Scope

This ITBS Security and Usage Guideline ("Guideline") applies to the entire Afrimat Limited ("Afrimat" or "Company") group.

Purpose

Information systems are a key enabler within Afrimat and it is becoming increasingly dependent on information systems. The purpose of the Guideline is to improve data security, to maximise systems uptime and to ensure maximum line speed for users.

Accountability

Users are responsible for understanding, respecting and implementing the Guideline.

Management and supervisory staff should assist IT staff to ensure full adherence to the Guideline.

Only trained users may be allowed to use the Company's computer facilities (i.e. computer equipment, computer network, application software, personal computer software, email, internet).

Standards

The following standards, rules and limitations should be adhered to by all users and IT staff:

- **Protection of computer equipment**

  All file servers to be kept in a locked computer room that is suitable for the purpose;

  All users and other computer equipment (including laptops) to be kept in locked offices/buildings after hours. Line managers should approve the use of laptops at an employee's home;

  Computer equipment to be cleaned regularly;

  Laptops, memory sticks and disks may not be left unattended (in particular left in cars); (leaving a laptop in the car's boot is also not allowed);

  No private computer equipment may be linked to the Company's network except if approved by the IT manager and the required access and anti-virus standards are being adhered to;

- **Access to computer network/equipment/information**

  Only authorised users may have access through unique log-in and passwords;

  Authorised users may not allow other parties to have access using their logins or passwords. If a user is forced to share a login/password due to operational requirements then this may only be done with approval of IT staff and then the password must be changed to a new password before the end of the day;

  Users may not link private email accounts to Outlook on the Company's systems;

  Users "security rights" on shared application systems to be restricted;

  At no time should a user's computer be linked to the Company's network via cable or 3G and simultaneously to another external modem/3G;

System administrator access to be restricted to authorised IT staff;

Users to log out from application systems/network when leaving the workstation unattended;

- **Use of computer network/equipment/information**

Computer network/equipment/information may only be used for Afrimat purposes

- Minimum private usage is however allowed during specific times (see "limitation on use" below);

Websites with offensive content may not be visited; (including sex, pornography, encourages tension/violence/racism, gender, political, sexual orientation, religious beliefs, nationality, age, disability);

Creation, storage, send/forward or distribution of any unlawful, offensive, rebellious, threatening or harassing material is prohibited; (including sex, pornography, encourages tension/violence/racism, gender, political, sexual orientation, religious beliefs, nationality, age, disability);

Any conduct that would constitute or encourage a criminal offence, lead to civil liability or otherwise violate any municipal, provincial, national or international regulations/laws are prohibited;

Wilful or negligent deletion or adjustment of Company related data and files are prohibited; (including spread sheets and word processing documents);

Wilful or negligent actions that damages or disrupts computing systems or networks are prohibited; (including altering its normal performance or causes it to malfunction);

Input and balancing controls to be done by users (including generation/checking of audit trails and input/output documents retention);

- **Distribution of information**

Company information may not be distributed to unauthorised persons;

No copy of information systems may be made except if needed as backup;

- **Storage of information**

All computers to be linked to a file server as far as possible thus stand-alone computers to be minimised;

Use of memory sticks and disks for additional storage of information not allowed (may only be used for backups and to work temporary on another computer;

- **Backup of systems**

Backups of computers to be done as follows:

File servers	Daily
Stand-alone computers	Monthly
Winbridge PC's	Daily;

Backup's retention to be in terms of the 'Backup Guideline'. Backups to be kept offsite in terms of the 'Backup Guideline' but at least in locked cupboards;

- **Antivirus and destruction**

All computers to have the standard Afrimat antivirus software in operation;

- Antivirus patterns to be updated automatically at least weekly;

Pointing or hyper linking of the Company's website or other internet/WWW sites are prohibited;

Wilful or negligent introduction of computer viruses are prohibited; (including Trojan horses, spyware or other destructive programmes into Company computer equipment and networks or into external systems and networks);

Unauthorised decryption or attempt at decryption of any system or user passwords are prohibited (include any other user's encrypted files);

Packet sniffing, packet spoofing or use of other means to gain unauthorised access to computer systems or networks is prohibited;

- **Intellectual property rights**

All application and operating system software must be licensed;

No personal software may be loaded on Company computers;

No software may be downloaded from the internet by users unless approved by IT staff;

Use, transmission, duplication or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets or patent rights of any other person or organisation are prohibited;

- **Changes**

Only head office IT staff may procure any computer equipment, software and services. This responsibility could be delegated to regional IT staff subject that the group specifications are being adhered to and that prior approval is gained from head office IT staff;

Only IT staff may make changes to IT infrastructure subject to strict change control i.e. approval by head office IT staff;

Only head office IT staff may facilitate software changes subject to strict change control;

- **Ownership of information**

All information on the Company's computer equipment is owned by the Company;

Company has the right to access any user's private emails received or sent and any user's data files for any purpose without informing the user;

Company has the right to disclose any user's private emails received and sent and any user's data files to law enforcement officials without informing the user;

- **Limitation on use**

Users must limit their impact on the Company's network and storage equipment through
- Minimising emails sent and received
- Limit size of sent email attachments ("ZIP" or compress files before sending)
- Minimise attachment with photos and video clips (use of photo resizer – e.g. VSO resizer recommended)
- Minimise internet browsing
- Minimise downloads from internet (in particular photos, video clips, movies, games and music);

Private usage of the Company's computer facilities is limited as follows
- Only allowed during lunch times and after normal business hours
  - Computer equipment usage
  - Sending of emails
  - Internet usage
  - Internet "Skype' usage
  - Internet social networks usage (e.g. Facebook, LinkedIn, Twitter, My Space)

- Playing online games e.g. Poker
- Playing of computer games;

- Not permitted at any time:
  - Generation, forwarding or storing of chain letters.

Private usage above is only allowed if such usage does not have any response time impact on the Company's network.

The Company reserves the right to revoke the privilege of private use of computer facilities without declaration or reason(s). Also, where the private usage (including private usage during lunch times and after normal business hours) would give a bad impression of the Company then such private usage may be revoked by management.

Non-adherence

Any known misuse or violation or breach of this Guideline to be reported immediately to IT management, financial manager and financial director.

Any misuse or violation or breach will be investigated by IT management and classified as follows:

Class of non-adherence	Examples
Serious	Visiting pornographic websites Negligent corruption of a computer system Sharing an access password Not making backup
Significant	Leaving laptop unattended in vehicle
Moderate	Forwarding a chain letter

Sanctioning will be in terms of the Company's Disciplinary Code.

Effective date

This revised Guideline became effective from 1 March 2013.

END.