ALTRON POLICY MANUAL

PART C - SECTION 5

DATA PROTECTION POLICY

Data Protection Policy of Allied Electronics Corporation Limited ("Altron")

Introduction

Altron and its subsidiaries ("the Altron group") collect, retain and use certain personal information of shareholders, staff members, suppliers, customers, business partners, associates and other stakeholders of Altron group (collectively, "data subjects") for the purposes of satisfying operational and internal and external governance requirements, and legal obligations. Altron recognizes the importance of the correct and lawful treatment of the personal information of both juristic persons and natural persons, and it expects its group companies and staff to do the same. Altron places a premium on high levels of ethical conduct as reflected by its *Code of Conduct,* its *Corporate Compliance Policy* and its *Code of Ethics,* all of which are published on Altron's public website with address ***www.altron.com***.

The types of personal information that the Altron group may deal with includes information about: current, past and prospective employees; company shareholders; suppliers; customers; business partners and associates; and others with whom it deals with or communicates. This personal information, whether it is held in paper format, on computer or other media, will*, inter alia*, be subject to the appropriate legal safeguards as specified in the Protection of Personal Information Bill and the legislation that may eventually arise therefrom ("POPI").

Altron fully endorses POPI and adheres to the eight conditions contained therein. These conditions specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal information. Employees and any other persons, for example contractors, who obtain, handle, process, transfer and store personal information for and on behalf of the Altron group ("operators") must adhere to these conditions.

For the purposes of this Policy, the "data subject" shall mean the person whose personal information is processed; "operator" means a person who processes personal information for a responsible party; "processed" means the collection, use, storage and every other activity in connection with the personal information in any manner whatsoever; the "responsible party" shall mean the person who determines the purposes of and means for processing personal information; and the "third party" shall mean the person to whom the personal information is disclosed. The definitions contained in POPI shall be deemed to apply to this Policy.

Application and status of this Policy

This Policy is applicable to the Altron group as a whole and all staff members and group companies are required to comply with this Policy. Depending on specific needs, circumstances and requirements, individual Altron group companies may adopt their own specific policies dealing with the subject matter hereof, provided the principles contained in this Policy and POPI are adhered to.

This Policy has been approved by the Altron Chief Executive and non-adherence hereof will not be tolerated.

Any employee who is aware of or has reason to believe that the Policy has not been followed should immediately raise the matter with their Line Manager or the relevant Altron group Information Manager or his/her deputy in the first instance.

Conditions

The 8 conditions require that personal information shall:

1. be dealt with only in a manner that ensures that the conditions are complied with **(Accountability);**
2. be processed lawfully and reasonably, in a manner that does not infringe the privacy of the data subject, in a minimal manner regarding its stated purpose, with the consent of the data subject or as necessary in terms of contractual obligations and obligations imposed by law, or to protect a legitimate interest, or the performance of a public law or duty, or to pursue the legitimate interests of the responsible party or a third party **(Processing Limitation);**
3. be dealt with in a manner that is purpose specific **(Purpose Specific);**
4. only be processed further if it is compatible with the purpose of the original collection **(Further Processing Limitation);**
5. be dealt with in a manner that ensures the quality and correctness of the personal information **(Information Quality);**
6. be processed in a manner that is open and transparent **(Openness);**
7. be dealt with in such a manner that the security and integrity of personal information is safeguarded by the responsible party **(Security Safeguards);** and
8. be processed subject to the data subject's right to participate in the entire process **(Data Subject Participation).**

Satisfaction of conditions

In order to meet the requirements of the conditions, the Altron group will:

- observe fully the conditions regarding the fair collection and use of personal information;
- meet its obligations to specify the purposes for which personal information is used; and to only use personal information for which consent was specifically given or for a compatible purpose;
- collect and process appropriate personal information only to the extent that it is needed to fulfill operational or any legal requirements;
- ensure the quality of personal information used and ensure that the personal information is accurate, current and available on request;
- apply strict checks to determine the length of time personal information is held;
- ensure that the rights of persons whose personal information is processed, can be fully exercised under POPI;
- take the appropriate technical and organizational security measures to safeguard personal information;
- ensure that personal information is not transferred across borders if the recipient party is not regulated by laws or legal obligations similar to what is contained in POPI; and
- ensure that personal information is not transferred to a third party without the data subject's consent. Such third party must have adequate data security measures in place and the third party must maintain the confidentiality of the personal information.

Designated Data Controller

Altron's Information Manager, for purposes of POPI, is responsible for ensuring compliance with this Policy and POPI on behalf of the Chief Executive Officer. The initial Information Manager is Chris Potgieter, the Altron Group Legal Manager. Any questions or concerns about the interpretation or operation of this Policy should be taken up in the first instance with the Information Manager. The Information Manager will also be the contact person for any complaints about the accuracy of personal information, or any other relevant complaint relating to this Policy.

Data Subject Access

All persons who are the subject of personal information held by the Altron group are entitled to be able to access and amend their personal information; subject to legal requirements are entitled to demand that their personal information is removed from the system; and shall be entitled to stipulate that their personal information may not be transferred to third parties.

On a regular basis, Altron group companies must ensure the accuracy and completeness of personal information. Altron group companies must verify the identity of persons who request access to personal information. Where consent has been given to transfer personal

information to third parties, and where there are changes to personal information, third parties must be advised accordingly.

Employee Responsibilities

All employees are responsible for checking that any personal information that they provide to Altron group companies is accurate and up to date; and for informing the Altron group of any changes to personal information, e.g. changes of address.

If, as part of their responsibilities, employees collect information concerning other people (for example, without limitation, other employees in the Altron group or of customers), they must comply with this Policy.

It is part of the responsible party's responsibilities to ensure that personal information is not retained for longer than is necessary to achieve the purpose for which the information is collected. Every employee will assist in achieving this legal requirement. It is the responsible party's responsibility to ensure that the personal information is destroyed at the end of the agreed period or when the personal information is no longer in use. Every employee will assist in achieving this legal requirement.

Data Security

The need to ensure that personal information is kept securely means that precautions must be taken against physical loss, damage, tampering, manipulation or theft and that both access and disclosure must be restricted. The responsible party and its employees are responsible for implementing appropriate actions and measures to ensure that adequate security and technical means are in place to protect the confidentiality, integrity and availability of the personal information. The responsible party must also ensure that all its operators have similar security and technical measures in place in order to comply with the responsible party's obligations. Such measures shall entail that: all reasonably foreseeable internal and external risks to personal information in its possession be identified; appropriate safeguards against such identified risks be established and maintained; regular verification of the effective implementation of such safeguards is undertaken; safeguards are continually updated in response to new risks or deficiencies in existing safeguards; due regard be had to generally accepted information security practices and procedures which may be generally applicable or be required in terms of specific industry or professional rules or standards.

Any personal information security breach will be reported to the data subject and will be dealt with as a serious incident.

If the data subject's consent has not been obtained, personal information will not be disclosed either verbally (orally) or in writing or otherwise to any unauthorized third party.

Rights to Access Information

Employees and other data subjects whose personal information is held by the Altron group have the right to access any personal information that is being kept about them on computer and also have access to paper-based personal information held in certain manual filing systems. This right is subject to certain exemptions which are set out in POPI. Any data subject who wishes to exercise this right should make the request in writing to the relevant company's Information Manager. Such request is to follow the procedures laid down by the Promotion of Access to Information Act, No. 2 of 2000.

Altron companies reserve the right to charge the maximum fee payable for each data subject's access request. If personal information is inaccurate, it can be amended upon request. Where no fee is allowed to be charged by law Altron companies will not charge a fee.

The Altron group aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of a written request, unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to such person making the request.

Publication of Personal Information

If information is already in the public domain, for example, personal information of a data subject contained in the published media, such personal information may be published by the responsible party. Any individual who has good reason for doing so, may request that his personal information must be excluded from such publications or that it be changed or updated, and such request should be directed to the relevant company's Information Manager.

Data Subject Consent

The need to process personal information for normal business purposes must be communicated to all data subjects. In some cases, if the personal information is sensitive, namely information about religion or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information of a data subject or criminal history in relation to an offence allegedly committed by a data subject (collectively, "special personal information"), express consent to process the special personal information must be obtained. Processing may be necessary to comply with other Altron group policies,

such as policies dealing with health and safety and equal opportunities, and with requirements of laws such as the Employment Equity Act. In the case where laws require the disclosure of personal information or even special personal information, the consent of the data subject is not required.

Retention of Personal Data

Some forms of personal information will be kept for longer periods than others. All employees are responsible for ensuring that personal information is not kept for longer than is strictly necessary. In this regard employees are referred to the retention period schedules attached to the Altron group's Records Management Policy as can be viewed on *Alix,* the Altron group's intranet, for guidance.

Data Subject's Rights

In the event of the responsible party not complying with this Policy, the data subject will be entitled to institute legal action against the responsible party for damages suffered by the data subject as a result of such non-compliance. The data subject will also be entitled to raise any matter with the Information Regulator.

Non-compliance

It is to be noted that non-compliance with POPI, the basic requirements of which are reflected in this Policy, can potentially lead to: claims for civil damages (including punitive damages); administrative fines of up to R10 million; or criminal prosecution where unlimited fines and imprisonment of between 1 and 10 years are prescribed.

Compliance with this Policy, and accordingly with POPI, is accordingly not negotiable and the strictest of actions will be taken where employees are found to act contrary to this Policy or POPI.

Third Party Service Providers

It is of the utmost importance to ensure that where the group makes use of external operators and third party service providers such as consultants, sub-contractors, professional advisers etc., to whom access may be given to the personal information of data subjects the protection of which is the responsibility of the group, such operators and third party service providers must contractually undertake to comply with POPI and the 8 basic conditions contained therein (and also forming part of this policy); to have appropriate technical and organizational security measures in place of such a standard as acceptable to the group and in respect of

which the group must have the right to inspect and audit same from time to time; and to indemnify the group and to hold the group completely harmless from any liabilities, damages, claims, losses or any other consequences which may be made against the group or which the group may suffer, which may be caused, directly or indirectly, by any failure (whether it be innocent, negligently or intentionally) of the third party or its staff, contractors or representatives, to comply with its obligations under POPI.