# Fincomp Services Limited
# Information Security Policy

## Table of Contents


**1. Introduction ..... 2**

**2. Acceptable Usage Policy ..... 8**

**3. Anti-Virus Policy ..... 11**

**4. Asset Management Policy ..... 13**

**5. Audit Policy ..... 16**

**6. Data Backup Policy ..... 19**

**7. Data Retention, Archiving and Destruction Policy ..... 22**

**8. Email Policy ..... 25**

**9. Encryption Policy ..... 28**

**10. Network Monitoring Policy ..... 31**

**11. Password Policy ..... 33**

**12. Physical Security Policy ..... 36**

**13. Server Security Policy ..... 38**

**14. Single-User Computer Equipment Security Policy ..... 40**

**15. Third-Party access Policy ..... 43**

# 1. Introduction

Information is a vital and valuable product of *Fincomp's* business activities. *Information Systems* are now a critical resource in enabling these core activities and communicating *our* work with *our* staff and business partners.

*Fincomp* recognises that global access to information provides many opportunities but also many challenges. The commercialisation and ubiquity of the internet has allowed hackers, virus writers and professional criminal gangs to attack free and open networks. We are now dependent on a secure environment to undertake our core business and protection of our *information systems* and information assets is essential. This **Information Security Policy** is built into *Fincomp's* management of risk framework at the highest level. It applies to all *Users* of *our information systems*.

## 1.1. Objective

The aim of the policy is to protect *Fincomp* from security problems with its *information systems* and the information stored on them that might have an adverse impact on its operations, infrastructure or reputation. A secondary aim of the policy is to raise awareness of information security issues for all *Users*.

## 1.2. Principles

### 1.2.1. Scope

Information security shall include protection of the following:

- Confidentiality: Ensuring that information and systems are accessible only to authorised *Users*.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorised *Users* have access to information and systems when required.

This policy shall apply to:

- All *information systems* owned or operated by *Fincomp* or connected to the *Fincomp network*.
- All software (including operating systems, network services and application software) installed on applicable *information systems*.
- All information stored on applicable *information systems*.

### 1.2.2. Approach

- *Fincomp* will use all reasonable, appropriate, practical, and cost-effective measures to protect its *information systems* and achieve its security objectives.
- ISO 27001/BS7799: Information Security Management will be used as a guide for determining policy and managing security.
- The policy will comply with all legal and contractual requirements including but not limited to the Regulation of Investigatory Powers Act (2000), the Data Protection Act (1998), the Human Rights Act (1998), the Computer Misuse Act (1990), and the Digital Economy Act (2010).
- The policy will not unnecessarily limit individual freedom.

### 1.2.3. Responsibilities

- All *Users* of *Fincomp's information systems* are responsible for protecting information assets. *Users* must at all times act in a responsible, professional, ethical and security conscious way, maintaining an awareness of and conformance with this policy.
- The *Managing Director (MD)* is ultimately responsible and accountable for ensuring that the objectives of this policy are met.
- The *Chief Information Officer (CIO)* is responsible for implementation of this policy and is authorised to pursue activities to achieve the objectives of this policy.
- The *CIO* is responsible for advising *Users* on security issues, preventative monitoring of *information systems* and investigating security incidents.
- *Users* should report any breach in information security or suspected breach to the *CIO* in accordance with the **Data Breach Policy**.
- Information security best practice and the terms of this policy *shall* be considered at all points in the lifecycle of equipment, software and services developed by, specified by or procured by *Fincomp*.

### 1.2.4. Practices

Further detailed policies will be produced to document specific areas of this policy. A list of the current detailed policies is provided in **Appendix A**. Supporting standards and guidelines will also be produced to provide technical information on how to implement policies for specific platforms and environments. Standards are obligatory security measures to be followed at all times. Guidelines are recommended security measures to be followed when practical to do so.

This **Information Security Policy** will be reviewed annually to determine whether it still meets the evolving needs of the information infrastructure.

### 1.2.5. Awareness

The *CIO* will publicise the policy, standards and guidelines to *Users*. Information on known vulnerabilities and patches will be made available to *Users* and *Administrators*. Information security awareness will be provided through published documents.

### 1.2.6. Applicability and Enforcement

The *CIO* will monitor *information systems* and the network to detect unauthorised activity, identify potential weaknesses and pro-actively prevent security incidents.

This policy and compliance with it applies to all *Users*. Appropriate disciplinary action under the **Acceptable Usage Policy** *may* be taken against anyone disregarding the policy.

### 1.2.7. Exceptions

Exceptions to this Security Policy *may* be made at the discretion of the *Administrators* subject to the level of additional risk to the network that may arise.

## 1.3. Appendix A: Detailed Policies

| Fincomp Services Limited<br>**Information Security Policy** |
|---|

| **Administrative Security** | **Physical Security** | **Technical Security** | **Data Management** | **Access Control** |
|---|---|---|---|---|
| Acceptable Usage Policy | Physical Security Policy | Anti-virus Policy | Audit Policy | Encryption Policy |
| Asset Management Policy | | Email Policy | Data Backup Policy | Password Policy |
| | | Server Security Policy | Data Retention, Archiving and Destruction Policy | Third-party Access Policy |
| | | Single-User Computer Equipment Security Policy | Network Monitoring Policy | |

## 1.4. Appendix B: Explanation of Terms

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given elsewhere can be found here.

### 1.4.1. Keywords

The keywords *Fincomp*, *company*, *must, must not, required, shall, shall not, should, should not, recommended, may,* and *optional* in this document are to be interpreted as follows:

- ***Fincomp***: this word, or the terms ***company, our, us*** or ***we***, means Fincomp Services Limited
- ***Must***: this word, or the terms ***required*** or ***shall***, means that the definition is an absolute requirement of the specification.
- ***Must not***: this phrase, or the phrase ***shall not***, means that the definition is an absolute prohibition of the specification.
- ***Should***: this word, or the adjective ***recommended***, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- ***Should not***: this phrase means that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- ***May***: this word, or the adjective ***optional***, means that an item is truly optional.

### 1.4.2. Other terms and definitions

The terms and definitions below have the given meaning throughout these policies. Any other computer-specific terms not included here shall be deemed to have the generally accepted computer industry definition given by **The Dictionary of Computer and Internet Terms** (Downing et al) or **Webopedia** (www.webopedia.com).

| **Term** | **Definition** |
|---|---|
| Administrator | Philip Robinson and/or Michael Robinson |
| Computer equipment | Any *server*, *personal computer* or *laptop*. |
| Chief Information Officer (CIO) | Michael Robinson (cio@fincomp.co.uk) |
| Fincomp network | The network which spans two physical locations (the London Office and the Suffolk Office) connected by a secure IPsec VPN using Triple DES encryption. |
| Managing Director (MD) | Philip Robinson |
| Mobile device | Any personal digital assistant, network-enabled mobile telephone or other small footprint device. |
| Information system | Any mechanism or method for storing information including but not limited to *IT equipment*. |
| IT equipment | Any *computer equipment*, *network equipment*, telecommunications equipment or handheld device. |
| Laptop | A portable personal computer. |

| | |
|---|---|
| London Office | 2 Keswick Road, Twickenham, TW2 7HL |
| Network equipment | Any hub, switch, router or other equipment used to transport data across a network. |
| Personal Computer (PC) | A small single-user computer based on a microprocessor. |
| Personal Data | Data that relates to a living individual that can be identified from that data, or data that when combined with other information that is in the possession of or likely to come into the possession of the data controller that can identify a living individual. |
| Responsible user | A user who normally operates a specific piece of IT equipment. |
| Server | A multi-user computer offering services over a network. |
| Single-user computer equipment | Any *personal computer*, *laptop* or *mobile device* that is used by a single person at a time and does not provide significant services to other network *Users*. |
| Suffolk Office | Dwell Deep Cottage, Low Road, Darsham, IP17 3PU |
| On-site | The *London Office* and/or the *Suffolk Office* |
| User | Phil Robinson, Michael Robinson, Kevin Tucker or any other person who is authorised to use *IT equipment*. |

# 2. Acceptable Usage Policy

## 2.1. Purpose

To establish acceptable usage guidelines for all Users of *Fincomp's Information Systems*.

## 2.2. Scope

This policy applies to all *Users* of *Fincomp's Information Systems*.

## 2.3. Policy

### 2.3.1 Context

To be permitted to use *Fincomp's Information Systems*, *Users* are deemed to have read and be bound by this policy, and the **Information Security Policy**.

*Users* need to be aware that their communications *may* be monitored by *Administrators* for the business purposes of *Fincomp* as permitted by UK legislation. The legislation allows the interception of network traffic without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised use, and ensuring the efficient operation of *Fincomp's* communications systems. *Users* should be aware that their communications *may* be released to requestors if deemed in the public interest under the Freedom of Information Act (2000).

In cases where there is suspicion of criminal activity or misconduct, further investigation by *Administrators may* result in the examination or seizure of any *Fincomp* owned *IT equipment* or media related to the suspected offence. Examination *may* include the opening and reading of email, files or other data stores deemed relevant to the investigation. *Fincomp may* disclose information to the Police or other authorities, as allowed by legislation, in the case of suspected criminal activity.

Access to a *User's* email, files or data stores related to the *Fincomp's* activities *may* also be granted to an *Administrator* if the *User* is unavailable for their normal duties for a period and the materials are necessary for the efficient operation of the *company*.

### 2.3.2. Rules for the use of the *Fincomp's Information Systems*

- Access to *Fincomp's Information Systems* is normally granted by the issue of an individual username and initial password. The individual concerned is solely responsible for work undertaken from any username issued. *Users must* only use their own username when accessing the *Fincomp network*. *Users* are responsible for the security of their passwords. Passwords *should* never be divulged to anyone and *should* be regularly changed, whilst ensuring that strong passwords are chosen. *Users should* be particularly wary of phishing attacks that appear to be official requests for your username and password, or other *Personal Data*, as these can be used for identity theft.

- Access to *Fincomp's Information Systems* is given and allocations of resources are made for the purposes of the business and for the operations and management of the *company*.
- *Users must not* damage *Fincomp*'s *IT equipment* or interfere with systems or any other user software housed on *Fincomp's Information systems*, e.g. by introducing viruses.
- *Users must not* use or attempt to use the *Fincomp network* for unauthorised purposes.
- All software used on *Fincomp IT equipment must* be appropriately licensed, and proof of such licences *must* be made available on request.
- Information issued by the *CIO* in official notices, circulars and instructions, and verbal advice given to *Users* is not confidential except where it is stated to be so. However, *Users* are warned to follow strictly any instructions issued regarding the use of proprietary software and any other confidential information. It is strongly emphasised that no such confidential information may be copied, modified or disseminated without the consent of the *CIO*.
- *Users must not* access, transmit, store, print, promote or display material where to do so constitutes a criminal offence or a civil wrong. Examples of criminal offences include the possession without a legitimate reason of an indecent photograph of a child; the possession without reasonable excuse of information of a kind likely to be useful to a person committing or preparing an act of terrorism. Examples of civil wrongs include defamation, breach of confidence and the misuse of private information.
- *Users should* ensure that any information related to *Fincomp* activities and stored locally on their desktop or laptop is backed up on a regular basis. This is to ensure that no vital data is lost. *Users must* store important data/documents on the *company's* shared drive (the L drive).
- *Users must not* use any third-party materials (including images, databases, text, sounds, logos, trade marks) in any documents (including emails and web pages) in breach of that person's intellectual property rights. As a general rule, *Users must not* copy any third-party material unless the permission of the owner has been obtained.
- *Users must not* send unsolicited bulk emails (spam)
- All use of *Fincomp's Information Systems must* comply with relevant legislation, in particular with the Data Protection Act (1998), the Human Rights Act (1998), the Copyright, Designs and Patents Act (1988), the Computer Misuse Act (1990), the Privacy and Electronic Communications (EC Directive) Regulations (2003), the Freedom of Information Act (2000) and the Counter-Terrorism and Security Act (2015).

## 2.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 2.5. Terms and Definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

## 2.6. Enforcement

Any *User* found to have violated this policy *may* be subject to disciplinary action.

# 3. Anti-Virus Policy

## 3.1. Purpose

To establish the requirements for effective virus detection and prevention.

## 3.2. Scope

This policy applies to:

- All *Fincomp* owned or operated *computer equipment* connected to the *Fincomp Network*
- All Third-Party *computer equipment* connected to the *Fincomp Network*
- All *Users* of the above *computer equipment*.

## 3.3. Policy

### 3.3.1. Use of Anti-Virus software

All *computer equipment* identified by the scope of the policy *shall* have anti-virus software installed and operational. On first installation of the anti-virus software a full virus scan of all attached storage devices (hard disks) *must* be completed.

### 3.3.2. Operation for *PCs* and *laptops*

For *PCs* and *laptops*, if the anti-virus software provides an 'always on' background process, this *must* be turned on. Regular, full virus scans *must* be undertaken.

Where the anti-virus software provides an automatic, scheduled virus scanning capability, this *must* be turned on. For *computer equipment* with 'always on' virus scanning, full virus scans *shall* be scheduled at least once a month. For *computer equipment* without 'always on' virus scanning, full virus scans *shall* be scheduled at least once a week.

Suspicious files received via email, network download, disk, CD or other media from unknown or untrusted sources *must* be scanned for viruses before being opened.

### 3.3.3. Operation for *servers*

For *servers*, if the anti-virus software provides an 'always on' background process, this *should* be turned on if this does not significantly affect the performance or operation of the *server*. Regular, full virus scans of the *server must* be undertaken at least once a month. Where a full virus scan affects performance or operation of the server, it is *recommended* that the scan be performed out of regular office hours, at weekends or during scheduled downtime.

Suspicious files found on the *server* or reported to the *Administrators* that come from an unknown or untrusted source *must* be scanned for viruses before being opened.

3.3.4. Updating virus signatures
Virus signature files *must* be updated regularly. Where the anti-virus software provides automatic checking for new virus signatures, this *must* be turned on. For *computer equipment* with automatic checking, the software *must* be scheduled to check for new virus signatures at least once a day. For *computer equipment* without automatic checking, manual checks *must* be made at least once a week.

3.3.5. Disinfecting Computers
Once a virus is detected the infected files *must* be disinfected, deleted or quarantined. If the file cannot be disinfected or removed automatically by the anti-virus software, the matter must be referred to an *Administrator.*

3.3.6. Creation or distribution of viruses
Any activities undertaken with the intention of creating and/or distributing viruses or other malicious code are prohibited, in accordance with the **Acceptable Usage Policy.**

3.3.7. Exceptions
Exceptions to this policy *shall* only be made in the following circumstances:

- No anti-virus software is available for the particular platform.
- All available anti-virus software conflicts with essential services or applications running on the *computer equipment* causing the system to crash or become unusable.

3.3.8. Responsibilities
*Users shall* be responsible for ensuring that anti-virus software is installed and operating on all *PCs* or *laptops* they have been personally allocated. *Users* may request assistance from *Administrators* in implementing this policy.

*Administrators shall* be responsible for ensuring that anti-virus software is installed and operating on *servers* or shared *computer equipment*.

## 3.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 3.5. Terms and Definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

## 3.6. Enforcement

Any *User* found to have violated this policy *may* be subject to disciplinary action.

# 4. Asset Management Policy

## 4.1. Purpose

To define the hardware, software and information assets of *Fincomp* and to define the minimum requirements for managing these assets in a secure way.

## 4.2. Scope

This policy applies to all hardware, software and information assets as defined below.

All *IT equipment* owned or operated by *Fincomp* are hardware assets of *Fincomp*.

All commercial software owned or licensed by *Fincomp* and all open source software operated by *Fincomp* are software assets of *Fincomp*.

The contents of all databases, electronic mailboxes, word processing documents, spreadsheets, web pages, data files, configurations files and other *information systems* created by *Users* in the course of their duties are information assets of *Fincomp*[1].

## 4.3. Policy

Information assets are the ultimate product of the use of hardware and software assets. The creation, manipulation and dissemination of information assets is the lifeblood of *Fincomp*.

Information assets *shall* be protected by the secure installation, configuration and updating of *information systems*. Secure installation, configuration and updating of hardware and software assets *shall* be verified, in part, by asset management and tracking.

### 4.3.1. Hardware assets

The *CIO shall* maintain an inventory of all hardware assets connected to *Fincomp's network*. The following information *shall* be maintained as part of the inventory.

- Location
- Owner (or Administrator)
- Media Access Code (MAC) address
- Internet Protocol (IP) address (if fixed)
- Hostname

[1] Note that this document is concerned only with the protection of information assets. Ownership of an information asset in this context implies only possession of the asset and does not infer any definition of copyright ownership or intellectual property ownership.

4.5. Software assets

The *CIO shall* maintain an inventory of all centrally licensed or owned commercial software. The following information *should* be maintained as part of the inventory.

- Software product
- Version
- Number of licensed copies
- Number of installed copies
- Owner or locations of installed copies

4.3.2. Information assets

Information assets *should* be assigned an information classification based on the sensitivity of the information they contain. The classification should be one of the following:

| Information Category | Description |
|---|---|
| *Public* | This category covers information intended for public consumption or that can be made public without any negative implications for the business activities or reputation of *Fincomp*. |
| *Internal* | This category covers information regarding the day to day business of *Fincomp* and is intended primarily for staff use. Some of the information in this category may be relevant for external parties who work closely with *Fincomp* (suppliers, business or partners etc) but external recipients would be expected to limit access to the information. The information would not be considered as of interest to the general public and therefore not appropriate for full public access, although public release would not cause serious reputational damage to *Fincomp*. |
| *Confidential* | This category covers information of a more sensitive nature for the business operations of *Fincomp*. The information represents *Fincomp's* basic intellectual capital and know-how. Access should be limited within the organisation to those people who "need to know" for the performance of their duties. |
| *Highly Confidential* | This category covers highly sensitive information that if released will cause significant damage to *Fincomp's* business activities or reputation or lead to a breach of the data protection act or similar legislation. Access to this information should be very restricted and the number of people who "need to know" will be relatively small. |

If an information asset includes information from different categories, it should be classified as the most sensitive category.

Each information asset *shall* have an owner. By default, the owner of information assets stored on *IT equipment shall* be the person responsible for the user account under which the asset is stored (i.e. the possessor of the asset). Where the assets of multiple owners are collected into a common data store not under the control of a single person (e.g. a database), an *Administrator shall* be assigned as the notional owner.

Owners or notional owners of information assets *should* classify the relative value of their assets. Risk analysis *should* be performed for all assets that are critical to the operation of the core functions of *Fincomp's* business.

### 4.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

### 4.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

### 4.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 5. Audit Policy

## 5.1. Purpose

To provide the authority for *Administrators* to conduct security audits on *IT equipment* in order to investigate security breaches or ensure compliance with the **Information Security Policy** or other legal or contractual requirements.

## 5.2. Scope

This policy applies to:

- All *Fincomp* owned or operated *IT equipment*.
- All third-party *IT equipment* permanently or temporarily connected to the *Fincomp network*.
- All *Users* of the above *IT equipment*.

## 5.3. Policy

### 5.3.1. Reasons for audit

Audits may be conducted to:

- Investigate known or suspected security breaches.
- Monitor conformance with the **Information Security Policy** and other legal or contractual requirements.

### 5.3.2. Authorised personnel

*Administrators may* conduct audits on any *IT equipment* within the scope of this policy. *Administrators may* request and *shall* expect assistance from *Users* responsible for the *IT equipment* being audited.

### 5.3.3. Limits of audit

The audit *should* only investigate those aspects of *IT equipment* related to its security functions and its compliance with policies and legal or contractual requirements.

### 5.3.4. Types of audit

***Security breach audit***

Where the audit is required to investigate a known or suspected security breach, an inspection of the *IT equipment* shall be made to attempt to discover how it was compromised and what damage was caused. The *User shall* facilitate access to the system for the auditor. Information collected by authorised network monitoring activities *may* also be used in conjunction with information collected during the audit to draw conclusions.

***Conformance audit***
Where the audit is required to show conformance with the **Information Security Policy**, the auditor *may* require that the *User* provides evidence that the *IT equipment* complies with the policy. An inspection of the *IT equipment* is *not required* unless the evidence requested is not provided or inconclusive. Automated auditing tools *may* be used in place of manual audits to facilitate the audit process. Information collected by authorised network monitoring activities *may* also be used to confirm or contest the evidence provided.

5.3.5. Audit follow-up
A report *shall* be produced by the auditor describing the findings of the audit and the required actions, if any, to recover from a security breach or ensure compliance with the **Information Security Policy**. An *Administrator* or the *User* responsible for the *IT equipment* *shall* complete all required recovery actions at the earliest opportunity.

Compromised or non-compliant computers *may* be disconnected from the network or have their network access restricted if their continued connection is deemed to present a serious and significant threat to the security or normal operation of the network or other *IT equipment* connected to the network.

5.3.6. Special situations
Special situations can be considered as follows:

- Where an audit is instigated at the request of a law enforcement agency investigating a criminal matter.
- Where there is a suspicion that child pornography is involved.
- Where a normal audit uncovers a potential criminal matter including child pornography.

In the above special situations detailed notes of the investigatory steps taken *must* be made and signed by the auditor on completion of the audit.

Where a normal audit uncovers a potential criminal matter or child pornography, the audit *must* be stopped immediately and the *IT equipment* quarantined, if possible, and the Police notified.

## 5.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 5.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

## 5.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 6. Data Backup Policy

## 6.1. Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. This policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

## 6.2. Scope

This policy applies to all data stored on *Fincomp's Information Systems*. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

## 6.3. Policy

### 6.3.1 System *Backups*

- The *company* share on Livedrive (the L drive) *must* be backed up daily and stored *on-site.*
- The contents of the *company's* MySQL database(s) *must* be backed up daily and stored on the L drive.
- The following directories on the *company's* Terminal *Server must* be backed up daily and stored on off-site cloud storage:
    - C:\Fincomp
    - C:\ProgramData\Sage\Accounts\2012\Company.000\ACCDATA
- The contents of the *company's* website(s) *must* be backed up monthly and stored on the L drive.
- Image backups of the *company's* Terminal *Server must* be made monthly and stored *on-site*.
- The contents of the following programs *must* be backed up monthly and stored on the L drive:
    - Sage
    - Fincomp Database
    - HMRC Basic Tools
- The configurations of *company* router(s) *should* be backed up when configuration changes are made and stored on the L drive.

Note that no *Single-User computer equipment* is backed up. *Users* are responsible for moving all critical data to the L drive.

6.3.2 Responsibilities

- The *CIO must* ensure facilities are available and *shall* take overall responsibility for trust adherence to this policy.

- *Administrators must* check the backup logs for completion, be responsible for the safekeeping and availability of all back-up media and logs and perform actual/test restores.

- *Administrators must* log any backup failures and investigate any reported exceptions.

6.3.3 Backup Retention

- Daily backups *should* be maintained for a period of 30 days
- Monthly backups *should* be maintained for a period of 3 months

6.3.4 Disposal of *Backup Media*
Prior to retirement and disposal, *Administrators must* ensure that:

- The media no longer contains active backups
- The media's current or former contents are irretrievable by ordinary commercially available means.

With all backup media, an *Administrator must* ensure the physical destruction of media prior to disposal.

6.3.5. Verification
On a daily basis, logged information generated from each backup job *should* be reviewed for the following purposes:

- To check for and correct errors.
- To monitor the duration of the backup job.
- To optimise backup performance where possible.

An *Administrator* will identify problems and *must* take corrective action to reduce any risks associated with failed backups.

Random test restores *should* be done once a month in order to verify that backups have been successful.

*Administrators must* maintain records demonstrating the review of logs and test restores so as to demonstrate compliance with this policy for auditing purposes.

6.3.6. Data *Recovery*
In the event of a catastrophic system failure, off-site backed up data will be made available to *Users* within 3 working days if the destroyed equipment has been replaced by that time.

In the event of a non-catastrophic system failure or *User* error, on-site backed up data will be made available to *Users* within 1 working day.

6.3.7 *Restoration* Requests
In the event of accidental deletion or corruption of information, requests for restoration of information *must* be made to an *Administrator*.

## 6.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 6.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

*Backup* means to copy data to a second location, solely for the purpose of safe keeping of that data.

*Backup Media* means any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

*Restoration* means the process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

*Recovery* means the process of thinking restored data ready for use by systems, applications, and *Users*.

## 6.6. Enforcement

Any *Administrator* found to have violated this policy may be subject to disciplinary action.

# 7. Data Retention, Archiving and Destruction Policy

## 7.1. Purpose

To set out the principles for retaining, archiving and destroying *Personal Data* to ensure that we only keep it for as long as is necessary for the purposes for which it was collected or for which it is to be further processed (unless there is a legal reason for us to keep it longer).

## 7.2. Scope

This policy applies to all *Users*. Goods and services providers are also expected to introduce and follow appropriate data retention practices.

This policy covers all *Personal Data* retained or in *Fincomp's* custody or control in whatever medium such data is contained in. This policy is not therefore restricted to information contained in paper documents but includes data contained in an electronically readable format. For the purposes of convenience, in this policy, the medium which holds data is called: "a Document".

## 7.3. Policy

### 7.3.1. Responsibilities

- All *Users must* report any breaches or suspected breaches of this policy to an *Administrator*.

- *Users must* return Documents in their possession or control to *Fincomp* upon separation or retirement.

### 7.3.2. *Retention*

*Fincomp* will keep some Documents for longer than others. Documents *shall not* be kept indefinitely, unless there are specific requirements. In line with principle 5 of the Data Protection Act (1998), Documents *shall not* be kept longer than is necessary.

The **Personal Data Retention Schedule**, gives a breakdown of timescales for the retention of the various types of Documents *Fincomp* processes. The maximum retention period for a Document is two (2) years. Exceptions to the documented retention period and the maximum retention period *may* been granted by the *CIO* under section 7.3.5.

After active use has expired and according to appropriate exceptions, Documents *shall* be archived in accordance with section 7.3.3 until the Documents are destroyed in accordance with section 7.3.4.

Documents used in staging, development, and testing or draft versions of Documents *shall not* be retained beyond their active use period nor copied into production or live environments.

7.3.3. *Archiving*
Paper Documents *shall* be archived in secured storage *onsite*, clearly labelled in archive boxes naming the contents and date to be destroyed.

Electronic Documents *shall* be archived to a secure area on a dedicated *onsite* file *server* in folders which clearly name the contents and date to be destroyed. They *must* be stored in a format appropriate to secure the confidentiality, integrity and accessibility of the Documents.

The **Personal Data Retention Schedule**, gives a breakdown of timescales for the archiving period of the various types of Documents *Fincomp* processes. The maximum archiving period for a Document is seven (7) years. Exceptions to the documented archiving period and the maximum archiving period *may* been granted by the *CIO* under section 7.3.5.

After the archiving period has expired, Documents *shall* be destroyed in accordance with section 7.3.4.

7.3.4. *Destruction*
Destruction of Documents *must* be performed by an *Administrator* and *must* be documented.

7.3.5. Exceptions to the retention and archiving periods
The *CIO may* grant exceptions to the retention and archiving periods but *must* justify and document each exception. The justifiable reasons for exceptions are:

- a client requirement;
- business requirement;
- legal requirement; or
- vital historical purpose.

## 7.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy** and **Personal Data Retention Schedule**.

## 7.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

*Retention* means the maintenance of documents in a production or live environment which can be accessed by a *User* in the ordinary course of business.

*Archiving* means the secured storage of Documents such that Documents can only retrieved by an *Administrator*.

*Destruction* means physical or technical destruction sufficient to render the information contained in the Document irretrievable by ordinary commercially available means.

7.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 8. Email Policy

## 8.1. Purpose

To establish the requirements for safe use of electronic mail (email).

## 8.2. Scope

This policy applies to all *Users* who send or receive email via the *Fincomp* email system.

## 8.3. Policy

### 8.3.1. *Administrator* responsibilities

All email entering or leaving the *Fincomp* email system *sha*ll pass through an email filtering service operated by an *Administrator*. Emails travelling entirely within the *Fincomp* email system are *not required* to pass through the email filtering service.

The email filtering service *shall* provide automated scanning of email to detect potential *malicious code* and to identify *spam*.

*Malicious code* signatures, *spam* identification rules, blacklists and other mechanisms required by email scanning tools to identify new or modified threats *must* be kept up-to-date.

***Detection of malicious code***

Email items or attachments identified as containing *malicious code* or suspected of containing *malicious code shall* be prevented from reaching the intended recipient. The intended recipient of an infected or suspected email *should* be informed that the email did not reach its destination.

***Identification of spam***

Email items identified as *spam* or suspected of being *spam shall*, where possible, be quarantined before reaching the intended recipient's mailbox. Quarantined email items shall be reported to the intended recipient at regular intervals so that they may confirm the items have been classified correctly. Incorrectly quarantined email items *shall* be released to the intended recipient when requested.

### 8.3.2. *User* responsibilities

*Malicious code* is developed and released on a regular basis. *Users must* remain vigilant for new threats which automated scanning tools may not yet be able to detect.

*Users must not* create or modify *malicious code*.

Users *must not* knowingly send *malicious code* through *Fincomp's* email system or otherwise allow it onto the *Fincomp network* by other means.

*Users must not* send, forward or otherwise distribute *spam* or chain letters.

Email attachments from unknown sources *must* be scanned for *malicious code* before being opened.

Since some *malicious code* can fake the sender of an email, messages from known senders that are unexpected or in any way unusual *should* be scanned for *malicious code* before being opened.

*Users must not* configure their *Fincomp* email accounts to automatically forward email to services not operated by *Fincomp*.

Users conducting *Fincomp* business or communications via email *must* use a *Fincomp* provided email account. Personal email accounts *must not* be used for conducting *Fincomp* business or communications.

***Phishing***
*Phishing* is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or fellow *Users* are commonly used to lure the unsuspecting. *Phishing* is typically carried out by e-mail or instant messaging, and it often directs *Users* to enter details at a fake website whose look and feel are almost identical to the legitimate one.

## 8.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**, **Password Policy**, and **Email Usage Policy**.

Further information on *phishing* can be found at the Anti-Phishing Working Group (APWG).

## 8.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

*Malicious code* means as any executable, script, macro or other programmable feature that has the potential to damage, control or otherwise compromise the security of a *user's* computer. This includes viruses, trojans, worms and spyware.

*Spam* means as indiscriminate, unsolicited, bulk commercial email. It is often about subject matter that is of no interest, or offensive, to the intended recipient.

*Phishing* is a targeted email that requests information such as usernames and passwords from the *user* purporting to come from a source of authority.

## 8.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 9. Encryption Policy

## 9.1. Purpose

To define the minimum requirements for the safe encryption of data

## 9.2. Scope

This policy applies to all *Users* of *Fincomp's IT equipment*.

## 9.3. Policy

Encryption is the process of disguising data so as to hide its substance from any casual observer gaining access to it. This is done by applying a mathematical function, known as a *cryptographic algorithm* or *cipher*, to the data to render it unreadable. A mathematical function that reverses the encryption process is used to decrypt the data. One or more unique *keys* is used in conjunction with the cipher to perform the encryption or decryption.

### 9.3.1. General

- Data that is classified as *confidential*, as defined in the **Asset Management Policy**, *should* be encrypted.
- Data that is classified as *highly confidential*, as defined in the **Asset Management Policy**, *shall* be encrypted.
- Data requiring an integrity guarantee *should* be encrypted.
- *Users* requiring strong authentication of a person, service or data item *should* use encryption as part of the authentication technique.

### 9.3.2. Encryption strength

Only tools and products based on proven, mathematically sound *cryptographic algorithms*, subjected to peer review by the cryptographic community, *shall* be used for encryption.

For block ciphers, a minimum symmetric key length of 128 bits *should* be used. For long term security a symmetric key length of 256 bits is *recommended*. For public key ciphers, a minimum asymmetric key length of 2048 bits *should* be used. For long term security an asymmetric key length of 4096 bits is *recommended*.

All keys *shall* be stored safely. Where a key is secured by use of a pass phrase, the *pass phrase shall* be at least 12 characters in length.

The requirements and recommendations for password selection and password protection described in the **Password Policy** *shall* apply for pass phrases.

9.3.3. Ciphers and products

The following ciphers are *recommended* for use on *Fincomp IT equipment*:

- *Block Ciphers*: 3DES, IDEA, RC5, AES, CAST, Blowfish
- *Public Key Ciphers*: RSA, Diffie-Hellman
- *Hash Functions*: MD5, SHA

The following products are *recommended* for use on *Fincomp* IT equipment:

- Remote Access: SSH, IPSec, L2TP and PPTP VPNs.
- Web Security: SSL
- Email: Pretty Good Privacy (PGP), TLS, Authenticated SMTP
- File Security: PGPDisk

Note that some of the above ciphers and products contain patented algorithms or methods which may require the purchase of a suitable licence.

## 9.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 9.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

- A *cryptographic algorithm* or *cipher* is a mathematical function applied to data to make it unreadable to a casual observer.
- A *block cipher* is a cipher that is applied to a block of data (a number of characters or bits) at the same time. This is different from older ciphers which are applied to a single character at a time.
- A *public key cipher* is a cipher that uses different keys for encryption and decryption. A public key is used for encryption and a private key is used for decryption. The public key cannot be used to decrypt the data and so can be freely published or given to correspondents that need to send you confidential data.
- A *hash function* is a cipher that produces a unique sequence of characters or numbers (the hash) for any different collection of input data. A hash function can be used to verify that the data has not changed since the hash was generated.
- A *key* is a sequence of characters or numbers, like a password, that is used with a cipher to encrypt or decrypt data.
- A *pass phrase* is a sequence of characters or numbers, like a password, that is often used to gain access to a stored key.

## 9.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 10. Network Monitoring Policy

## 10.1. Purpose

To establish the requirements for monitoring, logging and retention of traffic on the *Fincomp network*.

## 10.2. Scope

This policy applies to:

- All *IT equipment* connected to the *Fincomp network*.
- All *Users* of the above equipment.

*Users* should also be aware that the **Audit Policy** allows for the auditing of *IT equipment* to investigate security breaches and monitor compliance with policy.

## 10.3. Policy

The Regulation of Investigatory Powers Act (2000) allows *Administrators* to monitor network traffic for operational and security reasons.

Specifically, *Administrators may* intercept network traffic without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime, gross misconduct or unauthorised use, and ensuring the efficient operation of *Fincomp* communications systems.

The primary aims of network monitoring are:

- To maintain the integrity and security of the *Fincomp network*, *IT equipment* and information assets.
- To collect information to be used in network design, engineering, trouble- shooting and usage-based accounting.

## 10.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy** and the **Audit Policy**. This policy complies with the requirements of the Regulation of Investigatory Powers Act (2000).

## 10.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

## 10.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 11. Password Policy

## 11.1. Purpose

To establish minimum standards for password selection and use.

## 11.2. Scope

This policy applies to all *Users* of *Fincomp IT equipment*.

## 11.3. Policy

### 11.3.1. General

All *IT equipment* that supports an access control mechanism based on user accounts and passwords or PINs *shall* have the mechanism enabled.

User accounts *must* have a password or PIN set.

Passwords *must* contain at least seven characters. It is *recommended* however that passwords contain at least twelve characters to reduce the chance of compromise by a brute-force password-cracking attack.

Passwords *shall* contain a combination of numbers, and upper and lower-case letters.

If the access control mechanism allows it, a password *should* contain at least one special character (e.g. underscore, dollar, ampersand).

Passwords *must not* be words found in a dictionary, personal information that can be associated with the owner (e.g. birthdays, telephone numbers) or simple patterns (e.g. abc123).

The *recommended* process for choosing a password is:

- Think of a memorable phrase on which to base the password.
- Replace words by meaningful numbers or special symbols (e.g. to, too = 2, for = 4, and = &, money, cash = £).
- Use the first letters of the remaining words in the phrase.
- Capitalise some of the first letters.
- Replace letters by numbers or special characters that look similar (e.g. I = 1, o = 0, s = 5 or $).

Examples:

- aPi4Lnj4C = a puppy is for life not just for Christmas
- Tl0£iTr0aE = The love of Money is the root of all evil

Passwords for *Users must* be changed every 180 days.

11.3.2. Multiple accounts
*Users* with multiple user accounts for different services or multiple computers *should* set a different password for each account. *Users should not* use the same passwords for *Fincomp* and non-*Fincomp* user accounts. This will limit the damage should any one user account be compromised.

11.3.3. User password protection
*Users must not* reveal their own passwords to anyone except *Administrators*.

All passwords *must* be treated as sensitive, confidential *Fincomp* information.
If someone demands a password, refer them to this document or have them contact an *Administrator*.

*Users must not* store passwords in a file on any computer without encryption.

*Users must not* write down or store passwords in any location easily accessible to others.

11.3.4. System password protection
*IT equipment* access control mechanisms *shall* enforce the password length, password complexity and password change requirements detailed in section 11.3.1 to ensure *user* compliance.

In addition, *IT equipment* access control mechanisms *shall* further limit the risk of password compromise by enabling the following features where available:

- Password History Control: The access control mechanism *must* prevent the reuse of a *user's* last eight passwords.
- Account Lockout: The access control mechanism *shall* prevent any further logins after three failed login attempts. The lockout *should* be for a fixed period of time or until the account is reset.
- Concurrent Connections: The access control mechanism *shall* prevent an excessive number of concurrent connections by the same *User* above and beyond those reasonably required to access authorised and necessary *Information Systems*.
- Grace Logins: The access control mechanism *should* allow the *User* seven login opportunities to change their password when the password age limit is reached after which the account *should* be locked.

## 11.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**, and **Email Policy**.

## 11.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

## 11.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 12. Physical Security Policy

## 12.1. Purpose

To establish the requirements for physical security of *information systems*.

## 12.2. Scope

This policy applies to:

- All *Fincomp* owned or operated *information systems*.
- All *Third-party IT equipment* located *on-site*.

## 12.3. Policy

### 12.3.1. Location of Information Systems

*Information systems should* be housed in a secure area protected by a defined security perimeter with entry controls.

***Secure areas***

A secure area *shall* be a room or building with a clearly defined security perimeter. The security perimeter, usually the walls, windows and doors of the room or building, *shall* act as a physical barrier between the secure area and any unsecured areas preventing access except through designated entry control points. The security perimeter *should* be physically sound to prevent possible break-in.

***Entry controls***

An entry control *shall* be a mechanism for limiting access to a secure area to authorised personnel only. An entry control *may* be a lockable door, a smart card entry system or a staffed reception area.

### 12.3.2. Access to IT equipment

Entry control mechanisms *should* be enforced at all times when *IT equipment* is left unattended. Where *IT equipment* is left unattended for significant periods (e.g. overnight or at weekends), additional security measures such as door or window alarms or motion detectors *may* be used.

Unauthorised personnel *should* be permitted into secure areas only when accompanied by authorised personnel.

### 12.3.3. Protection of IT equipment

Secure areas *shall* be operated and maintained so as to minimize the risk from theft, fire, explosion, smoke, water, dust, vibration, chemical effects, electrical supply interference or radiation.

***Backups***
*IT equipment* containing critical or important information assets *shall* have those assets backed according to the **Data Backup Policy**.

***Power supply***
*IT equipment* performing critical services or containing critical information assets *should* be fitted with an uninterruptible power supply to allow continued operation or controlled shutdown in the event of electrical supply interruption.

***Maintenance***
*IT equipment should* be maintained in accordance with the supplier's recommended service intervals and specifications.

12.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy** and **Data Backup Policy**.

12.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

12.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 13. Server Security Policy

## 13.1. Purpose

To establish minimum security standards for the configuration of *servers*.

## 13.2. Scope

This policy applies to all *Fincomp servers*.

## 13.3. Policy

### 13.3.1. Ownership and administration

*Servers* that provide critical or company-wide services in support of business functions *shall* be configured and maintained by *Administrators*.

*Administrators must* keep abreast of security issues for the operating systems, services and applications. They *shall* be expected to subscribe to any freely available email or other service that provides them with timely information on security issues or patches.

*On-site servers shall* be located in secure areas as described in the **Physical Security Policy**.

### 13.3.2. *Server* configuration requirements

- *Servers shall* be configured with a currently supported version of the operating system. Currently supported means that the manufacturer provides security patches or critical updates that protect against new vulnerabilities and that the version has not been designated as 'end of life'.
- *Servers shall* be configured with currently supported versions of software. Currently supported means that the manufacturer or developer provides security patches or critical updates that protect against new vulnerabilities in a timely manner.
- *Servers shall* be configured to provide only the services and resources for which they are intended. Services and applications that will not be required *must* be disabled.
- *Servers* that provide access to services, resources or information that is not intended for general public access *shall* be protected by access-control mechanisms (e.g. passwords, firewalls). Access *shall* be restricted to authorised *Users* only.
- If a *server* or service provides a logging mechanism, access to the service *shall* be logged in accordance with the **Network Monitoring Policy**.
- Security patches *must* be installed on the system as soon as is practical. The only exception to this requirement is when immediate installation would interfere with business requirements or adversely affect the service being offered.
- The principle of "least required access" *shall* be used to provide services and resources.
- Services *shall* be run from non-privileged rather than *administrator* accounts where it is feasible to do so.

### 13.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**, the **Physical Security Policy** and the **Network Monitoring Policy**.

### 13.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

### 13.6. Enforcement

Any *User* found to have violated this policy may be subject to disciplinary action.

# 14. Single-User Computer Equipment Security Policy

## 14.1. Purpose

To establish minimum security standards for the configuration of *single-user computer equipment*.

## 14.2. Scope

This policy applies to:

- All *single-user computer equipment* connected to the *Fincomp network*.
- All *single-user computer equipment* that is (from time to time) connected to the *Fincomp network*.
- All *single-user computer equipment* not connected to the *Fincomp network* but containing Fincomp related business data.
- All *Users* of the above equipment.

## 14.3. Policy

### 14.3.1. Ownership and administration

*Administrators* are responsible for information security issues on all *single-user computer equipment*.

*Users* of *single-user computer equipment must* inform an *Administrator* of any known or suspected security-related problem with the equipment.

*Users must* keep abreast of security issues for the operating systems they are using. They *shall* be expected to keep up to date with security announcements made by *Administrators*.

*Users should* be aware that *mobile computers* are at greater risk of exposure to security threats than fixed location computer equipment permanently connected to the *Fincomp network*. The reasons for this include:

- Maintaining the physical security of a *mobile computer* in-transit or locations outside *Fincomp's offices* may be more difficult.
- Theft or loss of *mobile computers* is more likely, increasing the risk of unauthorized access to data stored on them.
- *Mobile computers* may be connected to home or Third-party networks that are less secure than the *Fincomp network* leading to higher risk of exposure to malicious attack.

*Single-user computer equipment should* be located in secure areas, as described in the **Physical Security Policy**, whenever possible.

14.3.2. *Single-user computer equipment* configuration requirements

- *Single-user computer equipment shall* be configured with a currently supported version of the operating system. Currently supported means that the manufacturer provides security patches or critical updates that protect against new vulnerabilities and that the version has not been designated as 'end of life'.
- *Single-user computer equipment shall* be configured with currently supported versions of software. Currently supported means that the manufacturer or developer provides security patches or critical updates that protect against new vulnerabilities in a timely manner.
- *Single-user computer equipment shall* be configured to provide only the services and resources required by the *Users*. Services and applications that are not required *must* be removed or disabled.
- Information, services or resources that are not intended for general public access *shall* be protected by access-control mechanisms (e.g. passwords). Access *shall* be restricted to authorised *Users* only.
- If the *single-user computer equipment* provides a security event logging mechanism, this mechanism shall be turned on to assist auditing.
- If the *single-user computer equipment* provides other event logging capabilities, this mechanism *should* be turned on to assist with problem diagnosis.
- Security patches *must* be installed on the system as soon as they are available. If an automated facility to check for patches and updates is available, it *should* be used. The only exception to immediate patching is when this would adversely affect an application or service in use by a *user*.
- Services *shall* be run from non-privileged rather than administrator accounts where it is feasible to do so.

14.3.3. Mobile usage requirements

*Fincomp* does not require staff to store or access confidential information using computing devices that it does not own or manage. Should *Fincomp* require one of its staff members to use a mobile or home computing device to store or access confidential data, a suitably configured *Fincomp* owned device *shall* be provided.

*Mobile computers* are subject to the same general requirements as fixed location *personal computers*.

Access control mechanisms (e.g. passwords, PINs) *must* be used at all times to prevent unauthorised access to *mobile computers*. If the access control mechanisms are equipped with time-out protection such as automatic log-out or password protected screen locking, these *shall* be implemented. Where possible these *may* be implemented through administrative policies.

Personal firewalls provided as part of the operating system or a security suite *shall* be turned on and configured to allow only required programs and services.

Mobile communication services such as wireless networking, Bluetooth or infrared *should* be disabled when not in use.

Disk encryption *must* be used to protect *highly confidential* data as defined in the **Asset Management Policy**.

Physical security devices, such as laptop cable locks, *should* be used to protect *mobile computers* from theft when outside of secure areas.

*Fincomp* owned mobile devices may be remotely wiped following report of loss where this service capability exists to *Administrators*.

### 14.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**, the **Physical Security Policy**, the **Encryption Policy** and the **Asset Management Policy**.

### 14.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

A *mobile computer* is a *laptop, mobile phone, handheld device* or other item of easily moveable *computer equipment*.

### 14.6. Enforcement

Any *User* found to have violated this policy *may* be subject to disciplinary action.

# 15. Third-Party access Policy

## 15.1. Purpose

To establish expectations for *third-parties* and contractors about maintaining the security of *Fincomp's information systems*.

## 15.2. Scope

This policy applies to all *third-parties* working on *information systems* belonging to or provided for the *Fincomp* including *formally* or *informally* outsourced services. It also covers:

- Guest-access to *Fincomp's* systems
- Third-party support, maintenance & development

## 15.3. Policy

### 15.3.1. Risk

In the absence of control or accountability by *Fincomp*, there is a degree of risk associated with entrusting information to *third-parties*.

- Who may have access to the data
- How user data is used
- Where user data is stored
- Security of user data
- Availability in the short, medium & long term
- Whether user data is recoverable in the event of a disaster
- Availability of support in the event of a problem
- How the facility may change in terms of the user interface or nature of the service

### 15.3.2. Managing risks

Use of *informally outsourced* services to store sensitive or *personal data* may be in breach of the Data Protection Act (1998).

*Informally outsourced* services *must not* be approved or promoted for handling confidential information.

An assessment of the potential impact to *Fincomp* that could result from the *third-party* suffering or causing a problem *should* be carried out.

European Union law requires that *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*.

The *third-party must* agree to follow *Fincomp's* **Information Security Policy**.

15.3.3. Guest access by third-parties
Where *third-parties* are providing support and maintenance, *Fincomp's information systems* it may be necessary for them to access these systems at the highest level of privilege. It is essential that:

- All such privileged access to or via *Fincomp network* is approved by an *Administrator*
- An *Administrator* is responsible for managing the access in terms of scope, level and duration. All access by *third-parties* should be monitored or logged.
- Remote access to *information systems* must only be permitted via secure encrypted network protocols.
- The *third-party should* provide *Fincomp* with the code of practice that their staff or agents must follow when handling the customer's information. It is preferable that this code of practice forms part of the agreement with the *third-party* for provision of service

*Users must not* permit information security safeguards and policies to be bypassed or allow inappropriate levels of access to *Fincomp's information systems*.

Any access to *information systems* provided to *third-parties* must follow recognised procedures.

## 15.4. Related policies, standards and guidelines

This policy *should* be read in conjunction with the **Information Security Policy**.

## 15.5. Terms and definitions

All words or phrases shown in italics are policy terms. Definitions for policy terms not specifically given in this section can be found in **Appendix B** of the **Information Security Policy**.

*Third-parties* are external organisations or individuals other than *Users*.

*Informally outsourced services* are services provided by *third-parties* for which there is no formal bilateral agreement or control over data (e.g. Gmail)

*Formally outsourced services* are services provided to *Fincomp* by *third-parties* and subject to a formal bilateral agreement or contract, with clear understandings setting out standards and expectations regarding information security.

15.6. Enforcement

Any *user* or *administrator* found to have violated this policy *may* be subject to disciplinary action.

Contracts and agreements with Third-parties *should* include means for redress by *Fincomp* in the event of a dispute.