PART C – SECTION 3.2

IT SYSTEMS END USER POLICY

Table of Contents

1. DOCUMENT CONTROL 4

1.1. DOCUMENT SIGNOFF 4
1.2. CHANGE RECORD 4
1.3. DOCUMENT INFORMATION 4

2. INTRODUCTION 5

2.1. PURPOSE 5
2.2. INTENDED AUDIENCE 5
2.3. CONDITION OF EMPLOYMENT 5
2.4. CONDITION OF CONTRACT 5
2.5. ACCOUNTABILITY FRAMEWORK 5
2.6. AREAS COVERED IN THIS POLICY 6

3. POLICY DETAIL 7

3.1. END USER DEVICE USAGE 7
3.2. PERSONALLY OWNED DEVICES 7
3.3. USE OF COMPANY IT FACILITIES 9
3.4. INTERNET AND E-MAIL USAGE 10
3.5. SOCIAL MEDIA IN A PRIVATE CAPACITY 12
3.6. MALICIOUS SOFTWARE PROTECTION 14
3.7. USER ACCOUNTS AND PASSWORDS 14
3.8. PHYSICAL SECURITY 14
3.9. SOFTWARE COPYRIGHT AND LICENSE AGREEMENTS 15
3.10. MOBILE AND HOME COMPUTING USAGE 16

4. ACKNOWLEDGEMENT OF END USER POLICY 18

5

1. Document Control

1.1. Document signoff

Designation	Name	Signature	Date

1.2. Change Record

Version Number	Date	Author	Details
0.92	13 Aug 2008	Debra-Lynn Marais, Shanil Batohi	Changes from Powertech Transformers and Aberdare Cables applied.
2	24 Jan 2011	Debra-Lynn Marais, Energy Zonde	Changes from Altron IM Council
August 2011	18 August 2011	Chris Potgieter Energy Zonde	Legal review of I.T. policies
August 2012	14 August 2012	Energy Zonde & C Potgieter	Changes from Altron IM Council

1.3. Document Information

Filename:	End User Policy

2. Introduction

Computer information systems, data and networks are an integral part of business within the Altron Group. The group has made a substantial investment in human capital and financial resources to create and maintain these systems and networks. The integrity and operation thereof should be protected at all times.

2.1. Purpose

The purpose of this policy is to manage the use of the Information Technology (IT) facilities provided by the company, and to prevent abuse. This policy specifically addresses the IT facilities and thus has to be read in conjunction with all other Altron policies which govern the conduct and behaviour of all staff.

This policy has been established in order to:

- Protect the company's IT investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the reputation of the group and its companies.
- Limit and manage the legal risks to which the group is exposed to.

2.2. Intended Audience

The intended audience for this policy is:

- All employees of the Altron Group.
- All subcontractors that make use of Altron IT facilities.
- IS Manager, IT Manager or Manager responsible for IT.
- All Managers and Supervisors.

2.3. Condition of employment

Adherence to this IT Systems End User Policy is a condition of employment. Any Employee found to have violated these policies might be subject to disciplinary action as set out elsewhere in the Altron Policy Manual.

2.4. Condition of contract

Adherence to this IT Systems End User Policy is a condition of any contract with any sub-contractors making use of the Altron IT facilities. Where appropriate such sub-contractors should be made aware of this policy whenever they are appointed. A failure by any of them to comply herewith shall constitute a breach of contract with resultant potential legal liability as recognised by law.

2.5 Accountability Framework

The accountability framework for IT risk and policies is as follows:

Role	Recommend	Approve	Responsible	Accountable
Authority	Altron IM Council	Altron Risk Committee	Users	Managers and Supervisors
Review and Reporting	Annual Review	Annual Review	On-going	Bi annual consolidated risk reports (Audit/Risk committees)

Compliance to policy will also be audited by internal audit during their computer audit reviews conducted with the companies.

The following sections list the additional specific responsibilities.

2.5.1 Manager responsibilities

Managers and supervisors must ensure that all employees are aware of and comply with this policy.

2.5.2 Employee responsibilities

The employee must ensure that he or she adheres to the content of this policy and enquire from the IS/IT Manager clarity on any aspect of this policy that is unclear or needs further explanation.

2.6. Areas Covered in this Policy

The topics covered in this document include:

- **End User Devices**: This section details requirements regarding the use of any end user device that is used to access the company's networks, systems and data. The company owned end user devices will henceforth be called "company end user device" and non-company owned end user device will be called "personal devices". References to "end user device" will include both company owned and non-company owned end user devices.
- **Personally Owned Devices**: This section details requirements regarding the use of any end user owned device that is used to access the company's networks, systems and data.
- **Use of Company IT facilities**: This section details the company's requirements in terms of the use that employees and other people make of the company's IT facilities.
- **Internet ,E-mail Usage and Social Networking usage**: In order to protect the company and ensure the optimum utilisation of company communications facilities this section details policy regarding the use of E-mail, Social Networking and any Internet facilities accessed via facilities provided by the company.
- **Social media in a private capacity**: this section details how to conduct yourself when using social media in a private capacity.
- **Malicious Software Protection**: The Company's facilities data and systems need to be protected from Malicious Software of all types. The regulations that need to be adhered to by the users are contained in this section.
- **User Accounts and Passwords**: This section details the behaviour and conduct of all people who have access to the company's networks.
- **Physical security**: This section details the manner in which any equipment containing company data is protected from physical loss or damage.
- **Software copyright and licence agreements**: The section details the rules that must be applied in the company in terms of software applications and licenses.
- **Mobile and Home Computing Use**: This section details the requirements of the company in terms of the use of mobile devices that are company owned and personally owned devices used to access the company network.

3. Policy Detail

3.1. Company owned End User Device Usage

Access and use of company owned end user devices is provided to employees for the benefit of the company and its business. Access to the company owned end user devices is a privilege and such access is entirely at the discretion of the CEO/Managing Director or specific delegates. Employees are able to connect to a variety of business information resources by using the company owned end user device. Due care needs to be taken by users to ensure that company end user devices are not used for illicit or unauthorised purposes.

This section of the policy applies to users of devices that can be used to access the company's resources including but not limited to:

- Desktop workstations.
- Laptop computers.
- PDA's and Smartphones.
- Cellular Phones of any type.
- Thin Client Terminals, collectively known as "end user devices".

The usage of the device includes both the use of the hardware and the software located on these devices.

This section of the policy, applies to all end user devices that access or interacts with company data and information systems.

3.1.1. Acceptable use

Company employees and other authorised users may make use of the end user devices for the purpose of conducting the company's business.

3.1.2. Unacceptable use

Users must not use the end user device for purposes that are illegal, unethical, and harmful to the company. Examples of what employees shall not do, include but are not limited to:

- **Secondary business use**: Conducting a personal business using the end user device.
- **Excessive use**: Excessive use of an end user device for personal use, which then interferes with business functions being performed by the device.
- **Personal software**: Loading of personal software (legal or illegal) onto the end user device without the prior permission of the IS/IT Manager or the employee's relevant manager. This also includes games whether legal or illegal.

3.2. Personally Owned Devices

Under special circumstances employees and other users are allowed to connect personal devices to the IT resources or facilities of the company. This includes connections to desktop computers, laptop computers, network points etc. This includes situations where the company has a "bring your own device" (BYOD) policy as an alternative to the supply of a company owned end user device.

Special care has to be taken in connecting these devices to the company's networks as the company could be liable for any and all information contained in these devices. This is particularly important if this information or software is transferred into the company IT systems, or if this information is not fully legally held by the user.

The personally owned devices being referred to include but are not limited to:

- Computers of any kind (Laptop, desktop, PDA, etc).
- Storage Devices (Memory Sticks, USB Hard Drives, Music Players, Data recorders).
- Communications devices (Cellular Phones, Modems, 3G Cards).
- Storage Media (CD and DVD Disk, Floppy Disks).

Personal devices are any devices that are not owned by the company, regardless of where the actual ownership resides.

3.2.1. Requirements

The following requirements must be taken into consideration in the use of personally owned devices.

- Personally owned devices of any kind can only be connected to the company's networks after permission has been obtained from the IT Department.
- Confidential company data should not be loaded onto any device without there being a critical requirement for the data to be stored on the device and prior permission having been obtained.
- Portable devices can be used for backup of less sensitive information if absolutely required e.g. the user is offsite at a location where the backup to the company's networks is either impractical (due to large size, cost) or impossible (unavailability of connection to companies network).
- Portable storage devices should not be used for long term backups of the user's data. This should be done on the company's servers.

3.2.2. In using a personal device for the purpose of accessing company systems and information special software may be loaded onto the device and a mobile device management system may be implemented centrally. With this system in place the company will be able to force certain security measures onto the personal device before access is allowed. This includes in addition to the normal requirements of company owned devices:

- Minimum Standards: The mobile device may need to have a minimum standard in terms of operating system version prior to the device being allowed access.
- Antivirus Protection: The mobile device may need suitable anti-virus and anti-malware software installed prior to being allowed access.
- Acceptable Configuration: The mobile device may need to have a configuration that is acceptable to the company prior to being allowed access e.g. devices that have been "jail-broken" or phones with specified apps installed may not be allowed access.
- Password Protection: The entire device or company area may need the user to enter a password prior to being allowed access. This password could be required every time the user enters the company area on the device.
- Password Strength: The password strength could be centrally set to ensure that it complies with Altron Policy.
- Encryption: It may be possible for all company related information or all information in either native or removable storage on the device to be encrypted to specified minimum encryption strength.
- Remote Lock Phone: It may be possible for the company or the user to lock a phone thus making it inoperable.

- Wipe Data: It may be possible for either the company or the user to delete all company related information in the mobile device. It may also be possible for the user to choose to wipe the entire device (perform a factory reset).Employee might have to sign a wipe waiver prior to accessing the company network authorising the company to wipe the mobile device when it deems it necessary.

3.2.3 Unacceptable use

Users must not use the personal devices for purposes that are illegal, unethical or harmful to the company. Example of this are:

- **Illegal Information**: Copying of unauthorised material onto the company's networks. The company would be liable if this information was found in the possession of the company. This includes the transfer of all types of Illegal Content.
- **Illegal and Harmful Programs**: Personal devices are not to be used for the transfer or loading of computer programs onto the company's IT resources, especially if these are illegal or potentially harmful software.
- **Pornographic Material**: Personal devices must not contain pornographic material if they are connected to the company's network and could thus become available on the network. Breach of this policy is subject to company disciplinary procedure. This applies to 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.

3.3. Use of Company IT Facilities

The company's IT facilities have been put into place for the benefit of the company and its business. Access to the IT resources and facilities is a privilege and such access is entirely at the discretion of the operations CEO/managing director or their specific delegates. Furthermore, access to the computing resources does not necessarily imply permission to use them, this permission needs to be granted. It is however understood that employees of the company, who have such permitted access may from time to time utilise certain part of the companies IT facilities for limited private use. Care should however be taken by the employees to ensure that the IT facilities are not abused, and at no time should private use hinder the operations of the business.

This policy applies to any IT facilities that are provided by the company, and to which the user has access. This includes:

- Printers.
- Scanners.
- Copiers.
- Server and Networked storage capacity.
- Server processing capacity.
- Server based applications e.g. SharePoint, Unified Messaging .

Company employees and other authorised users may make use of the IT resources and facilities for the purpose of conducting the company's business.

Users of the company's IT facilities are encouraged to:

- Take consideration of the environment and not print documents if not required, to attempt to print duplex (on both sides of the paper) if possible, or to print multiple pages in a single page in order to reduce the use of paper.
- Print out draft copies in draft mode if possible and print colour only when required (not for draft copies).

- Avoid storing multiple version of the same document either in server or workstation based storage, unless needed for business reasons.

3.3.1. Unacceptable use

Employees must not use the IT resources and facilities for purposes that are illegal, unethical or harmful to the company. Examples of what employees shall not do are:

- **Secondary business activities**: Use any company resources or facilities for performing any business activities not related to the company's business.
- **Private use**: Excessively use company resources or facilities for personal use.

3.4. Internet, E-mail usage and Social Networking

The Internet is a large, publicly accessible network of networks that has millions of connected users and organisations world-wide. The Internet is the base for the provision and search for information, for the transfer of E-mail messages outside the company, and the provision of collaboration services such as instant messaging, news groups, chat rooms, social networking etc.

Access to the Internet, social networking sites and e-mail is provided to employees for the benefit of the company and its business. Access to the Internet, e-mail and social networking sites is a privilege and such access is entirely at the discretion of the operations CEO/managing director or their specific delegates. Employees are able to connect to a variety of business information resources around the world, through the Internet. Internet access through the group company network is limited to group company employees and others that the group company may authorise.

Conversely, 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 policy has been established for using the Internet, e-mail and social networking.

The Internet, e-mail and social networking facilities provided by the company are primarily intended for official business usage and to enhance the company's business. Private and personal use, in moderation, will be tolerated, subject to the rules detailed in this policy. The company will not accept any liability regarding the use of the Internet or e-mail facilities and social networking sites when used for private use, and the employee hereby indemnifies the company against any such liability.

E-mail users need to clearly understand that the use of electronic communications may cause the company to be held liable for legal liability arising through or caused by such use.

The company will manage and monitor E-mail to allow for the most productive use of IT resources.
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. The company also reserves the right to block any type of message that is deemed not to be in the best interests of the company's business, e.g. download or upload of music files, images.

3.4.1. Acceptable use

Company employees and other authorised users may access the Internet, E-mail and social networking sites through the company's network for the purpose of conducting the company's business. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner.

Examples of acceptable use of E-mail are:

- Using e-mail for business contacts and correspondence.
- Utilising the Internet, including e-mail, as a tool to advance the business objectives of the company.
- Limit the size of message sent via E-mail and avoid the download of large files from the Internet, especially during working hours. This is to prevent overloading of the electronic communication system resources.
- Not altering the contents of the original e-mail when forwarding e-mail or replying to e-mail. If the content needs to be changed, then all changes must be clearly marked as such.
- Not deleting E-mail data or attachments if required for company business.

Examples of acceptable use of the Internet are:

- Using the Internet to obtain business information for company use from commercial or academic web sites.
- Accessing databases for information as needed for company business.
- Generally searching the Internet directly for information useful in achieving the user's business objectives.

Examples of acceptable use of Social Networking

- Group communications allowed to use social networking sites for business purposes and objectives of the company.

3.4.2. Unacceptable use

Employees must not use the Internet, e-mail or Social Networking for purposes that are illegal, unethical or harmful to the company (including statements, actions or omissions that do, or could, lead to civil and/or criminal liability to the company or fellow employees or damage or loss to the company or its reputation). Examples of what an Employee shall not do are:

- **Unacceptable content**: Receive and fail to delete, store, download, print, distribute, send or access any content or material that is offensive, harassing, fraudulent, racist, illegal or obscene (including any form of pornography as defined by the company). All other policies which refer to content are also applicable and should be taken into consideration by the user.
- **Spam**: Participate in e-mail "chain letters" or unsolicited e-mail ("spam"), for example, e-mail messages containing instructions to forward the message to others where not for official or company business purpose.
- **Sending Unnecessary Information**: Send or forward joke e-mails, electronic greeting cards, Christmas cards, copyrighted music files (e.g. MP3), copyrighted video clips (not related to official business) and games that can negatively impact on the overall performance of the company's communication resources.
- **Incorrectly Representing Company**: Represent personal opinions as that of the company via e-mail or publication of unauthorised statements onto web sites, blogs, wiki's, bulletin boards, discussion areas or newsgroups, etc. All other Altron Policies regarding the transfer of confidential business information to unauthorised parties need to be taken into consideration.
- **Modifying E-mail Messages**: Modify an e-mail message and forwarding or replying therewith without noting the changes, i.e. deletions, removal of recipients or modification of content.
- **Masking Sender Information**: Send, reply to or forward e-mail messages or other electronic communications which hides the identity of the sender or represents the sender as someone else.

- **Fraud**: Use information, e-mail, files, downloads or data to commit fraud or any other criminal offence/s.
- **Secondary Business**: Conduct a personal business using company resources.
- **Disclosure of Confidential Information**: Transmit confidential information to any person not authorised to receive it.
- **Harming others**: Conduct any form of a campaign that may be considered as damaging against fellow employee/s or any third party by e-mail or by any other electronic means.
- **Modem use**: Use a peripheral communications device (3G Card) whilst connected to the company's internal network. Under no circumstances is any modem allowed to be used when a workstation or laptop is connected directly to the company's network, thereby bypassing existing security mechanisms. The only exception to this statement is covered in the section entitled "Altron IT Security Policy" and should be discussed with the IT/IS Manager.
- **Obtaining restricted information**: Obtain or use copyrighted or restricted information to which the user does not have a right to obtain or use.
- **Abuse of the IT facilities**: Make unreasonable use of the Company's IT facilities in a manner which amounts to the abuse of the company's IT facilities.
- **Cautionary use*:*** Employees exercise caution when using public, internet communication platforms to transfer information.

3.4.3. E-mail identification & disclaimer notice

To ensure that an e-mail message is properly identified apart from the sender's e-mail address it is compulsory that the sender places an e-mail signature and link to a separate disclaimer notice on the company's web site at the foot of each individual e-mail message. The IT systems will automatically link in the disclaimer and signature to the message. Any disclaimer attached in this way must NOT be removed, changed or moved. The approved disclaimer is available from the group's various IT managers and it will be their responsibility to ensure that it is loaded onto all e-mail users' computers.

3.4.4. Monitoring

With due regard to the Constitution of the Republic South Africa and the Regulation of Interception of Communications Act and Provision of Communications-Related Information Act, in order for the company to effectively manage its electronic communication resources the company reserves the right to;

- Intercept, monitor, block, delete, read and act upon any incoming or outgoing direct and indirect communications including but not limited to e-mail messages addressed to or originating from the employee. This includes all E-mail messages, even personal E-mails sent or received using the company's facilities.
- Intercept, monitor, read and act upon the employee's Internet browsing habits, including the user's history files, web sites visited, files downloaded and stored by the user; and
- Intercept, monitor, block, delete, read and act upon any file, in whatever format, stored by an employee on any computer or other facilities of the company.

By using the company's communication and IT facilities, especially using the company's computers, each and every employee has given his or her written consent, or shall be deemed to have given such consent, to the above, by way of accepting the login message that will appear on the screen whenever a user logs into his computer. The company will respect the employee's right to privacy as far as is reasonably possible, subject to the protection of the company's rights and interest in and to its business.

The initial login screen will display the said consent and needs to be accepted prior to obtaining access to the computer.

3.5 Social media in a private capacity

3.5.1 Confidential information

It is acceptable to talk about work and have a dialog with the community. Publishing confidential information about the Altron Group is however unacceptable. Confidential information is defined in the Standard Terms of Employment for all employees and includes, without limitation of the generality of this term, unpublished financial information, details of current projects, future product ship dates, research, and trade secrets. Respect the wishes of customers regarding the confidentiality of current projects. Be mindful of the competitiveness of our industries.

3.5.2 Protect your own privacy

Privacy settings that limit others from seeing your information that is personal should be set. Be mindful of posting information that you would not want the public to see.

3.5.3 Respect Altron and its employees

Do not embarrass Altron, the Sub-holding Companies, Group Companies, our customers, or your co-workers in any way.
The public in general, and the Altron group's employees and customers, reflect a diverse set of customs, values and points of view. Do not state anything contradictory or in conflict with the Altron Group websites or official Altron Group documents. This includes not only the obvious (no ethnic slurs, offensive comments, defamatory comments, personal insults, obscenity, etc.) but also proper consideration of privacy and of topics that may be considered objectionable or inflammatory - such as politics and religion. Use best judgment and be sure to make it clear that any views and opinions expressed are yours alone and do not represent the official views of the Altron Group or Group Companies.

3.5.4 Protect Altron Group customers, business partners and suppliers

Customers, partners or suppliers should not be cited or obviously referenced without their approval. Never identify a customer, partner or supplier by name without permission and never discuss confidential details of a customer engagement. It is acceptable to discuss general details about kinds of projects and to use non-identifying pseudonyms for a customer (e.g., Customer 123) as long as the information provided does not violate any non-disclosure agreements that may be in place with the customer or make it easy for someone to identify the customer.

3.5.5 Controversial Issues

If you see misrepresentations made about Altron, your Group Company or brand in the media, you may point that out to Corporate Communications who are better equipped to handle these issues.

3.5.6 Time spent

Please be cognisant of the amount of time spent on social media platforms. Personal social media use should not interfere with your job or commitments to customers.

3.5.7 Disclaimers

Social media users and bloggers who identify themselves as employees of the Altron Group should include a prominent disclaimer saying that they're not speaking officially on behalf of the Group. The Altron Legal Department can assist you with applicable disclaimer language and assist with determining where and how to use it.

3.5.8 Enforcement

Violations of this section and other Altron policies relating to the use of e-mail and social networks and social media will be subject to disciplinary action, which may give rise to dismissal in cases of serious misconduct.

3.6. Malicious Software Protection

Malicious software consists of programmes such as viruses, trojan horses, spyware etc.
This type of software is designed to make unauthorised changes to programmes and data, or gather information and passwords from a person's computer or send messages from a person's E-mail system pretending to be that person. Therefore, viruses can cause destruction of corporate resources, loss of confidential data, disabling of communications facilities. It is important to know that malicious software is much easier to prevent than to cure. Defences against malicious software include protection against unauthorised access to computer systems, using only trusted sources for data and programmes, and maintaining virus-scanning software. Employees shall therefore;

- **Not knowingly introduce software**: Not knowingly introduce malicious software into end user devices.
- **Not deactivate antivirus**: Not deactivate the anti-virus scanning engine on the end user device.
- **Not update antivirus**: Ensure that the Anti-virus signatures and engine is updated within 1 week of updates becoming available, especially if working offsite.
- **Not program updates**: Ensure that the Windows and other programme patches are applied as required. A substantial part of these are security patches.
- **Not running programs**: Avoid running any programmes or opening documents that have not been obtained from a reliable and trusted source. Even software and documents received from a trusted source should be reconfirmed with the sender since the software of program may have been sent by a virus or other malicious code that infected their system.

3.7. User accounts and passwords

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorised employees have access to it. This access will be restricted to only those capabilities that are appropriate to each employee's job duties.

The protection of all data and systems that the user has access to is based on the username and password of the individual. Persons who obtain access to someone's username and password will most likely have access to all the systems and data that the user has access to. This access may not only be from within the company's premises but also from outside the premises and even from the Internet depending on how the systems have been configured.

Users need to take special care in the choice and the use of their passwords. Simple passwords can be easily guessed by others. Passwords written down and stored with the computer can be used by others. A password can also become known to people when you type it in.

Each employee shall:

- **Responsibility**: Be responsible for all computer transactions that are made with his/her User ID (username) and password.
- **Password confidentiality**: Not share logon usernames or 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 or kept where they might be easily obtained.
- **Password complexity**: Use passwords that will not be easily guessed by others. Passwords should not consist of the personal details of the user e.g. spouses name, children's name, residential area. A minimum length of 6 (six) complex characters are required for a password.

3.8 Physical security

It is company policy to protect computer hardware, software, data, and documentation from misuse, theft, fraud, unauthorised access, and environmental hazards. Care is taken to safeguard the electronic equipment assigned to employees. Employees who neglect this duty will be accountable for any loss or damage that may result.
An employee shall ensure that;

- **Secure storage of data**: Diskettes or any other storage media is stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked up.
- **Secure storage of data**: Diskettes or any other storage media are kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
- **Hazardous substances**: Other hazards to hardware such as food, smoke, liquids, high or low humidity and extreme heat or cold are avoided.
- **Changes to equipment**: No equipment installations, disconnection, modifications, and relocations are done without the permission of the IS/IT Manager.
- **Taking equipment offsite**: All users who are allocated laptop computers as part of their job role need to sign a consent form regarding use and safekeeping of the computer. Aside from this no equipment is to be removed out of the office without the informed consent of their department manager and/or IS/IT 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.
- **Unauthorized equipment**: Under no circumstance connect any other equipment to the group company's network without prior, written approval by the IS/IT Manager.

3.9. Software copyright and license agreements

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. Employees shall therefore;

- **Copyright protection**: Not duplicate, copy or give to any unauthorised persons any copyrighted software.
- **Software installation**: No software should be installed unless authorised by the IS/IT Manager who needs to verify that software is appropriately licenced. Only software that is licensed to or owned by the company is to be installed on company end user devices. Under no circumstances will any assistance/support be given on unauthorised or illegal products.
- **Downloaded software**: Not download and install software unless authorised by the IS/IT Manager.
- **Unlicensed software:** not install any software for which the company does not have sufficient number of licenses for the number of users.

3.10. Mobile and Home computing usage

Please note that this section of the policy applies to any employee with a company owned laptop, personal digital assistant, tablet or equivalent mobile device used to access the company's network or information resources whilst travelling to or from home or any other location. Employees with personally owned devices should however take due consideration of the items below in the best interests of the company. Employees who carry and use mobile devices are at risk due to the mobile nature of these devices. Employees should thus take due care to ensure that mobile devices are not lost or stolen, nor that data is accessed by unauthorized persons. Employees thus need to be vigilant to the environment in which they are working in and concerned for the safety of the mobile device.

Employees shall therefore ensure the following:

- **Password protection**: Ensure that access to information contained on the mobile device will be protected by a minimum of a password into the operating system and screen savers. Additional access control through the device's BIOS or hardware levels are encouraged. This needs to be enabled by the IT department.
- **Encryption**: Where possible ensure that encryption for business related information is put into place by means of the device's operating system or any other similar application. This needs to be enabled by the IT department.
- **Unauthorized users:** Ensure that under no circumstances any unauthorised user is allowed to use the mobile device. This includes lending the device or handing over physical possession of the device to an unauthorised party.
- **Secure communications**: Ensure that when the company's network is accessed from home or during a business trip that the necessary security software that will establish secure communication to the company's security systems is utilised.
- **Foreign travel**: Understand that when travelling abroad all communications can be and frequently are intercepted and recorded.
- **Reading screens**: Take care that when travelling, especially in aircraft, buses or any other public transport, that external parties could easily read information off screens. Necessary caution should be exercised when working on company related information in public or non-company areas.
- **Hand luggage**: Ensure when travelling by aircraft, bus or any other means of mass or public transport, that the device is carried as hand luggage and not checked in. This will prevent damage to the device or the theft thereof.
- **Hotel security**: Ensure when staying in hotels to make certain that the device is locked in the hotel's safekeeping and not left unattended in the hotel room.
- **Device identification**: Make sure that the carry case and device is clearly identified by taping contact details onto it, for example by taping a business card onto the back of the device. Other methods of identifying the device, for example engraving or fluorescent marking are encouraged.
- **Storage in car**: Make sure that if you are unable to take the device with you it is locked away from sight when left in a vehicle, for example in the vehicle's boot – including when travelling. This does not include extended periods such as overnight, when the device shall be stored securely outside the vehicle.
- **Device locking**: Ensure that the device is securely locked with the supplied security cable when working at a desk outside of the company.
- **Data backups**: Make backups of crucial files on the device at least weekly and store it separately from the device on the company's server.
- **Passwords security**: Not save any passwords or access codes anywhere on the device. This includes taping notes onto the device or keeping it inside the carry case of the device.

- **Environmental protection:** Not leave the device in direct sunlight or where it is exposed to any other environmental hazards such as dust, liquids, chemicals and food. In the event that liquid is spilt onto the device, attempt to drain all excess liquid – DO NOT TURN THE DEVICE ON. Return it to the IS/IT Manager as soon as possible.
- **Cleaning**: Not use household chemicals or water to clean the device – use a dust cloth.
- **Physical protection**: Not drop or knock the device and perform a regular check on the condition of the strap of the carry case and the carry case itself.
- **Theft reporting**: In the event of a mobile device being stolen, immediately report the theft to the company IS/IT Manager to arrange for all security access to be suspended.

4. Acknowledgement of End User Policy

Each employee assigned a desktop or laptop computer or a mobile device, workstation or network account needs to sign the following acknowledgement form and return it to the IS/IT Manager who will then ensure that it is included in the relevant employee's personnel file.

Acknowledgement of the
Altron End User Policy

Acceptance of the end user policy

This form is used to acknowledge receipt of, and confirm agreement with, the [COMPANY]'s *End User Policy*.

Procedure:
Complete the following steps:

1. Read the "Altron End User Policy". If there are any aspects regarding this policy that are unclear please consult with your IS/IT Manager.
2. Sign in full and complete the details in the spaces provided below.
3. Return this acknowledgement form to your IS/IT Manager for record keeping purposes.

Signature
By signing below, I agree to the following terms:

- I have received and read a copy of the "*Altron End User Policy* " and understand the same.
- I understand and agree that any computer, software, and storage media provided to me by [COMPANY] contains proprietary and confidential information about [COMPANY] and its business and remains the property of the company at all times.
- I agree that I shall not copy, duplicate (except for purposes as part of my job here at [COMPANY]), or otherwise disclose, or allow anyone else to copy or duplicate any of the information or software on any computers, software or storage media provided to me.
- I agree that, if I leave [COMPANY] for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, storage media or computer equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control.
- I agree to abide by the terms set out in the "*Altron End User Policy*" and to be bound thereby. In particular, I understand and accept that in appropriate circumstances the [COMPANY] may monitor and intercept the information, data and e-mail on my computer, and I hereby grant my consent for such monitoring and interception in terms of section 5 and 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002.
- I understand and agree that failure on my part to comply with the terms as set out in the "*Altron End User Policy*" and this acknowledgement form may result in disciplinary action being taken against me.

Employee signature: _____

Employee name: _____ Personnel Number _____

Department:_____ Date: _____