1. APPLICATIONS AND DEFINITIONS

The Company may be held liable for the actions of employees and contractors using the Company's e-mail and Internet access services. This policy creates rules that aim to limit and manage the risk associated with unlimited e-mail use and Internet access.

Definitions:

"user(s)" means all employees employed by the Company and contract workers that have access to the Company's IT infrastructure.

"Illegal Content" means e-mail and web site content that contains material that is pornographic, oppressive, racist, sexist, defamatory against any user or third party, offensive to any group, a violation of a user's or a third party's privacy, identity or personality, copyright infringement, malicious codes such as viruses and Trojan Horses, and content containing any personal information of users or third parties without their consent;

"Personal Information" means personal information as defined in the Promotion of Access to Information Act (click here to download the Act):
http://www.polity.org.za/html/govdocs/legislation/2000/act2.pdf

"Pornographic" means all the content and actions, simulated or real, graphic or written detailed in Schedules 1, 2, 6, 7 and 11 of the Films and Publications Act 65 of 1996 (click here to download the Act): http://www.polity.org.za/html/govdocs/legislation/1996/act96-065.html); and

"Internet" shall in all cases include the Company's intranet.

Application:

This policy applies to all users as well as third parties that have temporary access to the Company's e-mail, Internet access or network and who:

- use the Company's facilities to send and receive e-mail messages (including attachments thereto);
- access the Internet and the Internet's services including but not limited to usenet newsgroups, the World Wide Web and Internet chat rooms; or

- save, retrieve or print files, e-mail messages or other electronic documents to and/or from the Company's network or a computer, hard drive, flash drive or disk.

2. PURPOSE

The purpose of this electronic communications policy is to:

- inform users on the use of e-mail and the Internet;
- create rules for the use of e-mail and the Internet;
- provide for disciplinary action against users who fail to comply with this policy; and
- ensure and maintain the value and integrity of the Company's equipment and network(s).

3. OWNERSHIP, RESPONSIBLE PERSONS AND RIGHT TO MONITOR

3.1 RESPONSIBLE PERSONS AND DUTIES

3.1.1 users are personally responsible to abide by the rules created in this policy and must delete all incoming e-mail messages that contain content or links to content that are not allowed in terms of this policy;

3.1.2 The Company's IT department (IT-Support) is responsible for:

- the technical issues related to e-mail use and Internet access;
- assisting the Company's managing director to conduct searches / monitoring of user's incoming and outgoing e-mail messages, stored messages, stored files and browsing habits;
- ensuring all outgoing e-mail messages contain the Company's official e-mail legal notice;
- scanning all incoming message and file downloads for malicious codes such as viruses or Trojan Horses;
- sustaining users' awareness of this and other Company polices related to the use of the Company's electronic facilities; and
- offering training for users in the proper use of the Company's electronic facilities.

3.1.3 The Company's management and Human Resources department are responsible for taking the necessary disciplinary action against users who fail and/or refuse to abide by this policy.

3.2. RIGHT TO MONITOR

With due regard to the South African Constitution and the Regulation of Interception of Communications Act, each and every user has given his or her written consent that, only with the written instruction of the managing director, the IT department and management of the Company may, without prior warning:

3.2.1. Intercept, monitor, block, delete, read and act upon any incoming or outgoing e-mail message addressed to or originating from the user;

3.2.2. Intercept, monitor, read and act upon the user's Internet browsing habits, including the user's history files, web sites visited, files downloaded and stored by the user; and

3.2.3. Intercept, monitor, block, delete, read and act upon any file, in whatever format, stored by a user on any computer or other facilities of the Company.

4. ACCEPTABLE USE AND GENERAL GUIDELINES

The following actions and content will be considered acceptable use of e-mail and Internet facilities by users:

4.1 users shall use e-mail and Internet access primarily for business and Company purposes. Private and personal use, in moderation, will be tolerated, subject to the rules detailed in this policy;

4.2. Equipment, systems, services and software on the Company's networks are to be used primarily for work related purposes. Common sense and good judgement should guide personal and private usage;

4.3. When forwarding or replying to e-mail messages, the contents of the original message should not be altered. If the contents need to be changed, then all changes must be clearly marked as such;

4.4. The Company has the right to limit the size of incoming and outgoing e-mail messages and attachments, downloads and other files and may block and delete e-mail messages, downloads, attachments or other files that are larger than the set maximum size. It is the responsibility of

users to limit the size of attachments and other files to prevent overloading of the electronic mail system resources;

4.5. E-mail messages should be kept brief and formulated appropriately;

4.6. Virus warnings or pop-ups that result from incoming e-mail or file downloads must be reported to the IT department immediately;

4.7. All outgoing e-mails must have the Company's standard e-mail legal notice at the end of the message. This e-mail legal notice may not be removed or tampered with by users;

4.8. Users must check e-mail recipients prior to sending, forwarding or replying to messages. When distribution lists are used the sender should consider whether or not each group member really needs, or really should, receive the e-mail;

4.9. The subject field of an email message should relate directly to the contents or purpose of the message;

4.10. Users must log-off or use screen savers with passwords in times of absence from a computer terminal to avoid improper and/or illegal use;

4.11. Notebook and/or offline users should load and update the "address book", if any, regularly; and

4.12. If users are out of the office for more than one day, they should activate the "Out of Office" function. This informs the sender of an e-mail of a recipient's absence. The "Out of Office" message should include both the period of absence and an alternative contact person.

5. NON – ACCEPTABLE AND PUNISHABLE USE

The following actions and content are not allowed and will lead to investigation and disciplinary action:

5.1 Sharing logon usernames with or disclosing passwords to any third person(s);

5.2 Modifying an e-mail message and forwarding or replying therewith without noting the changes (i.e. deletions, removal of recipients, modification of content, etc.);

5.3 Fabricating a message and/or sender of a message;

5.4 Intentionally bypassing the security mechanisms of the mail system or any other secure web site or network (e.g. creating bogus accounts);

5.5 Modifying the internal mail transport mechanism to forge a routing path that a message takes through the Internet;

5.6 Storing, downloading, printing, distributing, sending or accessing Illegal Content (as defined above);

5.7 Participating in e-mail "chain letters" or similar activities;

5.8 Downloading, receiving and/or installing software applications not approved by the IT department;

5.9 Knowingly burden the Company's network with non-work related data (e.g. forwarding, downloading or accessing large video clips or graphics to or from a distribution list or file-sharing server);

5.10 Using automatic forwarding of e-mails ("Auto Rules") to any person without such person's consent;

5.11 The creation, sending or forwarding of unsolicited mail (spam);

5.12 The creation, sending or forwarding of marketing information about non-work related issues;

5.13 Negligently or willfully sending or forwarding e-mail messages and/or attachments that are infected with malicious codes such as viruses and Trojan horses;

5.14 Using storage devices that may be infected with malicious code;

5.15 Accessing and using internet relay chat if such actions burden the Company's systems or prevent other users from using them;

5.16 Any non-work related actions that knowingly prevent other users from using e-mail or Internet access;

5.17 Taking any of those steps or actions criminalised and detailed in Chapter XIII of the Electronic Communications and Transactions Act 25 of 2002, including but not limited to hacking or developing, downloading and using any technology that may circumvent IT security measures (click here to download the ECT Act: http://www.polity.org.za/pdf/ElectronicCommunications.pdf see sections 85, 86, 87, 88 and 89);

5.18 Any destructive and disruptive practices either via e-mail or the Internet;

Indiscriminate storage and/or forwarding of e-mail, files, web sites and attachments for which permission has not been obtained from the originator or copyright holder;

5.19 Any purposes that could reasonably be expected to cause directly or indirectly excessive strain on any computing facilities, or unwarranted or unsolicited interference with others;

5.20 Any destructive or disruptive action that could interfere in the day to day operations of the Company. These include but are not limited to intentionally deleting data, files and e-mail which is essential to the business;

5.21 Sending, replying to or forwarding e-mail messages or other electronic communications which hides the identity of the sender or represents the sender as someone else;

5.22 Users of the Company's electronic mail systems who obtain access to materials of other organisations may not copy, modify or forward copyrighted materials, except under the specific copyright terms and conditions; and

5.23 Using information, e-mail, files, downloads or data to commit fraud or any other criminal offence(s).

6. ENCRYPTION OF DATA

6.1. It is required that all sensitive data on laptops being used for work purposes, whether the property of the Company or an employees' personal property, be encrypted.

6.2. Should an employee fail to encrypt such data on his/her laptop and the laptop get lost / stolen, the employee will be held liable for the loss of data.

6.3. Employees are responsible for the encryption of data on their laptops. They can ask IT support for assistance in this regard.

6.4. Failure to encrypt data on laptops is a dismissible offence.

7. CONSEQUENCES OF MIS-USE

Failure and/or refusal to abide by the rules detailed in this policy shall be deemed as misconduct and the Company may initiate the appropriate investigation and disciplinary action against users. Such steps may include dismissal or expulsion, as the case may be.