CIS GROUP

CODE OF CONDUCT

2025

Contents

1. INTRODUCTION 5
2. CIS GROUP VALUES 5
3. CODES OF ETHICS 5
3.1 Shareholders and Owners 5
3.2 Directors and Managers 6
3.3 Relation with Suppliers and Clients 6
3.4 In Relation to Competitors of the Company 6
3.5 Relation with Employees 7
3.6 Relation with Civil Society 8
4. General Standards 8
4.1 Compliance with Applicable Laws and Policies 8
4.2 Conflict of Interest 8
4.3 Outside Directorships and Other Outside Activities 9
4.4 Use of Company Resources 9
4.4.1 Internet and Electronic Mail Policy: 9
4.4.2 *Equipment and Supplies:* 10
4.4.3 *Proper Use of Organizational Assets:* 10
4.4.4 *Political Activity:* 11
4.5 Fairness and Justice 11
5. RESPECT FOR HUMAN RIGHTS 11
5.1 Equal Employment 11
5.2 Respect for Employees 12
5.3 Safe and Healthy Working Environment 12
5.4 No Child Labor 12
5.5 Discrimination & Harassment 12
6. CONDUCTING BUSINESS WITH INTEGRITY & FAIRNESS 13
6.1 Confidentiality and Privacy 13
6.2 Trade, Antitrust and Fair Dealing 13
6.3 Fraud - Protection of Company Assets/Accounting 13
6.4 Anti-Bribery and Anti-Corruption 14
6.5 Assignment of Personnel 14
6.6 Communication 14
6.7 Gifts, Meals and Entertainment 14
6.8 Advertising and Marketing 15
7. ETHICAL PERSONAL CONDUCT 15

7.1 Corporate Opportunities 15
7.2 Proper Maintenance of Records 15
7.3 Business Communication and Public Disclosure 15
8. COMPLIANCE WITH THE CODE 16
9. REPORTING ILLEGAL OR NON-COMPLIANT CONDUCT 16
9.1 Reporting 16
9.2 Consequences of Not Reporting 16
9.3 Investigating 17
9.4 Disciplinary Action 17
10. ETHICS 17
11. CERTIFICATES 18
12. USEFUL NUMBERS & ADDRESSES 19
ANNEX A EMPLOYEES ACKNOWLEDGEMENT FORM 20
ANNEX B SUPPLIERS ACKNOWLEDGEMENT FORM 21
ANNEX C CIS PROCEDURES TO FOLLOW ON-BOARDING RESELLERS AND END-USERS: 22
ANNEX D INTERNATIONAL TRADE COMPLIANCE 24
CIS INTEGRATION BUSINESS 28
HIPERDIST DISTRIBUTION BUSINESS 29
CIS PROFESSIONAL SERVICES BUSINESS 30

Dear CIS Family,

Since the inception of CIS, we have built strong relationships with our clients, vendors and communities by providing outstanding services and doing business according to the highest ethical standards, wherever we operate and whatever situation. Our commitment to the principles of common purpose, ethical behavior and leadership helps us to overcome the challenges we face and maintain the trust of our stakeholders throughout the countries the CIS Group is covering.

CIS Group's Code of Conduct outlines the standards that must direct our behavior. In today's economic environment, conducting business responsibly and ethically is critical to protecting our reputation for integrity and maintaining our competitive advantage. If you have any questions or concerns about your own conduct or that of others, I urge you to seek guidance from the Human Resources and Legal Departments of the group.

All our people must not only read the Code but also adhere to its letter and spirit. CIS Group's values and reputation are defined by our actions and the decisions we make every day. Through our own individual commitment to the Code, we uphold CIS Group's legacy and ensure our future as a leading ITC group.

This Code of Conduct applies to all CIS entities and business partners companies.

Thank you for all that you do for our company and our clients.

Antoine Kareh
General Manager

1. INTRODUCTION

This Code is based on the following basic assumptions:

Ethics are a key requisite in guaranteeing and corresponding the rights and interests of all stakeholders involved with CIS Group: employees, clients, shareholders, suppliers & business partners, and the society at large.

Ethics are a necessary element for companies in the 21st century to adequately meet their objectives, to the degree that Ethics ensure rigorous compliance with companies' applicable legislation, and internal regulations.

Ethics within the company require that shareholders and owners become guarantors of the compliance in respect to obligations of the management.

Even though this Code has been created with the intention of being applicable in general to all companies of CIS Group, it should also be understood that it is adaptable to specific circumstances of each business; thereby ensuring that it contemplates application of the principles of Ethics and sustainable development in accordance with the specific activity of the company involved.

2. CIS GROUP VALUES

- Quick and agile yet reliable and persistent.
- Innovative embracing yet experienced, and field tested.
- Leading and pioneering yet delivering and performing.

3. CODES OF ETHICS

3.1. Shareholders and Owners

In the exercise of their ownership rights, they should:

- Configure their company as an instrument at the service of creating wealth, making their indisputable objective of obtaining a profit compatible with sustainable, environmentally sound social development, ensuring that all activities are carried out in an ethical and responsible manner.
- Configure the company as a medium and long-term entity, not compromising its continuity through an interesting short-term enrichment.
- Exercise voting rights at the General Shareholders' Meetings on an informed and responsible basis and, in doing so, always demand ethical behavior from the company, including approval of the Code of Ethics and orchestrating effective application thereof.
- Search for a fair balance between capital and work, in such a fashion that, through their salaries, workers receive just compensation for their work.
- Appoint as directors and managers, professionals who meet the requisites established regarding adequate preparation and experience, and who carry out management functions in a professional, ethical and responsible manner.
- Define and defend the mission and values of the company in accordance with its Code of Ethics.

3.2. Directors and Managers

In relation to management functions:

- Carry out their activities in a professional, ethical and responsible manner.
- Ensure that the pricing given by a vendor for a deal must be reasonably applied as profit for that deal only. No provision can be made for marketing funds, or margin shortfalls or costs incurred by error in other deals. One example of a compliance fail in this context would be agreeing to do a deal at low margin with the corresponding margin recovery being loaded on a future deal. That second deal would be in breach of compliance. Another example would be if we agree to a margin on the HW component of a deal that compensates us for buying the Cloud element but invoicing the latter at a subsidized or even zero value.
- Comply and demand compliance with the Code of Ethics of the company and, to that end, make the Code known and establish appropriate mechanisms to guarantee application.
- Keep the books and ledgers of the company in an accurate and honest manner, in order to permit that information be obtained and decisions be taken on an informed and responsible basis.
- Provide external and internal auditors of the company with all such information and explanations as may be required to carry out their work.
- Immediately notify the administrative body as to any event or situation, which would represent or could give rise to a conflict between the interests of the company and the individual interests of the director or manager, and abstain from intervening in the resolution.
- Ensure a succession plan for key positions within the company, to guarantee the continuity of the company does not depend on the presence of any given director or manager.
- Choose their collaborators and subordinates in accordance with the principles of merit and capacity, based on performance management.

3.3. Relation with Suppliers and Clients

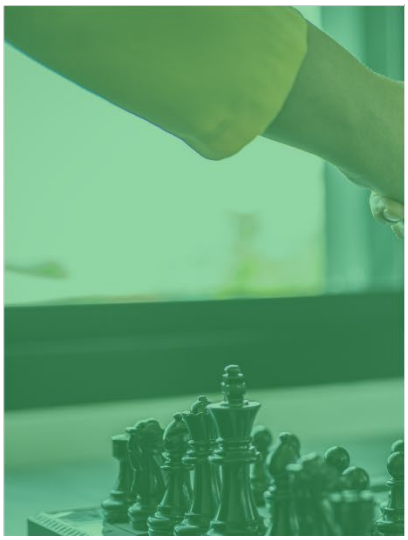
In relation to Suppliers and Clients of the Company:

- Maintain ethical and legal relationships with suppliers of goods and services.
- Search for and select only suppliers, whose business practices respect human dignity.
- Select suppliers on the basis of the appropriateness of their products or services, as well as of their prices, delivery conditions, and quality.
- Aspire to excellence in the goods and services of the company in such a way that clients and consumers obtain the satisfaction expected therefrom.
- Guarantee the products and services of the company and deal quickly and efficiently with consumer and user claims, with a view to achieving satisfaction beyond mere compliance with prevailing legislation.
- CIS Group Partners must provide a high level of customer service, including assisting customers in obtaining in-warranty and out-of-warranty services, professional call handling, and Customer Relationship Management.
- In the scope of business, CIS established a procedure to verify resellers and end-user profiles as stated as in the annex B for on boarding resellers and end users.

3.4. In Relation to Competitors of the Company

Compete in good faith with other companies cooperating to achieve a free market based on mutual respect between competitors and abstaining from engaging in unfair practices.

In particular, not employing unethical methods to take clients away from competitors.



3.5. Relation with Employees

In relation to Employees of the Company:

This present Code is an integral part of internal regulations of each company in CIS Group.

- Treat employees with dignity, respect, and justice, taking into consideration their different cultural sensitivities.
- Not permit any form of violence, harassment,or abuse at the workplace.
- Recognize the rights of association, union membership, and collective negotiation.
- Promote the professional development, training,and promotion of employees.
- Link remuneration and the promotion of employees to their conditions of merit and capacity. (Overtime, Targets, Project Completion)
- Establish and communicate clear criteria and rules, which maintain a balance between the rights of the company and those of employees in hiring processes, and in the separation thereof, even in the case of a voluntary change in employee.
- Seek to integrate persons with disabilities into the workforce, eliminating all barriers within the company to achieve full inclusion.
- Facilitate the participation of employees in the social action programs of the company.
- Ensure that all employees receive a salary equal to or greater than the legally mandated minimum wage or applicable union agreements, maintaining compliance with wage laws, promoting fair compensation, and upholding equitable workplace practices.
- Ensure that all employees receive at least one day of weekly rest, that weekly working hours do not exceed 44, and that any overtime is conducted in compliance with the maximum weekly duration and corresponding compensatory rest periods as required by local law. In case of overtime, employees are compensated with additional leave.

3.6. Relation with Civil Society

In relation to the Civil Society:

- Respect human rights and democratic institutions, and promote them wherever possible.
- Maintain the principle of political neutrality, without interfering politically in those communities where they carry out their activities.
- Maintain licit and respectful relationships with public authorities and institutions, not accepting or offering gifts or commissions in cash or in kind.
- Collaborate with Public Entities and non-governmental entities and organizations dedicated to improving levels of social attention for disadvantaged persons.

4. General Standards

We also ensure that all stakeholders involved in the CIS Group, "comply with International Standards" in relation to Money Laundering, as well as with the sanctions imposed on the governments of the countries in which the entities of the Group are located.

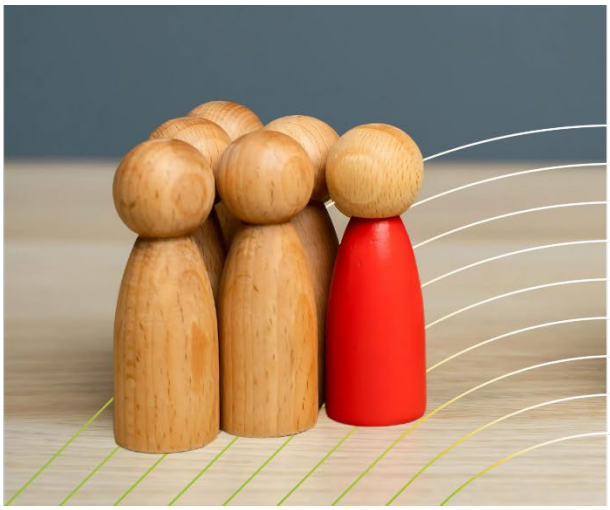
4.1. Compliance with Applicable Laws and Policies

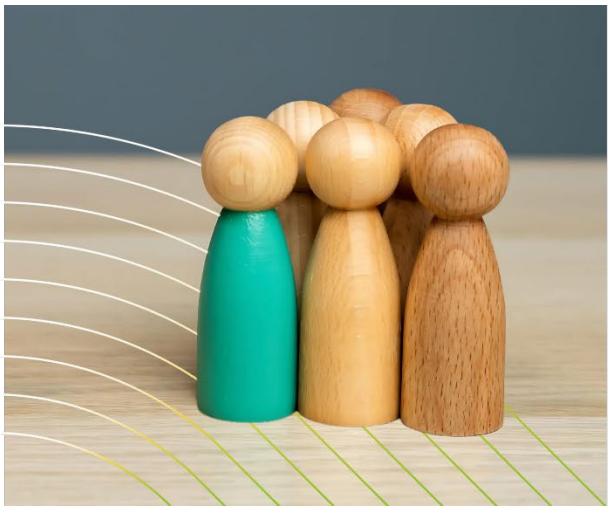
We ensure compliance with all applicable laws and regulations of CIS Group, and they must never be compromised. Additionally, employees shall adhere to internal rules and regulations as they apply in a given situation. Those internal rules are specific to the group and may go beyond what is required by the law.

4.2. Conflict of Interest

All stakeholders of CIS Group will always act in the best interests of the Group.

A Conflict of Interest occurs when personal interests of an employee or the interest of a third party compete with the interests of CIS Group. Employees shall avoid Conflicts of Interest whenever possible.





CIS Group Employees shall avoid any conflict - real or potential - between their personal interests and the interests of the Group. Private interests include any advantage to an employee or his/her family members, close relatives, friends, persons or organizations with whom they have or have had business or political relations with. Any employee of CIS Group, in case of Conflict of Interest, shall disclose it to his or her Line Manager and/or the HR or the Legal division to resolve the situation in a fair and transparent manner.

CIS Group Partners must avoid engaging in any business activity that would create a Conflict of Interest relating to their partnership with the group. Partners must not ask or encourage CIS Group employees to late the provisions of CIS Group Standards of Business Conduct and Ethics.

4.3. Outside Directorships and Other Outside Activities

We take pride in CIS Group's reputation and consider our best interests also in our outside engagements and activities outside of CIS Group. No activity shall be pursued should it interfere with the employee's responsibilities for CIS Group, or create risks for CIS Group's reputation, or in any other way conflict with the interests of the Group.

When in doubt about the permissibility of an activity, employees shall consult with the HR or the Legal or Compliance Function. Unless requested by the Company to take up a particular position or activity, employees shall pursue outside activities and positions at their own risk and cost and within their spare time only.

4.4. Use of Company Resources

4.4.1. Internet and Electronic Mail Policy:

- Employees may use Internet and send and receive electronic mail solely for business purposes.
- CIS Group's electronic mail system is a company resource, and CIS Group's Management reserves the right to read, view and copy any email communication.
- Employees must take reasonable care not to disclose confidential information, or acquire unauthorized information over the Internet.
- No one should access CIS Group's Information Systems without an authorized user identification code (user ID) and password.
- When creating a password that meets complexity standards, it's important to include a mix of uppercase letters, lowercase letters, numbers, and special characters.
- Receiving a user ID requires approval of the individual(s) responsible for the system in question. User IDs may be revoked or disabled to protect the system at any time. In case the employee terminates the relationship with the CIS Group, his/her user ID will be revoke. As for inactive user IDs, those are temporarily disabled until needed. Each user is responsible for/required to change his/ her password at least every ninety (90) days.

When creating a password that meets complexity standards, it's important to include a mix of uppercase letters, lowercase letters, numbers, and special characters.

Here’s an example: **P@ssw0rd!23**

This password includes:

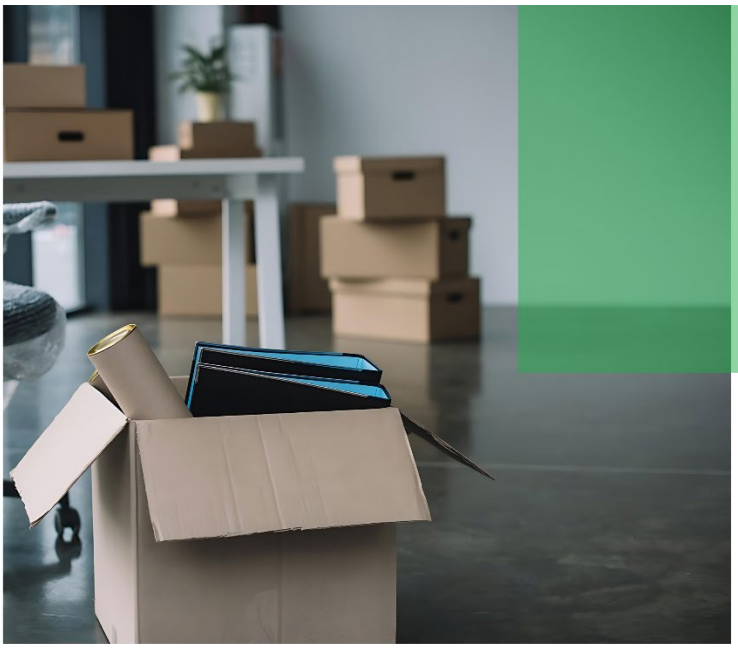
- Uppercase: P
- Lowercase: sswrd
- Numbers: 0, 2, 3
- Special character: @, !

4.4.2. *Equipment and Supplies:*

All equipment and supplies purchased by CIS Group remain CIS Group's property, including but not limited to office supplies, office furniture, fax machines, computers, software, hardware, supplies and equipment and may not be used by CIS Group's employees for personal reasons.

4.4.3. *Proper Use of Organizational Assets:*

- CIS Group Employees may only use, transfer, or dispose of funds or assets for the lawful and legitimate business purposes for which they were approved by CIS Group Management.
- All information systems resources will be protected against fire, water, physical damage and theft. The appropriate protection will be selected from among physical barriers, environmental detection and protection, insurance, and other risk management techniques. Also, the group's information must be daily kept and stored on an External System.
- CIS Group Data Center (Server Room) is equipped with an access control system with closed circuit camera surveillance, only authorized employees can access the room.
- All data and program files on CIS Group Information Systems are protected against unauthorized changes. Sensitive data and program files are protected against unauthorized reading and copying. CIS Group System Administrator and Senior Management shall control which user IDs can read and/or write to any given file. Every file shall be associated with an owner. The owner of each file is responsible for specifying whether the file is sensitive and which user IDs should be allowed to read and/or write to it.
- When technically feasible, applications and systems should automatically enforce this. CIS Group applications are programmed so that only users with authorized user IDs can access them.



4.4.4. *Political Activity:*

- Employees may not use CIS Group's resources, reputation or assets to support a political candidate.
- Corrupt payments to Political Parties or Party Officials or candidates for Political Office or Government Officials to obtain or retain business, or to gain any other improper business advantage, or to get any government authorization or documentation, such as any approval, permit, or license are strictly prohibited.
- Although these requirements apply to all corporate transactions, a CIS Group Employee should take special care to ensure that any expenditure of Company funds related to any Government Official or Other Covered Party, is accurately and completely documented, regardless of the amount of such transactions.

4.5. Fairness and Justice

CIS Group is committed to dealing fairly with its clients, suppliers, distributors, partners, competitors, and employees. No person acting on behalf of CIS Group may take advantage of anyone through manipulation, abuse of confidential information, misrepresentation of material facts, or any other unfair dealing or practice.

5. RESPECT FOR HUMAN RIGHTS

5.1. Equal Employment

CIS Group believes that diversity in our staff is critical to our success as a global organization, and we seek to recruit, develop and retain the most talented people from a diverse candidate pool. Advancement at CIS is based on merit. We are fully committed to equal employment opportunities and compliance with the letter and spirit of the full range of laws regarding fair employment practices and non-discrimination.

The Human Resources Director of CIS Group is ethically responsible for promoting and fostering Equal Employment for all employees and candidates.

Following points must be considered:

- The organization must realize the intrinsic value of its employees.
- Giving opportunities to the employees equally to develop their competency skills.

- Making employees feel as if they own the organization, so that they would be committed towards it.
- Laying down policies and procedures, which will ensure equitable treatment for all.
- The individual goals of an employee must be streamlined with the organizational goals. Individual goals of an employee should not obstruct him/her to achieve the organizational goals.
- The organization must be fair and honest with its staff. Decisions taken by the management must be ethical and legal.

5.2. Respect for Employees

We shall create and maintain a working environment in which the dignity of employees is mutually preserved. A climate in the workplace should be created and maintained wherein there is no concession for the following:

- Any verbal or non-verbal conduct that undermines the person's dignity and privacy.
- Talking badly about others behind their backs.
- Lying, gossiping, manipulating, false testimonies, and bad influence.
- Indecent or improper clothing

CIS Group respects the privacy of its staff and will not seek to regulate private conduct unless such conduct impairs the ability of the employee to perform work satisfactorily.

5.3. Safe and Healthy Working Environment

CIS Group is committed to conducting its business in a manner that delivers leading Environmental, Health and Safety performance. This is consistent with our commitment to corporate citizenship, social responsibility, and sustainability.

The health, safety, and wellbeing of all employees, contractors, and stakeholders are fundamental priorities. No activity or decision shall be pursued that compromises the safety of individuals or creates risks to the health and wellbeing of others, either within the workplace or in any external engagements. All individuals are expected to uphold the highest standards of health and safety, complying with relevant regulations, including the Work Health and Safety Act 2001, ISO 45001, and applicable local laws. Any actions or conditions that conflict with these standards, or that could jeopardize the safety, security, or integrity of operations, must be reported promptly to maintain a safe and sustainable working environment.

By adhering to these principles, all individuals contribute to a culture of responsibility and proactive risk management, aligning their conduct with the broader commitment to corporate social responsibility and environmental stewardship.

5.4. No Child Labor

The law categorically prohibits the employment of children who have not completed sixteen years of age/ thus no person shall be employed at an age younger than 16.

The company must take the necessary preventive measures to ensure that it does not employ anyone below the legal age of employment.

5.5. Discrimination & Harassment

We embrace diversity and respect the personal dignity of our fellow employees. CIS Group respects the personal dignity, privacy and personal rights of every employee and is committed to maintaining a workplace free from discrimination and harassment.

Therefore, employees must not discriminate on the basis of origin, nationality, religion, race, gender, age, or sexual orientation, or engage in any kind of verbal or physical harassment based on any of the above or any other reason. Employees who feel that their workplace does not comply with the above principles are encouraged to raise their concerns with the HR Department.

6. CONDUCTING BUSINESS WITH INTEGRITY & FAIRNESS

6.1. Confidentiality and Privacy

- We value and protect our confidential information and we respect the confidential information of others. CIS Group continued success depends on the use of its confidential information and non-disclosure to third parties. Unless required by law or authorized by their management, employees shall not disclose confidential information or allow such disclosure. This obligation continues beyond the termination of employment. Furthermore, employees must use best efforts to avoid unintentional disclosure by applying special care when storing or transmitting confidential information.
- All employees, and especially those who are involved in marketing, sales and purchasing, or who are in regular contact with competitors, have the responsibility to ensure that they are familiar with applicable competition laws. When in doubt, the Legal division should be contacted in order to provide competition law advice and training.
  CIS Group respects that third parties have a similar interest in protecting their confidential information. In case those third parties, such as joint ventures, partners, suppliers or customers, share with CIS Group confidential information, such information shall be treated with the same care as if it was CIS Group's confidential information.

6.2. Trade, Antitrust and Fair Dealing

CIS Group is competing successfully in today's business environment with compliance to all applicable trade, antitrust, competition, and fair dealing laws. Therefore, employees must at all times adhere to the following rules:

- Commercial policy and prices will be set independently and will never be agreed, formally or informally, with competitors or other non-related parties, whether directly or indirectly.
- Customers, territories or product markets will never be allocated between CIS Group and its competitors but will always be the result of fair competition.
- Customers, Partners, and Suppliers will be dealt with fairly.

6.3. Fraud - Protection of Company Assets/Accounting

Employees must never engage in fraudulent or any other dishonest conduct involving the property or assets or the financial reporting and accounting of CIS Group or any third party. This may not only entail disciplinary sanctions but also result in criminal charges.

CIS Group financial records are the basis for managing the Company's business and fulfilling its obligations to various stakeholders. Therefore, any financial record must be accurate and in line with CIS Group accounting standards. Employees shall safeguard and make only proper and efficient use of CIS property.

All employees shall seek to protect CIS Group property from loss, damage, misuse, theft, fraud, embezzlement, and destruction. These obligations cover both tangible and intangible assets.

6.4. Anti-Bribery and Anti-Corruption

It is the policy of CIS Group to conduct all of its business in an honest and ethical manner.
At CIS Group neither the Group companies, nor any employee shall offer, pay, promise, authorize or receive any bribe, kickback or other illegal payment or benefit in violation of the national or international anti-corruption laws.
CIS Group aims to ensure that all employees possess the necessary competencies to handle corruption cases in accordance with the established guidelines. Staff need to be conscious of CIS Group values, rules and procedures, and able to supply a high level of service to companies in the form of advice and guidance on bribery and corruption, local conditions and specific legal issues.
Acceptance or use of corruption and bribery causes damage to CIS Group's reputation and a consequent decline in its economic fortunes, whereas a clean, non-corrupt reputation can be an economic advantage for the company.

6.5. Assignment of Personnel

Directors and managers are responsible for ensuring that the corruption risks are effectively managed at strategic and operational levels, and with competent and trained staff working within systems that incorporate effective anti-corruption controls, in addition to appropriate targets, and performance review for all risk areas.

6.6. Communication

CIS Group effectively communicates this Policy to all personnel, partners and third parties, and provides appropriate anti-corruption education and training to all employees.
The requirements of the anti-corruption policy, in accordance with ISO 9001 and ISO 27001 standards, are communicated to employees and managers during the ISO awareness sessions, employees' induction program, internal audits and management meetings.

6.7. Gifts, Meals and Entertainment

Receiving favors shall not influence employees nor shall they try to improperly influence others by providing favors. Gifts, hospitality and entertainment promised, offered or provided on behalf of CIS Group to a

customer or Government Official or any other Covered Party, must be reasonable, in accordance with customary courtesies, related to a legitimate business purpose and lawful under applicable laws.

No payment or promise of payment for gifts, hospitality, or entertainment to a customer,
Government Official or Covered Party may be made by or on behalf of CIS on the basis that it is permitted as provided above, unless such payment or promise has been approved in accordance with the procedures set forth by the Corporate Legal Department

6.8. Advertising and Marketing

CIS Group marketing and sales practices must reflect a commitment to honest and fair dealings with the Group's current and potential customers. CIS Group Partners must not engage in any misleading or deceptive practices.

If a CIS Group Partner is, with CIS Group's prior written approval, engaged in any advertising, marketing, or promotional activities that reference or implicate CIS Group, its name, logo, or services in any manner, the advertising, marketing, or promotional materials must comply with all laws, rules, and regulations, and must be truthful and accurate.

CIS Group Partners may not misrepresent products, services, and prices, or make unfair, misleading, inaccurate, or false claims about, or comparisons with, competitor offerings.

7. ETHICAL PERSONAL CONDUCT

7.1. Corporate Opportunities

Employees shall not compete with CIS Group. Nor shall they take personal advantage of business opportunities that they discover during the course of their employment, unless the Company expressly waives its interest in pursuing such opportunity.

If employees want to pursue business opportunities that might be of interest to the Company, they shall inform their Line Manager who will seek a management decision as to whether or not the Company wants to pursue the opportunity. Even if the Company decides against pursuing the opportunity, the employee may seize the opportunity on his or her own behalf only if it is clear that doing so will not result in direct or indirect competition with the Company's operations.

7.2. Proper Maintenance of Records

CIS Group's records are stored either electronically or as hard copies in appropriate locations to avoid damage and deterioration. Custodians of records have been identified by the management of CIS Group.

Electronic records are backed up on removable media at sensible intervals. Such removable media shall be safeguarded against fires and any other contingencies.

7.3. Business Communication and Public Disclosure

CIS Group maintains electronic information resources, which are essential to performing its business. Similar to any other capital resources owned by CIS Group,these resources are to be viewed as valuable assets over which CIS Group has both rights and obligations to manage, protect, secure, and control. CIS Group employees

and other affiliates are expected to utilize these resources for appropriate purposes, protect access to them, and control them appropriately.

8. COMPLIANCE WITH THE CODE

- Waivers

While some of the policies contained in this code must be strictly adhered to and no exceptions can be allowed, in other cases exceptions may be appropriate. Any employee is entitled to suggest an amendment to the Code of Business Conduct and Ethics, if he/she feels that the existing document does not reflect the current practice or status.

To that end, the person requesting amendment shall address a request to his/her direct supervisor with annotated or highlighted clause to be reviewed. If the supervisor agrees that the exception is appropriate, the approval of the HR & Legal departments must be obtained.

The HR and Legal departments will communicate any exceptions they approve to the HR Director who shall be responsible for maintaining a complete record of all requests for exceptions to any of these policies and the disposition of such requests.

Any executive or director who seeks an exception to any of these policies, should contact the HR and Legal departments. Any waiver of this code or any change to this code that applies to an executive or director, may be made only by the board of directors of the company and will be disclosed as required by law or regulation.

9. REPORTING ILLEGAL OR NON-COMPLIANT CONDUCT

9.1. Reporting

Obligation to Report

It is critical to CIS Group's success and reputation that all team members follow the Code. Each team member has a duty to report actual or suspected breaches of the Code. Employees shall report any practices or actions, believed to be inappropriate under this Code or even illegal, to their Line Managers or the appropriate members of the HR, Legal or Compliance function carried out by a compliance officer to insure that each company runs legally and ethically as per the regulations. Reports of violations may be made directly to higher levels including the HR & Legal Department. Where appropriate, complaints may be made on a confidential basis.

All complaints shall be properly investigated. CIS Group prohibits retaliation against any employee for such reports made in good faith, while it also protects the rights of the incriminated person.

9.2. Consequences of Not Reporting

Adherence to the Code is a condition of employment. Failure to report an actual or suspected breach of the Code by yourself or others is a serious matter and may result in disciplinary action of employee including reprimands or termination of employment or relationship with CIS Group.

9.3. Investigating

CIS Group may employ a variety of methods to conduct investigations for allegations of misconduct. Investigations will be commenced and conducted only by the Human Resources Director in an ethical manner and in compliance with applicable law and CIS Group policies. Investigation methods may include interviews with the parties and witnesses, review of relevant financial and other records, criminal and background checks, and monitoring and/or analysis of computers, systems, offices, social networks and other resources.

Employees have a duty to fully cooperate with investigations and to promptly, completely, and truthfully comply with all requests for information, interviews, or documents during the course of an investigation. CIS treats as confidential all reports of alleged misconduct and only those persons with a need to know are informed of and involved in an investigation.

9.4. Disciplinary Action

We promote consistency in the application of disciplinary action. Factors considered in determining appropriate disciplinary action may include violation of any law; whether the CIS Group Code of Ethics and Business Conduct or any other company policy.

At the end of an investigation, appropriate disciplinary action will be taken, or no disciplinary action may be necessary, based on the findings. In addition, CIS Group Management may report civil or criminal violations to the relevant authorities.

CIS Group will take disciplinary action against any individual violating the Code or Group Policies. Specifically, it will take disciplinary action against any employee or manager who is found to have:

- Authorized, overlooked, participated in, or concealed actions that are in violation of CIS Group's policies or business conduct standards.
- Disregarded or approved a violation.
- Through lack of diligence in supervision, failed to prevent or report violations.
- Retaliated, directly or indirectly, or encouraged others to retaliate, against an employee who reported a potential violation of CIS policies or business conduct standards.

10. ETHICS

Unsubstantiated allegations will have no effect on an employee accused of wrongdoing, and retaliation will not be tolerated against any employee who reports a concern in good faith or cooperates with a compliance investigation.

The CIS Group Code of Business Conduct and Ethics positions CIS Group in the forefront with those corporations throughout the world that emphasize the importance of honest business conduct and solid business ethics. We can meet these standards only with the cooperation of our employees, long recognized as CIS Group's most valuable asset. To do the right thing and to ensure the highest standards of integrity is each employee's personal responsibility that cannot be delegated.

When in doubt, employees should always be guided by the basic principles stated in this Code. Any failure to comply with this Code may result in disciplinary action, including the possibility of dismissal and, if warranted, legal proceedings or criminal sanctions.

11. CERTIFICATES

CIS Group is dedicated to maintaining the highest standards of quality and information security, as evidenced by our ISO 9001:2015 and ISO 27001 certifications.

- **ISO 9001:2015** certifies our Quality Management System (QMS), a reflection of our dedication to continuously improving and refining the way we operate. This certification ensures that we maintain a structured approach to all aspects of our work—from planning and leadership to resource management and product realization. It's a promise that we will always meet customer expectations, adhere to regulatory requirements, and uphold the highest industry standards. By empowering our team with the right training and clearly defined leadership roles, we create a culture where quality and operational excellence thrive. Through consistent monitoring and audits, we keep pushing ourselves to improve, ensuring that every product and service we deliver exceeds expectations.
- With **ISO 27001**, we embrace a global standard for information security that helps us protect sensitive data through a thoughtful, risk-based approach. This certification guides our Information Security Management System (ISMS), which ensures the confidentiality, integrity, and availability of data, and requires us to regularly assess risks, implement security controls, and continuously improve our practices. It is more than a set of standards, it's a promise to protect what matters most. By reinforcing our ability to defend against threats like cyberattacks and comply with global data protection regulations, we safeguard critical information, fostering trust with our customers and partners.

Together, these certifications validate our commitment to quality and security, positioning CIS Group as a reliable and trustworthy partner. By maintaining these rigorous standards, we offer clients peace of mind, ensuring the integrity of their data and fostering long-term, trusted relationships in an increasingly data-driven world.

12. USEFUL NUMBERS & ADDRESSES

- Human Resources Department:

+961 4 410410 Ext: 10222- 10266

- Legal Department:

+961 4 410410 Ext: 10206

- CIS Group

Location: Jal-el-Dib Square, CIS Building, Beirut, Lebanon
Tel: +961 4 410 410
Fax: +961 4 525 181
Email: info@cis.com.lb
Website: www.groupcis.com
P.O. Box: 11-6274, 11072210 Riad el Solh, Beirut, Lebanon

- Scan the QR code to add CIS to your contacts

ANNEX A

EMPLOYEES ACKNOWLEDGEMENT FORM

I have read and am familiar with CIS Group Code of Business Conduct & Ethics.

I understand my responsibility to promptly report any incident of misconduct or perceived misconduct that I may experience or witness.

I further understand that CIS Group and all partners companies take zero tolerance approach to violations of this Code, and that violations of the Code or retaliation against whistle-blowers will result in termination of employment.

By signing this acknowledgement, I am indicating that I have read and will abide by CIS Group's Code of Business Conduct & Ethics.

Employee Name:

Position:

Date:

Employee Signature:

This signed and completed form must be returned to your Human Resources representative within 5 calendar days of receiving this booklet.

ANNEX B

SUPPLIERS ACKNOWLEDGEMENT FORM

I have read and am familiar with the Supplier Code of Business Conduct.

I understand my responsibility to promptly report any incident of misconduct or perceived misconduct that I may experience or witness.

I further understand that CIS Group and all partners companies take zero tolerance approach to violations of this Code, and that violations of the Code or retaliation against whistle-blowers will result in termination of employment.

By signing this acknowledgement, I am indicating that I have read and will abide the Code of Business Conduct of all the suppliers of the group.

Employee Name:

Position:

Date:

Employee Signature:

This signed and completed form must be returned to the Human Resources representative within 5 calendar days.

ANNEX C

CIS PROCEDURES TO FOLLOW ON-BOARDING RESELLERS AND END-USERS:

1. Customer Identification and Data Collection

Prior to engagement, the customer or company is identified through the CIS database, with essential information collected, including the full legal name (individual or business), registered business or personal address, contact details (phone, email), government-issued identification or business registration documents, tax identification number (TIN/VAT), and business activities and source of funds (for corporate entities).

After that, the customer's business sector is verified to ensure alignment with CIS target markets: banking, telecommunications, healthcare, education, and extended manufacturing.

2. Internal Screening

Following the initial customer identification and data collection process, the customer's eligibility is now tested internally through World Check, a comprehensive database that provides restricted party screening. This screening solution exclusively researches and covers the following areas of Risk:

- Global Sanctions, Law Enforcement, and Regulatory Enforcement lists.
- It identifies Politically Exposed Persons (PEPs), their Sub-categories, Associates, and Relatives.
- It screens Individuals and businesses connected to Financial Crimes, Fraud, Money Laundering, Terrorism Financing, Specially Designated Nationals, and to other high-risk categories such as Shell Banks, Arms Trafficking, Narcotics Trafficking, Organized Crime, and Corporate Crime.

Media checks and ongoing monitoring are also performed to maintain compliance with international regulatory standards.

3. External Investigation and KYC Validation

For unknown customers, an external agency conducts an investigation. Identity and address verification are performed by cross-referencing government databases, utility bills, or business registration documents. Corporate customers undergo ownership structure validation, including confirmation of ultimate beneficial owners (UBOs).

4. OEM Due Diligence

A compulsory review by the OEM includes KYC verification. High-risk customers require additional documentation (e.g., financial statements, proof of operations) and a deep-dive investigation using Reuters reports and open-source intelligence, subject to senior management approval. The OEM is formally informed of concluded sales with the customer.

5. Credit Insurance evaluation: Financial Risks Classification and Solvency

A credit-insurance provider evaluates the customer's financial stability, classifying risk as follows:

- Low Risk: Fully covered by insurance; eligible for full credit terms.
- Medium Risk: Partial coverage; credit terms require internal approval.

- High Risk: No coverage; transactions require prepayment or guarantees.

CIS proceeds with the relationship only when the customer is classified as Low or Medium Risk.

As for the financial solvency verification, financial statements (balance sheets, income statements, cash flow) and payment history are reviewed to assess creditworthiness, particularly if collateral support is required.

6. Enhanced Due Diligence (EDD)

High-risk customers undergo EDD, including additional documentation requests, in-depth investigations, senior management approval, and continuous monitoring with frequent re-screening.

7. Ongoing Monitoring

Periodic re-screening via Reuters ensures compliance. Suspicious transactions or behavioral shifts trigger reviews, and customers reclassified as high-risk are subject to EDD.

8. Compliance and Reporting

Suspicious activities are escalated to management. Records are retained for a period of ten years per regulatory standards (Refer to CIS-GDPR-01-Records Retention & Disposal Schedule.REV02). The compliance team ensures KYC/AML processes adhere to evolving trade laws and global screening standards.

ANNEX D

INTERNATIONAL TRADE COMPLIANCE

1 PURPOSE

This Annex defines the procedures to ensure compliance with all applicable legal, regulatory, and internal requirements in the execution of projects, trades, and other business transactions. It establishes clear responsibilities for adhering to export control and economic sanctions laws of the United States, the European Union, and other relevant jurisdictions (collectively, "Applicable Trade Laws"). The objective is to minimize legal, financial, and reputational risks through a structured and thorough due diligence process.

2 SCOPE

This annex applies to all employees, subsidiaries, agents, distributors, and third parties. It covers all international trade transactions, including imports, exports, re-exports, technology transfers, and business dealings in sanctioned regions.

3 TRADE COMPLIANCE

3.1 Understand Regulatory Frameworks

Research Laws: Ensure compliance with international trade laws, including:

- U.S. Export Administration Regulations (EAR)
- International Traffic in Arms Regulations (ITAR)
- EU Dual-Use Regulations

3.2 Trade Compliance Screening Checklist

For entity & individual verification purposes, CIS obtains the customer's following documentation:

- Business Registration Certificate
- Tax Identification Number (TIN) or VAT Registration
- Articles of Incorporation or Business License
- Government-Issued ID (for Individuals)

3.3 Trade Compliance Screening

CIS conducts thorough trade compliance screenings using databases such as World-Check, enabling us to avoid engaging with risky or sanctioned parties. CIS also performs the following screenings:

- Restricted /Denied Party List Check (OFAC, BIS, UN, EU, etc.)
- Sanctions List Check (U.S., EU, UK, UN, etc.)
- Watchlist Screening (Fraud, PEP, AML checks)

3.4 KYC/ KYS Documentation

3.4.1 KYC Documentation

- Company Profile or Website Information
- Ownership Structure & Beneficial Owners

- Customer/Supplier Due Diligence Form
- End-Use & End-User Certificate (if applicable)

3.4.2 Internal Compliance Documentation

- Screening Records & Logs
- Risk Assessment Report

3.5 Product Classification

- **HS Codes:** Classify all products using Harmonized System (HS) codes for accurate tariff calculation and customs procedures.
- **ECCN:** Determine Export Control Classification Numbers (ECCN) for items subject to U.S. export controls and identify any licensing requirements.

3.6 Licensing And Permits

- **Apply for Licenses:** Ensure all necessary export licenses (e.g., BIS for dual-use items, DDTC for defense articles) are obtained before shipping controlled goods.
- **Automate License Checks:** Use software to flag items requiring licenses based on product classification.
- **Request Consignee Forms** (confirmation that the goods will not be shipped to an Unnamed Party, Sanctioned Organization, or Embargoed or Sanctioned Country). The signed Consignee Form must be submitted before any release of goods. Consignee Forms must be renewed annually.

3.7 Leverage Technology

- **Compliance Software:** Utilize tools like E2open or Oracle Global Trade Management to automate:
  - Screening
  - Product classification
  - Licensing checks
- **ERP Integration:** Embed compliance checks into procurement and order fulfillment workflows to streamline processes.

3.8 Engage Experts

- **Customs Brokers:** Work with certified customs brokers to:

  Navigate complex customs procedures
- **Legal Counsel:** Consult with trade attorneys to:
  - Address ambiguous regulations
  - Assist with dispute resolution.

3.9 Accurate Documentation

- Maintain Records: Ensure commercial invoices, packing lists, and certificates of origin are precise and retained for audits. CIS may retain documents for up to 10 years, depending on their type (Refer to **CIS-GDPR-01-Records Retention & Disposal Schedule.REV02**).
- Automated Record-Keeping: Implement ERP systems (e.g., SAP GTS) to generate and store compliance documents automatically, ensuring easy access during audits. In case of customers handling their shipments, our forwarder is issuing the customs export declaration.
- Transportation document is mandatory to be provided by the customer or his forwarder.
- We receive written commitment from the customer forwarder on above before delivery is released.

- Both documents will be kept in our records as a proof that goods were shipped to the correct destination and reseller.

3.10 Audit And Risk Management

Yearly audit to review compliance processes and rectify gaps. Prioritize high risk areas and implement mitigation strategies when necessary.

3.11 Inspection

Supply chain handles inspection of goods for specific countries (i.e. Gabon, DRC, Uganda, Tanzania, Kenya, etc...). Quality and quantity check is done by certified companies SGS or Veritas before shipment.

3.12 Open Cover Insurance

All shipments are insured against all risks, from warehouse to warehouse, to ensure safe delivery to their final destination.

4 ORDER PROCESSING

- Check whether customer country is Embargoed or Sanctioned.
- Check whether end customer country is Embargoed or Sanctioned.
- Ensure that customer PO is adequality detailed (letterhead, customer particulars, bill of materials, pricing, currency, Incoterms, payment terms).
- For back-to-back deals, check that there is an end customer purchase order or contract prior to ordering.
- Bill of materials checked for Restricted Technologies; if included, check status of required Export License with Supply Chain Management team.

5 RESPONSIBILITIES

The key responsibilities fall on the following:

5.1 Compliance Department / Officer

- Develops and updates compliance training programs based on regulatory requirements.
- Ensures the training materials align with legal and industry standards.
- Monitors and enforces compliance policies across the organization.

5.2 Human Resources (HR)

- Integrates compliance training into onboarding for new employees.
- Tracks and records employees' participation and completion of training.
- Addresses any employee concerns regarding compliance training.

5.3 Legal Department

- Reviews training content to ensure legal accuracy.
- Advise on regulatory risks and required compliance measures.
- Ensures that compliance training meets legal and contractual obligations.

5.4 Department Heads & Managers

- Ensure their teams complete the required training.
- Reinforce compliance principles in day-to-day operations.
- Identify and report any compliance issues within their departments.

5.5 Employees

- Complete assigned compliance training on time.
- Follow the company's compliance policies and guidelines.
- Report any compliance violations or concerns.

6 TRAINING

Regarding Training and Awareness, this annex is to ensure that a high standard of compliance is maintained through mandatory training and awareness programs of employees as well as subcontractors and partners involved in projects, trades, or transactions. The training frequencies are as follows:

- Initial Training: All new employees, subcontractors, and partners involved in projects, trades, or transactions must complete compliance training as part of their onboarding process. This includes training in trade compliance, regulatory requirements, ethical practices, and due diligence procedures.
- Bi-Annual Training: All employees, subcontractors, and partners must complete mandatory refresher training every two years to ensure continuous awareness of evolving regulations, industry standards, and internal policies.

7 REPORTING VIOLATIONS

Any suspected violations must be reported immediately to the Legal & Human Resources departments or via the company's whistleblower mechanism.

Retaliation against employees reporting violations in good faith is strictly prohibited.

8 ENFORCEMENT & CONSEQUENCES

Violations of this annex may result in disciplinary action, including termination of employment or legal consequences.

Non-compliance may lead to regulatory fines, penalties, or restrictions on business operations.

9 REGULATORY UPDATES:

Monitor Regulatory changes through subscription like Thompson Reuters for real time regulatory alerts.

Whenever there are significant updates to relevant laws, regulations, or company compliance policies, additional ad-hoc training sessions will be conducted to address these changes. Employees, subcontractors, and partners will be required to attend these sessions within 30 days of notification.

ANNEX E

CIS INTEGRATION BUSINESS

1. COMPUTER INFORMATION SYSTEMS INTERNATIONAL OFFSHORE SAL (CIS INT'L)
2. COMPUTER INFORMATION SYSTEMS - CIS LEBANON SAL.
3. CIS INTEGRATION INTERNATIONAL GBL (MAURITIUS)
4. COMMUNICATION INGÉNIÉRIE SYSTÈMES - CIS BÉNIN SA
5. COMPUTER INFORMATIQUE SYSTÈME – CIS BURKINA FASO SARL
6. SOCIÉTÉ CAP INFORMATIQUE (CAP INFO) LIMITED
7. COMMUNICATION INGÉNIÉRIE SYSTÈMES CAMEROUN- CIS CAMEROUN SA
8. COMMUNICATION INGÉNIÉRIE SYSTÈMES CONGO - CIS CONGO SARL
9. COMMUNICATION INGÉNIÉRIE SYSTÈMES CÔTE D´IVOIRE - CIS CI SA
10. COMMUNICATION INGÉNIÉRIE SYSTÈME GABON - CIS GABON SA
11. CEDAR INFORMATION SYSTEMS GHANA LIMITED
12. COMPUTER INFORMATION SYSTEMS - CIS GUINÉE SA
13. COMPUTER INFORMATION SYSTEMS KENYA - CIS KENYA LIMITED
14. COMPUTER INFORMATION SYSTEMS MALI - CIS MALI SA
15. COMPUTER INFORMATION SYSTEMS AFRICA NIGER - CIS AFRICA NIGER SA
16. COMPUTER INFORMATION SYSTEMS NIGERIA - CIS NIGERIA LIMITED
17. COMMUNICATION INGÉNIERIE SYSTÈMES RDC - CIS RD CONGO SA
18. COMMUNICATION INGÉNIERIE ET SYSTÈMES - CIS REUNION SARL
19. COMPUTER INFORMATION SYSTEMS SÉNÉGAL - CIS SENEGAL LTD
20. COMPUTER INFORMATION SYSTEMS TANZANIA - CIS TANZANIA LTD
21. COMPUTER INFORMATION SYSTEMS UGANDA - CIS UGANDA LTD
22. COMPUTER INFORMATION SYSTEMS - CIS RWANDA LIMITED
23. SYSTEM MAINTENANCE SOLUTION ANGOLA - SMS ANGOLA LIMITADA
24. COMPUTER INFORMATION SYSTEMS AFRICA – CIS AFRICA SA
25. SOLUTION MICRO SYSTEM - SMS FRANCE SA
26. REALISATION TELEMATIQUE ET INFORMATIQUE – RTI ALGERIE SPA
27. (ALQARIYA) LEKHADAMAT ALHASEBAT W ANTHMA AL MAALUMAT - LTD
28. (CONTINENTAL) COMPANY FOR PROVIDING INFOMARTION, TELECOMS AND COMPUTING SERVICES - LTD

HIPERDIST DISTRIBUTION BUSINESS

1. INTERNATIONAL DISTRIBUTION (INTERDIST) OFFSHORE SAL
2. DISTRICOM OFFSHORE SAL
3. HIPERDIST LIMITED(UK)
4. A. HYPERDIST SPA (ALGERIA)
5. HIGH PERFORMANCE DISTRIBUTION AFRICA LIMITED (IC)
6. HIPERDIST ALLIANCES JORDAN LIMITED
7. HIPERDIST ALLIANCES - TUNIS LIMITED
8. HIPERDIST LIMITED - KENYA
9. HIGH PERFORMANCE DISTRIBUTORS GHANA LIMITED
10. HIPERDIST ALLIANCES - MAROC LIMITED
11. HIGH PERFORMANCE DISTRIBUTION - SENEGAL
12. HIPERDIST LEBANON SAL
13. HIGH PERFORMANCE DISTRIBUTION NIGERIA LIMITED
14. HIPERDIST INFORMATION TECHNOLOGY NAMIBIA (Proprietary) LIMITED
15. LEVANT DISTRIBUTION FZO
16. HIGH PERFORMANCE DISTRIBUTION (NIGERIA) LIMITED
17. HIGH PERFORMANCE DISTRIBUTORS (REUNION)SARL
18. HIPERDIST INFORMATION TECHNOLOGY TRADING LLC DUBAI
19. INTERDIST ALLIANCES LTD - NIGERIA
20. HIPERDIST ALLIANCES LDA – MOZAMBIQUE
21. HIPERDIST ALLIANCES PROPRIETARY LIMITED - BOTSWANA
22. INTERDIST ALLIANCES LTD- ZAMBIA
23. IT4 ANGOLA – LIMITADA
24. IT4 TANZANIA LIMITED
25. IT FOR AFRICA KENYA LIMITED
26. HIPERDIST (PTY) LTD SOUTH - AFRICA
27. HIPERDIST COMPANY LIMITED (TANZANIA)
28. SCRIPETRA LIMITED (NIGERIA)
29. SUPERDIST LIMITED (MAURITIUS)
30. UNIVERSAL DISTRIBUTORS UNIDIST HOLDING SAL
31. UNIVERSAL DISTRIBUTORS UNIDIST HOLDING OFFSHORE SAL
32. INTERDIST GLOBAL TRADING – UAE

CIS PROFESSIONAL SERVICES BUSINESS

1. PROCOMIX TECHNOLOGY GROUP SAL - LEBANON
2. PROCOMIX TECHNOLOGY GROUP SAL HOLDING - LEBANON
3. PROCOMIX TECHNOLOGY GROUP SAL OFFSHORE - LEBANON
4. PROCOMIX TECHNOLOGY GROUP LTD - KSA