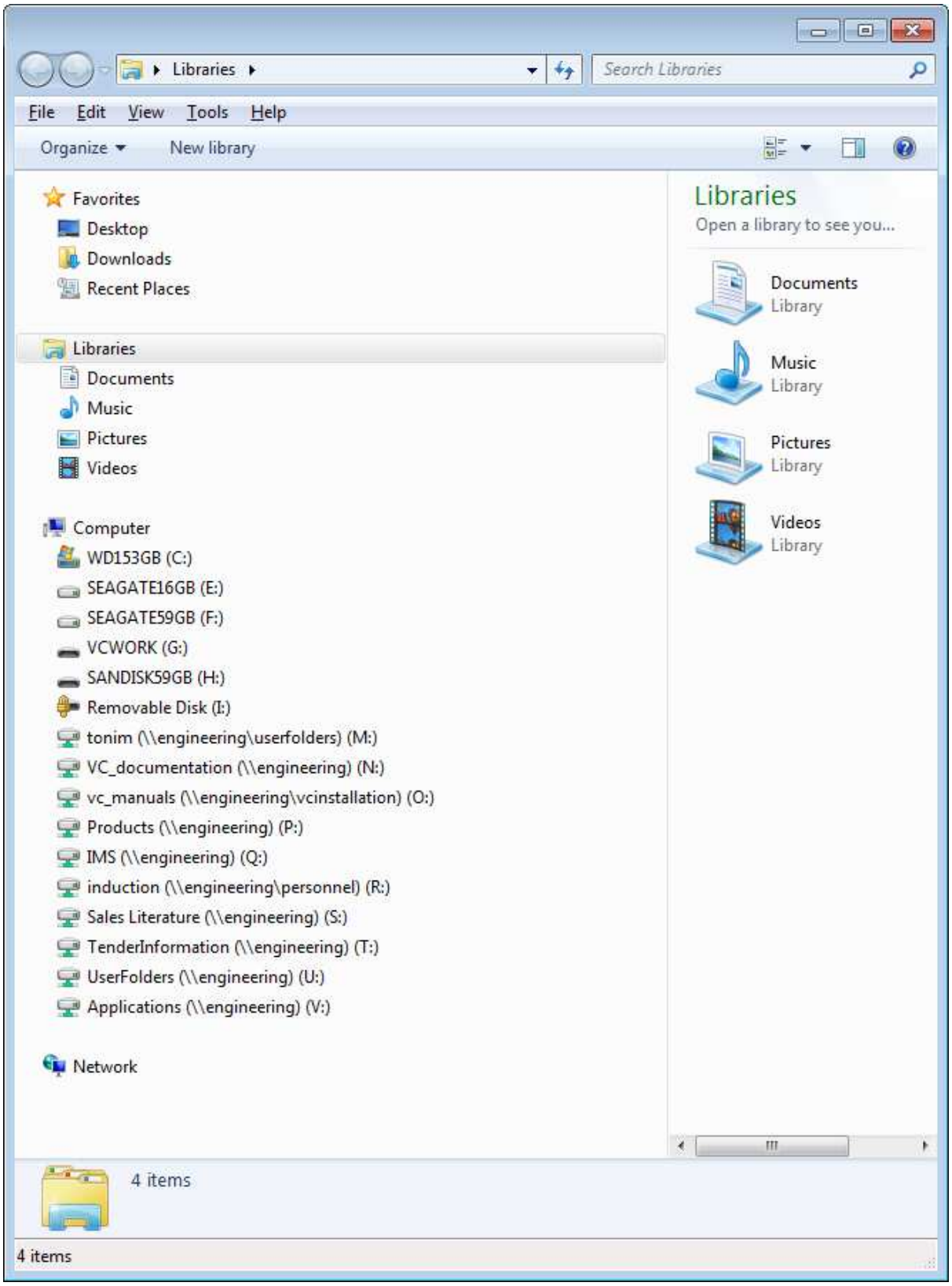
(9) Windows encrypts the USB storage device.



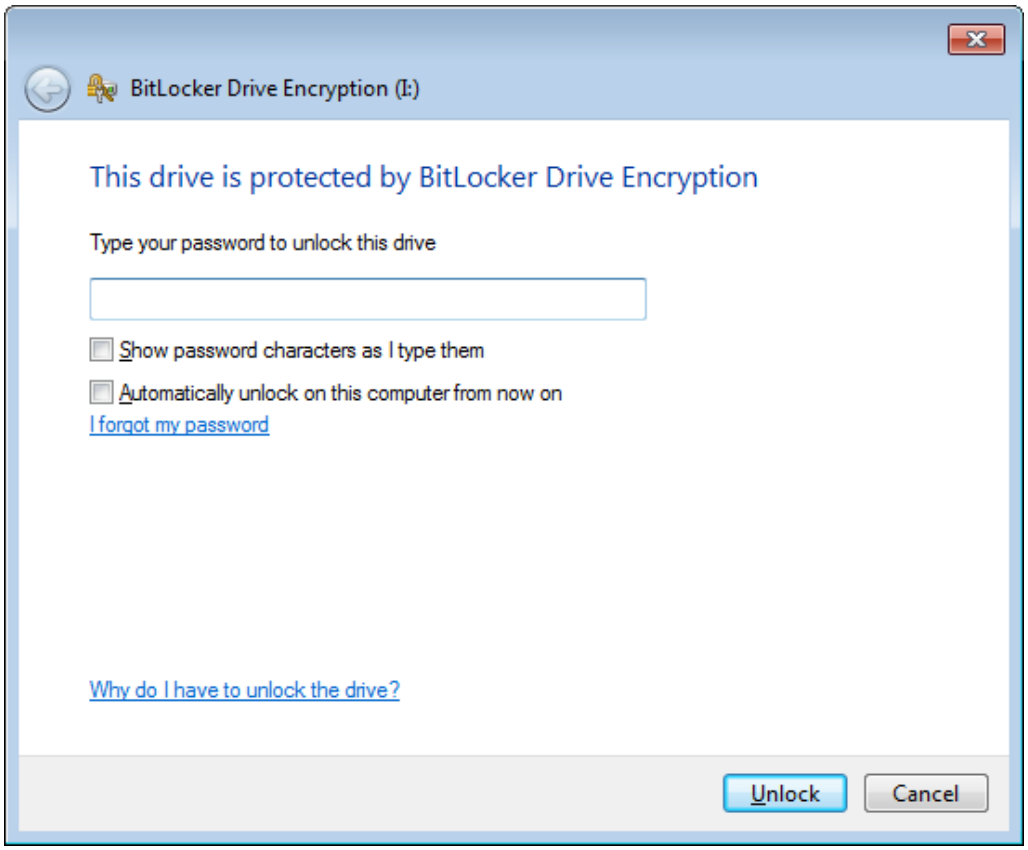
Access a USB storage device encrypted by BitLocker

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

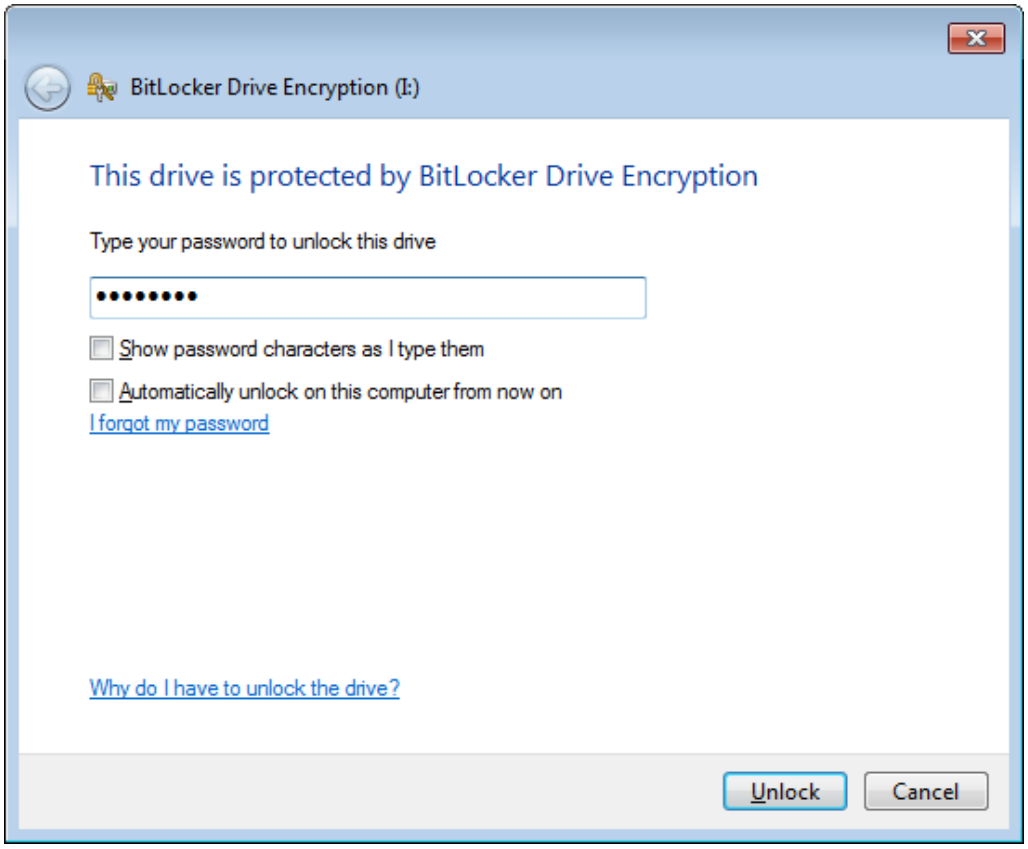
(1) Attach the USB storage device. Windows Explorer shows it with the BitLocker Icon (Drive I).



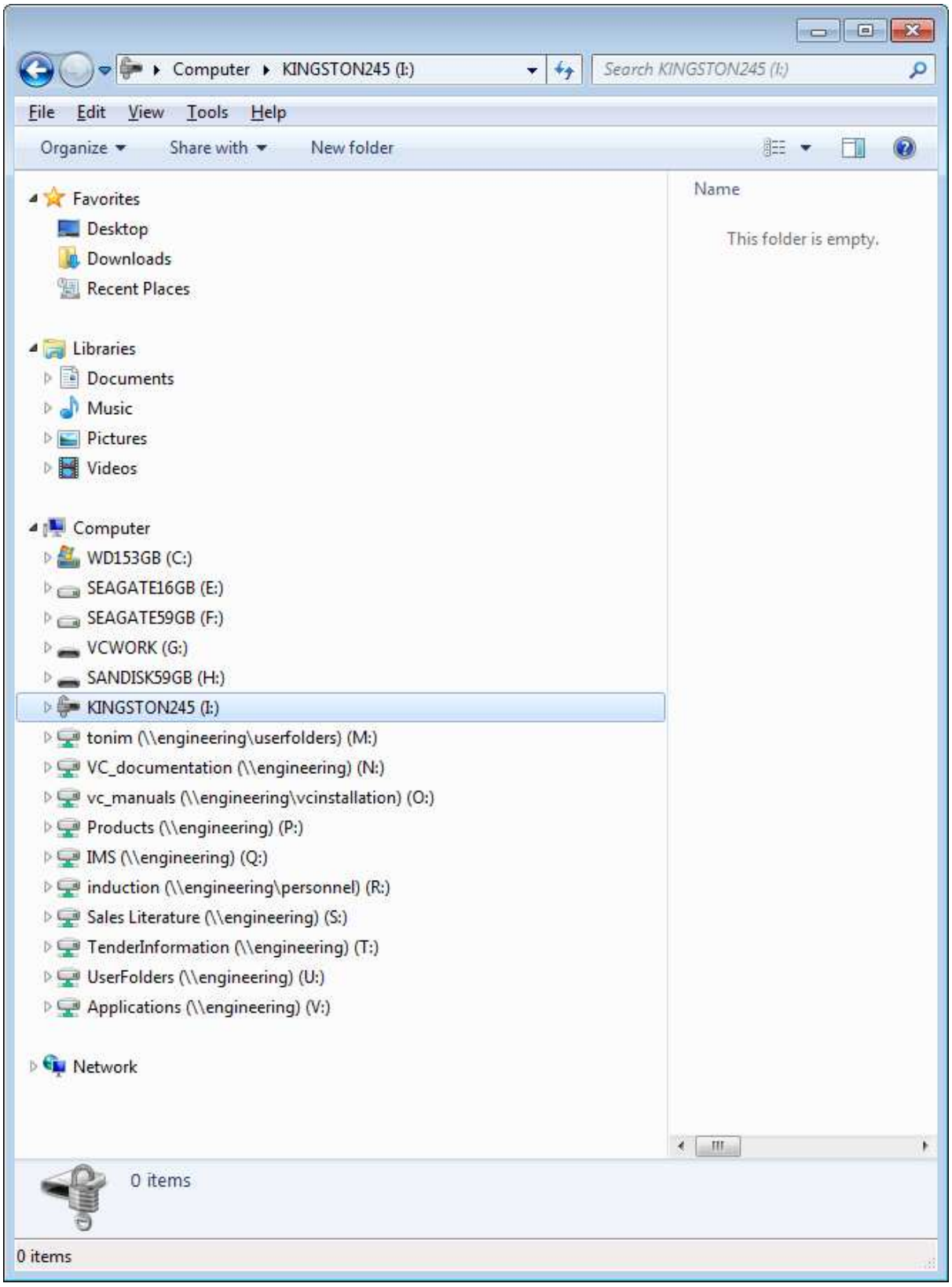
(2) Windows displays the following prompt.



(3) Key in the password and click the **Unlock** button..



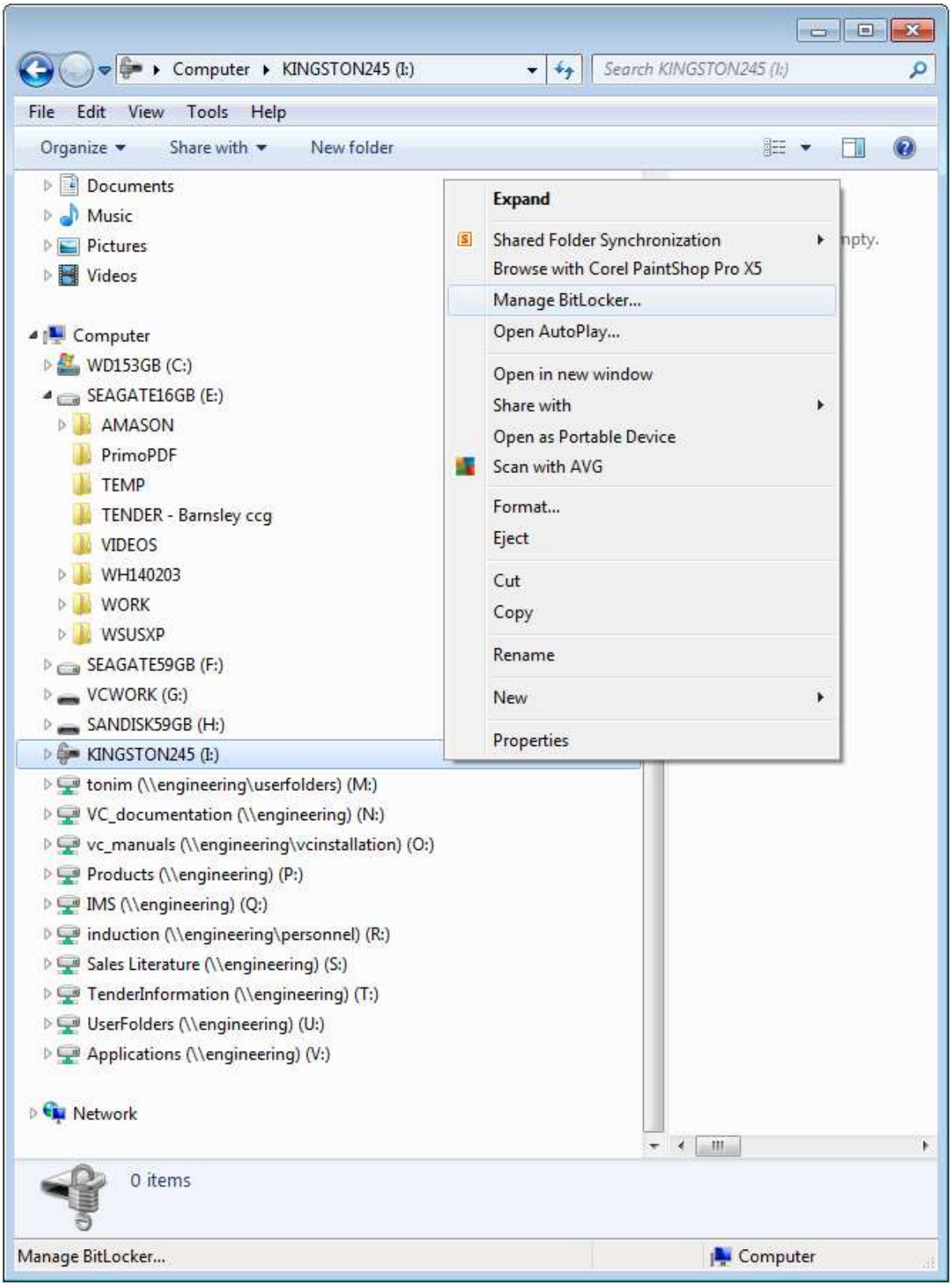
(4) Windows unlocks the USB storage device.



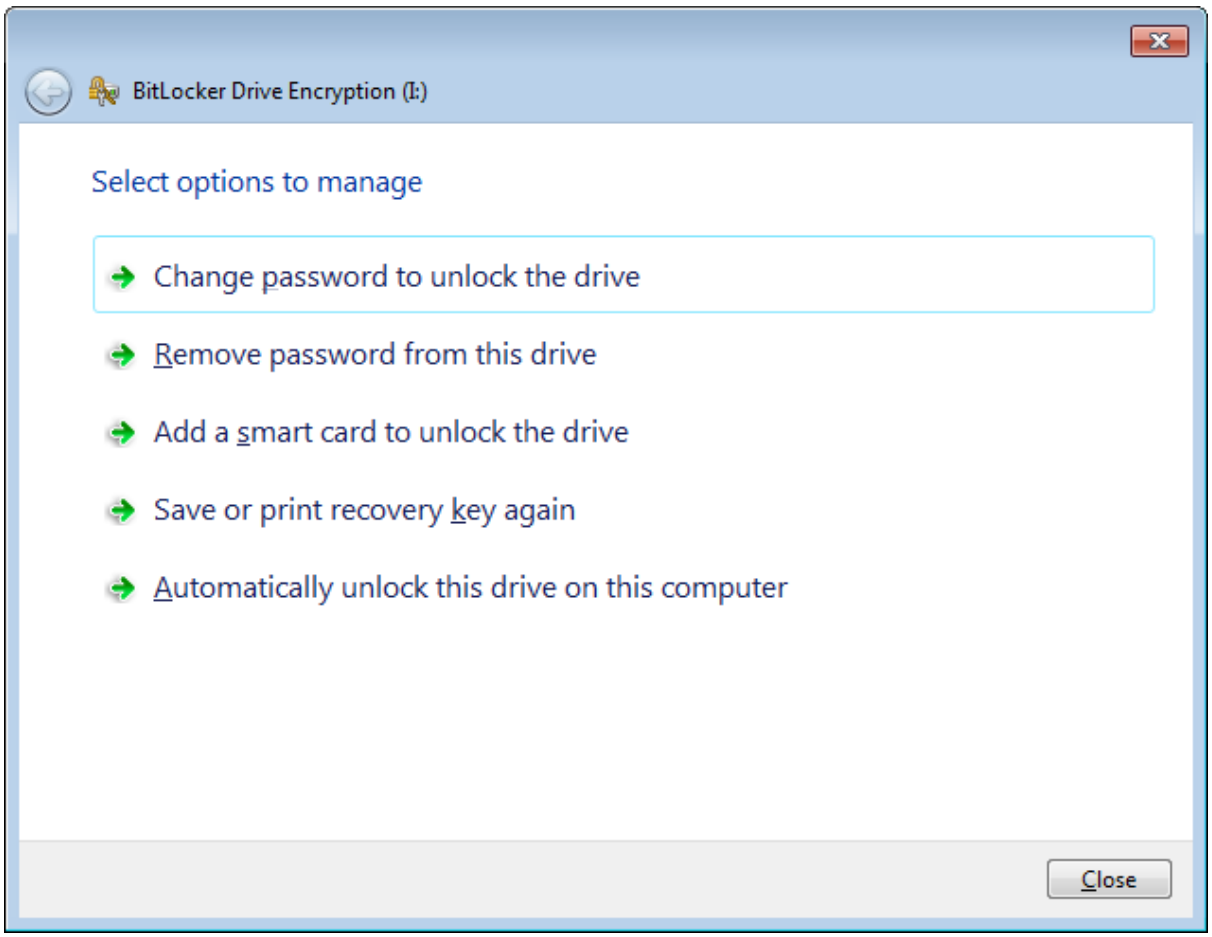
Manage BitLocker

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.



Appendix 10 - Company Information

Company Registration Numbers

Voice Connect Limited: 02689638

Voice Connect Managed Solutions Limited: 03098344

VAT Numbers

Voice Connect Limited: GB 558 7440 08

Voice Connect Managed Solutions Limited: GB 660 6393 29

Dun & Bradstreet D-U-N-S Number

Voice Connect Limited: 771171204

NHS (PASA) SID Number

Voice Connect Limited: SID 002 432

Data Protection Act - Registration Numbers

Voice Connect Limited: Z7735602

Voice Connect Managed Solutions Limited: Z632065X

Appendix 11 - Important Dates

Microsoft End of Support

NOTE *No date or* ***Bold Italics*** *indicate that the date has passed (and that the support has ended).*

Product	End of Mainstream Support	End of Extended Support
Windows XP SP3		***8 April 2014***
Windows Server 2003		***14 July 2015***
Windows Vista		***11 April 2017***
Windows 7 and Windows Server 2008	***13 January 2015***	14 January 2020
Windows 8.1	9 January 2018	10 January 2023
Windows Server 2012	9 October 2018	10 October 2023
Windows 10	13 October 2020	14 October 2025
Windows Server 2016	11 January 2022	11 January 2027
Office 2003 SP3		***8 April 2014***
Office 2007 SP3		10 October 2017
Office 2010 SP2	***13 October 2015***	13 October 2020
Office 2013 SP1	10 April 2018	11 April 2023
Office 2016	13 October 2020	14 October 2025
Exchange Server 2003 SP2		***8 April 2014***
Exchange Server 2007 SP3		***11 April 2017***
Exchange Server 2010 SP3	***13 January 2015***	14 January 2020
Exchange Server 2013 SP1	10 April 2018	11 April 2023
Exchange Server 2016	13 October 2020	14 October 2025
SQL Server 2005 SP4		***12 April 2016***
SQL Server 2008 R2 SP3	***8 July 2014***	9 July 2019
SQL Server 2012 SP3	20 July 2017	12 July 2022
SQL Server 2014 SP2	9 July 2019	9 July 2024
SQL Server 2016 SP1	13 July 2021	14 July 2026

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 12 - 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 a follows.

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

Dated Documents

This manual contains the following four documents.

Quality Policy
Information Security Scope and Policy
Environmental Scope and Policy
Information Security and Computer Use Agreement

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.