INTUATE GROUP AND ITS SUBSIDIARIES IT & TELECOMMUNICATIONS POLICY

Version 3.1

TABLE OF CONTENTS

Intuate Group and its Subsidiaries IT & Telecommunications Policy

1. INTRODUCTION

Intuate Group and its Subsidiaries' electronic communication and information systems have become an integral part of company operations. On the one hand it provides an effective communications tool and on the other hand, it provides access to company information which is vital for the quality of work produced, and the access to accurate and timely information for all operations. The operation of the Company is therefore dependent upon the systems used and all information maintained electronically, form part of company assets.

This policy describes the reasonable steps that need to be taken to ensure the security of critical information and assets as well as the Company's standards and guidelines with regard to the use of systems. The policy furthermore explains the Company's right to access and the disclosure of system usage by the Company's employees and other users.

2. SCOPE AND FRAMEWORK

This policy applies to all users of Intuate Group or any of its Subsidiaries' systems and applies to all company information, including any electronically generated and stored information, and all handwritten, typed, printed, faxed, emailed or scanned information.

The policy provisions as contained in this document, as amended from time to time, are by reference incorporated in the Company's service conditions.

3. INTERNET DEFINITIONS

Certain terms in this policy should be understood widely to include related concepts:

3.1 **Intuate Group and its Subsidiaries** include all employees, contractors, fixed term contractors, including the Company's Service Partners.

3.2 **Document** covers any kind of file that**:**

- Can be read on a computer screen as if it were a printed page;
- Can be read in an Internet browser
- Is meant to be accessed by a word processing or desktop publishing program or its viewer.
- Is prepared for the Adobe Acrobat reader and other electronic publishing tools

3.3 **Graphics** includes photographs, pictures, animations, movies, or drawings

3.4 **Display** includes monitors, flat-panel active or passive matrix displays, monochrome LCDS, projectors, televisions and virtual-reality tools.

3.5 **Computer Systems** includes networks, PC's, laptops, servers and telephony.

3.6 **Electronic Information** includes any information stored on Intuate Group or any of its Subsidiaries infrastructure e.g. email, documents and presentations.

4 PRINCIPLES

4.1 Information technology and equipment is expensive and use thereof and access to it must be used primarily for business purposes for example, communication with customers and suppliers, researching relevant topics, obtaining useful business information.

4.2 All employees are expected to conduct themselves honestly and appropriately when using technology, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as in any other business dealings.

4.3 The use of Internet is subject to compliance with all existing Company policies particularly (but not exclusively) those that deal with intellectual property protection, privacy, misuse of company resources, sexual harassment, accessing any form of sexually explicit material, accessing pornographic information, transmitting personal information of self or others, soliciting or proselytizing non-job-related commercial ventures, religious, personal causes, data security and confidentiality.

4.4 Unnecessary or unauthorised Internet usage causes network and server congestion. It slows down other users, affects productivity, consumes supplies, and ties up printers and other shared resources. Unauthorised Internet usage may also expose the organisation to significant legal liabilities.

4.5 The desktop and laptop computers and all related equipment shall remain the property of the Company.

4.6 The use of any equipment or technology supplied by the Company is intended for business use only.

5 SECURITY

Employees are obliged to comply with the security procedures implemented from time to time by the Company in order to prevent any damage or unauthorised access to the computer systems;

6 PASSWORDS

The Company's computer systems require passwords and all users are allocated passwords in order to access the system. Where employees choose passwords these should be constructed carefully and employee names, spouse names, children's names, birthdays, etc or actual words should not be used. A combination of letters and special characters (e.g. #) should be used.

Employees are obliged to keep all passwords confidential. Employees should not share their password with anyone inside or outside the Company. Any employee who shares a password / pin with a fellow employee, as well as the person whom it was shared with, will be held liable for any damages suffered as a result of this.

6.1 LOG OFF

All computer users must exit the computer system at the end of each working day and "log off" from the relevant network so as to prevent the possibility of any unauthorised access to the computer system. Employees must, in addition, ensure that during the day appropriate measures are in place to prevent unauthorised access to the Company's systems e.g. screensaver passwords, logging out of systems when leaving the office, etc.

6.2 BACKUP

All users are required to place sensitive / important business data on their personal user folder which is backed up on a daily basis. Users should furthermore ensure that the Attix5 backup software runs daily. If the backups do not run on a daily basis, the user should report this to the Service Desk.

Backup services are only intended for business related data. Users should not save any personal data i.e. music, pictures, videos in the folders that are backed up. Personal data will be deleted from the backup servers.

7 HARDWARE & SOFTWARE

All the Company's computers are provided with the necessary hardware and software, which meets the Company's requirements. Should any user require additional or specific hardware or software, such employee should obtain approval from their manager.

Employees are prohibited from installing any unlicensed and/or unauthorised software on any computer of the Company's system. The employee will be liable for any cost, expense and losses incurred by the Company as a consequence of such unlicensed and/or unauthorised installation. This includes and is not limited to fines and penalties payable by the Company as a result of unauthorized installations.

Commercial computer software purchased by the Company are authorised for the Company's use only. Making copies of the Company's purchased software for personal or any other use is illegal and prohibited.

If a virus detection program indicates that a virus has been discovered, the involved employee must immediately log a call with the Service Desk. Employees must not attempt to eradicate a virus or otherwise use the affected computer until trained personnel have addressed the problem. If a virus is detected, the affected computer should not be connected to the Company's network or if already connected, should be disconnected immediately.

Externally supplied disks or other storage media may not be used on any of the Company's computers unless these disks/media have first been checked for viruses.

Employees are not allowed to bring laptops/personal computers to the office or connect to the Company's network unless written permission has been obtained from HR and the relevant Executive.

8 EQUIPMENT

Transport of equipment should be handled with caution. Where it is necessary for employees to transport IT equipment all the necessary steps should be taken to ensure that the equipment is properly packaged and secured as per the supplier warranty/instructions. Employees should make sure they read and understand the instruction manuals provided by the manufacturer on how to package, handle and transport the equipment.

8.1 No equipment may be left in an unattended car i.e. parked at shopping malls or anywhere else.

8.2 The employees are responsible for sending an email to their Line Manager to inform them of the anticipated transport (for all equipment with a value of more than R10,000-00). If the notification is not done prior to the transport, no insurance cover will be confirmed and the employee will be liable for any damages/theft and associated costs.

If loss or damage occurs due to the negligence of an employee, the full value of the equipment may be deducted from the employee's salary to replace the equipment. Employees are required to obtain written permission from their managers before transporting any equipment and at the same time acknowledge that they will be held responsible for the full value of the equipment should the above conditions not be met.

9 LAPTOPS

Where an employee is located at a client site, laptops should not be left unattended (e.g.: using the restroom, talking with friends, attending meetings) unless the appropriate security cable is in use. All costs associated with damage to, loss of, or theft of the laptop (10% of the claim, minimum R500-00) whilst checked out to the employee will be deducted from the employee's salary. If loss or damage occurs due to the employee's negligence, the full amount based on the replacement value of the laptop, including software and warranties, will be deducted from the employee's salary.

It is the responsibility of the employee to obtain a security cable from the IT Department should one not be issued with the laptop.

10 UNAUTHORISED USE OF THE COMPUTER SYSTEM / SOCIAL MEDIA

Any unauthorised use of the Company's computers or systems is strictly prohibited. Such unauthorised use includes, but is not limited to:

10.1 Sending, connecting to, posting, printing, down-loading or disseminating material that is: fraudulent, pornographic, obscene, defamatory, harassing, intimidatory, disruptive, racist, sexually explicit, obscene, or sexist or material which constitutes "hate speech".

10.2 Engaging in destructive activities and the gaining of unauthorised access to computer networks whether of the Company or of any entity outside the Company.

10.3 "Hacking", "cracking" or any similar activities and the creation and/or distribution of destructive programs (viruses and/or self replicating code).

10.4 Attempting to access, disable or compromise the security of any information contained in the computer systems of the Company or of any entity outside the Company.

10.5 Excessive frequency and duration of use other than in the performance of business responsibilities.

10.6 The distribution of chain letters, petitions, wealth schemes, etc.

10.7 The display of any kind of sexually explicit image or document on any company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

10.8 The Company's Internet facilities and computing resources must not be used knowingly, to violate the laws and regulations of the Republic of South Africa or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way.

10.9 No employee may use the Company's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

10.10 Employees are prohibited from knowingly using the Company's facilities to download or distribute pirated software or data.

10.11 The use of the Company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap door program code is prohibited.

10.12 Where an individual participant is identified as an employee or agent of the Company, the employee must refrain from any unauthorised political advocacy and must refrain from the unauthorised endorsement or appearance of endorsement by the Company of any commercial product or service not sold or serviced by the Company, its subsidiaries or its affiliates.

10.13 Employees may not participate in chat groups.

10.14 Employees with Internet access may not upload any software licensed to the Company data owned or licensed by the Company without explicit authorisation from the manager responsible for the software or data.

10.15 Employees are reminded, that newsgroups are public forums where it is inappropriate to reveal confidential information, customer data, trade secrets, and any other material covered by existing secrecy policies and procedures. This includes, but is not limited to Facebook, Twitter, Blogging and LinkedIn. Should your job function require that you use these forums you are reminded that you are not allowed to reveal any confidential information about the company, its employees or prospective employees, its customers or prospective customers. The social media sites should be used with discretion at all times.

10.16 Employees releasing protected information via a newsgroup - whether or not the release is inadvertent - will be subject to all penalties listed in existing data security policies and procedures.

10.17 Use of the Company's Internet access facilities to misuse the Company's assets or resources. Sexual harassment, unauthorised public speaking and misappropriation or theft of intellectual property are also prohibited.

10.18 Downloading of games, videos and other large files such as shareware is prohibited as this involves excessive use of the bandwidth.

10.19 The use of P2P connections such as Kaza, Bearshare etc is prohibited.

10.20 Video and Radio streaming (watching videos and listening to the radio through the internet) is also not permitted as these activities use excessive bandwidth.

11 ACCEPTABLE USE

Employees with Internet access may download only software with direct business use, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.

12 COPYRIGHT

Any software or files downloaded via the Internet into the Company's network become the property of the Company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. Copies may be used for reference only.

Employees with Internet access must take particular care not to put the Company at risk.

The Company retains the copyright to any material posted to any forum, news group, and World Wide Web page by any employee in the course of his or her duties.

13 OFFICE TELEPHONES

Although staff may use the office telephone for private use, each employee is required to use the phone responsibly by keeping such use to an absolute minimum.

Each telephone user will be required to justify monthly costs, and will be required to pay for personal calls in excess of R50.00 pm.

14 ACCESS TO AND DISCLOSURE OF AN INDIVIDUAL'S USE OF THE COMPANY'S ELECTRONIC COMMUNICATION SYSTEM

14.1 Although the Company respects the privacy of its employees and other users of its systems, restriction of this right is unavoidable in the context of the employee's work-related conduct or the use of the Company's provided equipment, supplies or system. The systems have been installed by the Company to facilitate business communications and to provide in the Company's operational needs.

14.2 The Company is obliged to manage and protect its systems. Management has been tasked with the responsibility to monitor the systems and usage to ensure compliance with this policy and may, without further notice to the user/employee, intercept, inspect, monitor or refuse to make a communication available or to pass it on to its intended receiver in the exercise of its responsibility.

14.3 Although each employee has an individual password to access this system, the system belongs to the Company and the facilities belonging to and controlled by the Company (telephones, electronic mail, fax machines, modems, computers, network tools and application including Internet access facilities, web browsers), and the content of email communications and Internet usage should be accessible at all times by the Company's management for any

business purpose. All system passwords and encryption keys must be available to management, and employees may not install encryption programs without turning over encryption keys to their Line Manager.

14.4 The system may be subject to periodic unannounced inspection, and should be treated like other shared filing systems. The Company also routinely monitors usage patterns for its email/Internet communications. The reasons for the inspection and monitoring are many, including cost analysis/allocation and the management of the Company's gateway to the Internet.

14.5 All messages created, sent or retrieved over the system and all other searches, transmissions or downloads are the Company's records which remain the property of the Company and should not be considered public information. The Company reserves the right to access, monitor and disclose without the employee's permission, where necessary, all system usage (including messages and files on the company's email/Internet system). Employees should not assume electronic communications are private or confidential.

14.6 Employees (other than Management in the circumstances mentioned above) are prohibited from unauthorized use of the password and encryption keys of other employees to gain access to the other employee's email messages.

14.7 Any alleged contravention of the above will be investigated by Management, and all users are required to report any contravention of the above which comes to their attention.

15 CONFIDENTIALITY OF INFORMATION

15.1 The electronic and paper systems contain information about the business and its operations, its customers, products, supplier information, and its managers and employees.

15.2 This information is classified as confidential and sensitive information and may not be accessed unless for work related to the user role, and no other information may be accessed without written explicit and specific management permission.

15.3 Users who come into possession of such information may not disclose this to any other person without written explicit and specific management permission.

15.4 Technical users who have access to confidential information by virtue of their roles, should refrain from accessing information not related to their role/function/purpose.

15.5 No user may make any business related statement to any form of external media – including placing information on the internet – without the written explicit and specific management permission.

16 BREACHES OF POLICY

Any breach of this policy will result in the necessary disciplinary action being taken by the Company and may result in dismissal of the employee in question.

17 LIABILITY & INDEMNITY

Any employee who violates the security, hardware and software provisions of this policy shall be liable for any cost, expense, loss, penalty and/or damage incurred by Intuate Group or any of its Subsidiaries in that regard.

Furthermore, the employee shall indemnify the Company in respect of any violation of this policy, for any fees, fines, penalties or charges incurred by or imposed upon Intuate Group or any of its Subsidiaries as well as any loss of profits and productive working time occasioned by such violation.