Information Security, Acceptable Use and Access Control Policy

Mirats Insights, LLC

1. Introduction

1.1 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and information assets at the Company. These rules are in place to protect Mirats Insights and all employees/contractors. Inappropriate use exposes the Company to risks including unauthorised disclosure of information, virus attacks, compromise of network systems and services, and potential legal issues.

1.2 Definition of Information Security

Information security encompasses the management processes, technology and assurance mechanisms that will allow business to trust their transactions (integrity), the information is usable and can appropriately resist and recover from failures due to error, deliberate attacks or disaster (availability), and that confidential information is withheld from those who should not have access to it (confidentiality).

1.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Company.

1.4 Communication

Awareness of this policy will be included in all induction training for new Mirats Insights staff and will be included as appropriate on refresher training courses for existing staff.

All employees will be requested to sign-off this policy on an annual basis (unless otherwise determined by executive management) and copies will be placed on personal files for record keeping purposes.

All new employees will receive a copy of this document together with the job offer and nondisclosure agreement and be requested to hand over a signed copy on the first day of employment.

1.5 Policy review

This policy will be reviewed annually.

2. The Internet and E-mail Policy

The Internet is a very large, publicly accessible network that has millions of connected users and organisations worldwide. One popular feature of the Internet is e-mail.

2.1 Policy

Access to the Internet is provided to employees for the benefit of Mirats Insights and its customers.

Employees are able to connect to a variety of business information resources around the world. Mirats Insights provides its users with Internet access and electronic communications services as required for the performance and fulfilment of job responsibilities. These services are for the purpose of increasing productivity and not for non-business activities.

In order to ensure the continuous availability and usability of the e-mail system, it is necessary to implement the following controls:

a) Mailbox sizes are limited to 30GB per e-mail account. Users will be informed automatically when they reach 30GB in capacity. Once the threshold is reached, sending of e-mails will not be allowed. On reaching 30GB both sending and receiving facilities will be suspended. Please note that this is a system enforced policy and therefore all employees should manage their e-mail accounts (download to workstation for regular back-ups). All members of the executive team will be treated on an individual basis.

b) All emails are processed and stored by an external mail solution for security, archiving, compliance and other required corporate purposes. The current solution is provided by Google Workspace.

c) Outgoing mails will be limited to 25Mb per mail no matter when it is send. Only the Google Drive and the local authorized user computers may be used for storing company data. Any synchronisation of personal files while on the corporate network is may be monitored.

The Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the company's interests, the following guidelines have been established for using the Internet and e-mail.

2.2 Acceptable Use

Employees using the Internet are representing the company. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Occasional and reasonable personal use of Mirats Insights's Internet and e-mail services is permitted, provided that this does not interfere with work performance. These services may be used outside of scheduled hours of work, provided that such use is consistent with professional conduct.

Accessing and communicating on social networks such as Facebook is done on a reasonable usage basis. Staff are entrusted to ensure that any social media usage does not impact negatively on their work. Staff are responsible and accountable for posting any content to social media or other public forums that may be associated with the company in any way. It is a serious breach of this policy to post items to social media that may bring the company into disrepute or affect its public profile negatively in any way.

Information passing through or stored on company equipment and infrastructure can and will be monitored. Examples of acceptable use are:

a. Using Web browsers to obtain business information from commercial Web sites.

b. Accessing databases for information as needed.
c. Using e-mail for business contacts.
d. Using company issued mobile devices and smart phones for business purposes.

2.3 Unacceptable Use

Employees must not use the Internet for purposes that are illegal, unethical, harmful to the company, or non-productive. Examples of unacceptable use are:

a. Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
b. Create and/or send "spam." Spam is defined as any unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication. It will be considered a greater offence if the company's electronic communications resources are exploited to amplify the range of distribution of these communications.
c. Conducting personal business using company resources. Internet banking is considered acceptable use.
d. Accessing, downloading, uploading, saving, receiving, or sending material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent, or defamatory language.
e. Accessing and or listening to radio and streaming non work related content over the Internet, as such activities severely degrade bandwidth and in so doing hampers the overall productivity of the company
f. “Testing” the security configuration of Mirats Insights in any way whatsoever (vulnerability scans by itself may contain harmful code thus exposing Mirats Insights to serious breaches in security).
g. Bypass the proxy server that provides access to the Internet (this may introduce malicious code and breach the security setting of Mirats Insights)

h. Have simultaneous dual connections for example through the network cable and a wireless modem (such connection will bypass the Mirats Insights firewall, interconnecting the Mirats Insights secure network with the non-secure Internet).

2.4 Employee Responsibilities

Non work related file downloads from the Internet are not permitted unless specifically authorised by the applicable Line Manager

2.5 IT Department Responsibilities

The IT Department shall ensure that all staff members have access to e-mail facilities. This involves creating mailboxes. In the creation of mailboxes IT shall:

a. Ensure that no one other than the user will have access to that mailbox.
b. Ensure that the format of the e-mail address is consistent with the company standards e.g. firstname.lastname@miratsinsights.com
c. Mirats Insights aligns itself to the latest compliance as provided in India and USA and also in line with the appropriate legislation and regulations of India, or other locations as it may deem relevant. Upon written approval from the CEO and/or Head of Global Sales, The IT Department will be allowed access to any employee's e-mail, internet usage logs, or other historic electronic information.
d. Implement technical controls to enforce the policy requirements as stipulated above.
e. India's and/or USA's regulation as per point c) above applies to all employees operating under the jurisdiction of Indian and USA legislation. However, the same principle will apply in all other countries where there is a valid legal requirement (e.g. a police investigation) that requires access to a specific individual's computer or mobile device and the information stored on it.

2.6 Employee Responsibilities

An employee who uses the Internet or e-mail shall:

a. Read their E-mails regularly.

b. Ensure that all communications are for official purposes and that they do not interfere with his/her productivity. E-mail messages of a personal nature (selling goods, advertising meetings, etc) should only be issued in accordance with the standard procedures determined by People's Department Head for all such communications.

c. Know and abide by all applicable company policies dealing with security and confidentiality of company records and information.

d. Avoid transmission of non-public (sensitive) customer information. If it is necessary to transmit non-public information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorised to receive such information for a legitimate use.

e. Not download and/or distribute pornographic or other offensive material from the Internet and/or Email. Users found downloading any forms of pornography or other offensive material will be liable to disciplinary action (as per the normal People's Disciplinary Procedures). Participating in the download or distribution of any form of pornographic material involving children is a criminal offence and must by law, be reported to the Police Services.

f. Report the receipt of pornographic or offensive material to IT Department and the Information Security Officer. Users who fail to report will be liable to disciplinary action.

g. Not download non-work related data or applications from the Internet.

h. Use file compression services (ZIP, RAR) to decrease file sizes before transmission over the network.

2.7 Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the organisation and/or legal action by the copyright owner. Please bear in mind that approval has to be obtained from the IT Department to load/save any software not forming part of the Mirats Insights standard.

2.8 Monitoring

All messages created, sent, or transferred over the Internet and/or Intranet is the property of the company. Mirats Insights reserves the right to access the contents of any messages sent over its facilities if the company believes, in its sole judgment, that it has a business need to do so or where there is suspicion of abuse. All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

3. MOBILE DEVICE SECURITY

3.1 Background

The general use of mobile devices for business purposes has increased considerably over the recent past. Mobile devices include, but are not limited to, notebook computers, Tablet PCs, smart phones, compact discs, DVD discs, memory sticks, USB drives, and other similar devices. Small, powerful and connected to essential enterprise information, mobile devices have been embraced by professionals and are fast becoming a standard enterprise productivity tool. It is precisely this small size and enterprise connectivity, however, that make the mobile device a potential risk to the enterprise. While they may contain vital data similar to a desktop or laptop, mobile devices are far more vulnerable to loss, theft or malicious use.

3.2 IT Responsibilities

a. Provide mechanisms and procedures to protect mobile devices against a breach of confidentiality (encryption, authentication and self-destruct function).
b. Establish reporting channels and incident handling in the event of a compromise.
c. Ensure that all devices are cleaned (data removed) before disposal or when switching users.
d. Provide mechanisms to protect against malicious code and general viruses.
e. Ensure that all devices are scanned before being allowed access to the Mirats Insights network.
f. Provide user education on the secure use of mobile devices.

3.3 Employee Responsibilities

a. All mobile devices must be password protected. Choose and implement a strong password – please refer to the section later in the document on the selection and use of strong passwords.

b. The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out of-sight.

c. If a mobile device is lost or stolen, promptly report the incident to the IT Department Help Desk and proper authorities.

d. Sensitive or confidential documents, if stored on the device, should be encrypted if possible.

e. Mobile device options and applications that are not in use should be disabled (for example Bluetooth or Wireless).

f. Sensitive and confidential information should be removed from the mobile device before it is returned, exchanged or disposed.

g. Whenever possible all mobile devices should enable screen locking and screen timeout functions.

h. No personal information shall be stored on mobile devices unless it is encrypted and permission is granted by the data owner.

i. Before a mobile device is connected to Mirats Insights IT systems, it shall be scanned for viruses (the user risks having files on the device deleted if any viruses are detected).

j. If media mobile device is used for transitional storage (for example copying data between systems), the data shall be securely deleted from the mobile device immediately upon completion.

k. Information stored on memory sticks shall be protected by using strong passwords and/or encryption technologies. Sensitive information on memory sticks may only be removed from the premises if approved by the information/data owner.

l. Just as with static devices (e.g. desktop computers), user remain responsible to ensure that the information is backed-up and available as and when required.

4. COMPUTER VIRUS POLICY (MALICIOUS CODE)

Background: Computer viruses are programs designed to make unauthorised changes to programs and data. Therefore, viruses can cause destruction of corporate resources. It is the responsibility of everyone who uses Mirats Insights's computer networks to take reasonable measures to protect the network from virus infections. This policy outlines how various viruses can infect Mirats Insights's network, how Mirats Insights's IT Department tries to prevent and/or minimise infections, and how Mirats Insights's network users should respond to a virus if they suspect one has infected Mirats Insights's network or their computers.

There are mainly three types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. When an infected file is opened from a computer connected to Mirats Insights's network, the virus can spread throughout the network and may do damage. A Trojan horse is an actual program file that, once executed, doesn't spread but can damage the computer on which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run. Viruses can enter Mirats Insights's network in a variety of ways, such as:

a) E-mail: By far, most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect Mirats Insights's network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know that his or her computer is infected.

b) Disk, CD, USB flash disk, or other media: Viruses can also spread via various types of storage media. As with e-mail attachments; the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.

c) Software downloaded from the Internet: Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.

d) Instant messaging attachments: Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software. It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defences against computer viruses include protection against unauthorised access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

4.1 IT Responsibilities

The IT Department shall:

a) Install and maintain appropriate antivirus software on all computers.

b) Install and maintain appropriate gateway and e-mail antivirus software.

c) Install and maintain appropriate antivirus software on all file servers.

d) Routinely updating virus definitions: Every morning, the computer antivirus software and server virus scanning programs check the Internet site for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated.

e) Configure anti-virus software to notify and inform the IT support staff of detected viruses.

f) Respond to all virus attacks, destroy any virus detected, and document each incident.

4.2 Employee Responsibilities

Even though all Internet traffic is scanned for viruses and all files on the company's servers are scanned, the possibility still exists that a new or well hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect Mirats Insights's network. The IT staff will attempt to notify all users of credible virus threats via e-mail or telephone messages. Because this notification will automatically go to everyone in the organisation, employees should not forward virus warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic. As stated, it is the responsibility of all Mirats Insights network users to take reasonable steps to prevent virus outbreaks. The following guidelines will assist you in minimising the risk of virus infections:

a) Do not knowingly introduce a computer virus into company computers.

b) Do not load disks/flash drives of unknown origin & incoming disks/flash drives shall be scanned for viruses before they are read.

c) If a file you receive contains macros that you are unsure about, disable the macros.

d) Never open an e-mail or instant messaging attachment from an unknown or suspicious source.

e) Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY DISCONNECT THE WORKSTATION FROM THE NETWORK and call the IT Department Help Desk.

f) Do not uninstall (remove) or disable the official anti-virus program on your computer, nor install a program of your choice.

4.3 Spyware

Spyware and adware can compromise system performance and allow sensitive information to be transmitted outside the organisation. Spyware installation programs can launch even when users are performing legitimate operations, such as installing a company-approved application. As a result, combating spyware requires user vigilance as well as IT management and control.

4.4 IT Responsibilities

The IT Department shall:

a) Install and update appropriate anti-spyware measures.

b) Respond to all reports of spyware installation, remove spyware modules, restore system functionality, and document each incident.

4.5 Employee Responsibilities

These directives apply to all employees:

a) Employees shall not knowingly allow spyware to install on the organisation computers.

b) Employees shall perform anti-spyware updates and run anti-spyware programs regularly, as directed by the IT Department (as a rule, anti-spyware software will form part of the anti-virus software implemented by Mirats Insights).

c) Employees shall immediately report any symptoms that suggest spyware may have been installed on their computer to the IT Department.

5. SOFTWARE POLICY

5.1 Acceptable use

This section defines the boundaries for the “acceptable use” of the company’s electronic resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by the company are to be used only for creating, researching, and processing company-related materials. By using the company’s hardware, software, and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy.

5.2 Software

All software acquired for or on behalf of the company or developed by company employees or contract personnel on behalf of the company, is and shall be deemed company property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

5.3 Purchasing

All purchasing of company software shall be centralised with the IT Department to ensure that all applications conform to corporate software standards and are purchased at the best possible price. All requests for corporate software must be submitted to the IT Department for approval. The IT Department will determine the standard software that best accommodates the desired request.

5.4 Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on company computers. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of local and or national legislation. In addition to violating such laws, unauthorised duplication of software is a violation of the company's policy.

5.5 Software standards

The following list shows the standard suite of software installed on company computers (excluding test computers) that is fully supported by the IT Department:

- Microsoft Windows Professional 10 or 11
- Microsoft Office
- Chrome OS
- Macintosh OS 11 Big Sug or 12 Monterey
- Apple Application (Pages, Notes, Reminders, Numbers, Maps, etc.)
- Microsoft Windows Defender
- Google Drive for Business
- Adobe Reader
- Skype
- Anydesk
- Zoom

Employees needing software other than those listed above must request such software from the IT Department. Each request will be considered in conjunction with the requesting users Manager and in accordance with the software-purchasing section of this policy.

5.6 Employee Responsibilities

Employees shall not:

a) Not copy, load or run any software that is not properly licensed.

b) Not load their own software onto a Mirats Insights computer, whether they own the license or not, without prior permission from IT.

c) Not load any software onto a Mirats Insights computer. This must always be carried out by the IT Department. This includes downloading any program files from the Internet - and games.

d) Not allow third parties to install software on Mirats Insights computers without the authorisation of the IT Department.

5.7 IT Responsibilities

The IT Department shall:

a) Install and configure all Mirats Insights computers with the standard operating system and office suite.

b) Store and protect all the Mirats Insights software.

c) Ensure that all the Mirats Insights software is licensed.

d) Periodically check Mirats Insights computers to ensure this policy is enforced.

5.8 Computer Hardware Policy

Computer hardware includes all physical IT equipment; this includes all front end (laptops, computers, photocopiers and printers,) and backend (servers, network switches, firewall, routers) devices. All hardware purchased shall comply with the minimum specifications as recommended by the IT Department in consultation with Mirats Insights Management.

5.9 Purchasing

All purchasing of company computer hardware devices shall be centralised with the IT Department to ensure that all equipment conforms to corporate hardware standards and is purchased at the best possible price. All requests for corporate computing hardware devices must be submitted to the IT Department, which will then in conjunction with the direct report determine standard hardware that best accommodates the desired request.

5.10 Hardware standard

The following list shows the standard minimum hardware configuration for new/ to be procured company computers (excluding test computers) that are fully supported by the IT Department:

- Desktops
- Laptops

5.11 IT responsibilities

The IT Department shall:

a) Be responsible for giving minimum specifications in the procurement of all computer hardware.

b) Setup and install such hardware.

c) Maintain all the computer hardware.

6. ACCESS CODES AND PASSWORDS

The confidentiality, integrity and availability of data stored on the organisation's computer systems must be protected by access controls to ensure that only authorised employees have access.

This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. All passwords used in order to gain access to the organisation's data must comply with the Mirats Insights Password Policy.

6.1 IT Responsibilities

The IT Department shall:

a) Be responsible for the administration of access controls to all in the organisation's computer systems. The IT Department will process additions, deletions, and changes upon receipt of a written request from the end user's line manager. Deletions may be processed by oral request prior to reception of the written request.

b) The Senior IT Specialist will maintain a list of administrative access codes and passwords and keep this list in a secure area.

c) The IT Department shall take the necessary steps to enforce password expiry and the changing thereof every 90 days.

d) Ensure that the Mirats Insights Password Policy (see below) is enforced.

6.2 Employee Responsibilities

Each employee:

a) Shall be responsible for all computer transactions that are made with his/her User ID and password (passwords should therefore never be shared).

b) Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.

c) Will change passwords at most every 90 days.

d) Shall use passwords that will not be easily guessed by others.

e) Shall log out when leaving a workstation for an extended period.

f) Shall not attempt to access the accounts of other users unless she/he has been authorised to do so by the line manager.

6.3 Management's Responsibility

Managers shall notify the IT Manager promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked/amended. Involuntary terminations must be reported concurrent with the termination. Managers shall authorise in writing, the granting of access of another employee's network account.

6.4 Human Resources Responsibility

The Human Resources Department will notify the IT Department monthly of employee transfers, terminations and new appointments. Involuntary terminations must be reported concurrent with the termination.

7. PASSWORD POLICY

7.1 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Mirats Insights's entire corporate network. As such, all Mirats Insights employees (including contractors and vendors with access to Mirats Insights systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

7.2 General Policy

a) All system-level passwords (e.g., financial system, application administration accounts, etc.) must be changed on a quarterly basis.

b) All user-level passwords (domain logon passwords) must be changed every 90days.

c) Passwords are not displayed or concealed on your workspace.

d) Password must be at least ten characters long.

e) Windows Password must be changed every 90 days and previous four passwords cannot be re-used (enforced by the IT Department). In order to circumvent the risk that users may request four password resets in order to re-use the same password, the policy will be set not to allow more than four password resets over the period of 5 working days. All requests for password resets will be dealt with on a case by case basis.

f) Typing incorrect password three times will disable the account until IT enables the account on receipt of a Help Desk request.

g) All user-level and system-level passwords must conform to the guidelines described below.

7.3 Strong Passwords

Strong passwords have the following characteristics: a. They contain both upper and lower case characters (e.g., a-z, A-Z) b. They have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) c. They are at least seven alphanumeric characters long. d. They are not a word in any language, slang, dialect, jargon, etc. e. They are not based on personal information, names of family, etc. f. NOTE: Do not use either of these examples as passwords!

7.4 Poor Passwords

Poor, weak passwords have the following characteristics:

a. The password contains less than eight characters.
b. The password is a word found in a dictionary (English or foreign).
c. The password is a common usage word such as: Names of family, pets, friends, coworkers, fantasy characters, etc. Computer terms and names, commands, sites, companies, hardware, software. Birthdays and other personal information such as addresses and phone numbers. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

7.5 Password Protection Standards

a) Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other, phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

b) Do not use the same password for Mirats Insights accounts as for other non-Mirats Insights access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Mirats Insights access needs. For example, select one password for logging on to the domain and a different one for logging on to the Financial System (unless a Single Sign On solution is provided by the IT Department).

c) Do not share Mirats Insights passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Mirats Insights information.

d) If someone demands a password, refer them to this document or have them call someone in the IT Department.

e) Do not use the "Remember Password" feature of applications (e.g. Skype).

f) If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

g) Password cracking or guessing may be performed on a periodic or random basis by IT. If a password is guessed or cracked during one of these scans, the user will be required to change it.

8. PHYSICAL SECURITY

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorised access, and environmental hazards. The entire organisation's important hardware e.g. servers will be locked away. The server room shall at all times be locked. Only authorised personnel will be allowed into the server room. Third party maintenance personnel shall at all time by supervised by the Mirats Insights IT representative whilst in the server room.

8.1 Employee Responsibilities

The directives below apply to all employees:

a) Each employee is responsible for the security of the PC (including screen, keyboard, mouse and any other peripheral such as a printer) provided by the Mirats Insights to him or her.

b) Any item missing or damaged must be reported by the employee to the IT Department without delay, and followed up with a written communication outlining all the circumstances.

c) Disks and portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked away.

d) Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.

e) Since the IT Department is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities unless authorisation is given by the IT Department. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.

f) Employees shall not take shared portable equipment such as laptop computers out of the office without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.

g) Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be held accountable for any loss or damage that may result.

h) Laptop users shall, at all times, use cable locks supplied by the organisation to secure their laptops.

i) Employees who share offices (and so cannot lock their office when leaving it) are expected to make use of the lock computer option on their computer by pressing the CTRL+ALT+DEL key combination on their keyboard and selecting the lock computer option. Where possible, the IT Department will set a policy that will automatically disable (lock) computers where no keyboard activity has been detected for a period of five (5) minutes.

j) Visitors should be received at reception and always be escorted by a Mirats Insights employee

8.2 IT Responsibilities

The IT Department shall:

a) Ensure that critical computer equipment are protected by uninterruptible power supply.

b) Ensure that all laptops are supplied with cable locks.

c) Perform all equipment installations, disconnections, modifications, and relocations.

d) Ensure that strict access control is implemented at all server rooms and data centres and that a register is maintained of who had access, when and for what purposes.

9. HELP DESK AND CHANGE MANAGEMENT

One of the primary roles of the IT Department is to provide user support for all IT related problems.

9.1 Employee Responsibilities

All employees will observe and adhere to the following:

a) Employees will use the e-mail facilities or the provided helpdesk system (phone call) to log their problems and request service from the IT Department. Employees must record exactly what has happened, and write down any error message(s) appearing on the screen.

b) No person may request the IT Department to fix a problem (hardware or software) on any equipment not owned by the Mirats Insights. c) Request for the creation or deletion of new users must be submitted to the IT Department with the relevant documentation 2 working days prior to the employee starting in his/her position.

9.2 IT Responsibilities

The IT Department shall:

a) Acknowledge all queries and problems and give an estimate of when the problem will be addressed.

b) b) Respond timorously to all user queries and problems.

10. GENERAL ACCEPTABLE USE REQUIREMENTS

10.1 System Backup and Recovery

Information is a valuable tool and must be protected at all cost. In the event of information loss the organisation should be able to recover the information.

10.2 IT Responsibilities

IT Department shall backup all the information on the servers in accordance to the Business Continuity and Disaster Recovery Plan.

10.3 Employee Responsibilities

Each employee shall save their work-related information on the Corporate Dropbox on a daily basis. They will ensure that the Dropbox synchronization process is running, and advise the IT Department if it is not.

10.4 Reporting of Incidents

Users are to report any security (or suspected) breaches to the IT Department who will provide further guidance on the approach that should be followed.

10.5 Copyrights and License Agreements

It is the Mirats Insights policy to comply with all laws regarding intellectual property.

ACRONYMS, ABBREVIATIONS AND DEFINITIONS

Term	Description
Access Control	Access Controls provide the means of establishing
Accountability or Auditability	Auditability ensures protected and reliable records of system activity with security significance (e.g. logins, logouts, file accesses, security
Adware	Adware is any software program in which
Authentication	Authentication provides the means of verifying the
Authorisation	Authorisation enables specification and the subsequent management of allowed actions for a
Availability	Availability is the assurance that information is available on a timely
Awareness	Actions taken to address knowledge, attitude and behaviour as the key
Confidentiality	Confidentiality is the protection of information

Term	Description
Information Assets	This takes many forms and includes data stored on computers, servers, transmitted across networks, Intranet, printed
Integrity	Integrity is the protection of information from
ISO1-7799 or 27002	International Organisation for Standardization's Standard for Information Security Management.
Nonrepudiation	Non-Repudiation protects against any attempt by the sender to falsely deny sending information, or subsequent attempts by the recipient to falsely deny receiving this information.

Mirats Insights, LLC

To access this document on web go to -

www.miratsinsights.com/shortlinks/it-security

support@miratsinsights.com