Logicom

Ethics and Compliance Manual

September 2019

Contents

Message from the Chairman of the Board of Directors

Dear Logicom Employees,

In today's fast moving and continuously evolving multifaceted business environment, compliance has gained a pivotal role in the management of modern organizations. The fast developments in laws and regulations that affect our operations as well as increased scrutiny by the relevant authorities demand our focus on compliance.

At Logicom, we adopt and promote very high standards of business and professional conduct. Our company is based on open communication, integrity, compliance with legislation and policies, principles of corporate governance, trust in our people and respect to our customers, partners and the society. As a result, our customers, partners and stakeholders around the world continue to trust our solutions and professional services.

This Logicom Ethics and Compliance Manual highlights our strong commitment to compliance with our policies, laws, and regulations as well as our ethical approach to business. Along with our Code of Business Conduct, it is to be used as a tool to help us all in taking the right decisions.

We are all responsible for protecting and improving Logicom's reputation for integrity, compliance with legislation and professional ethics. Every decision we take, affects our efforts to make valuable contributions to our customers and partners.

Thank you for your commitment to the Compliance and Ethical business practices underlined in this Ethics and Compliance Manual.

Takis Klerides

Chairman, Board of Directors

Message from the Managing Director

Dear Logicom Employees,

Logicom is committed on doing business in an ethical, legal and compliant manner and aims for these principles to be at the center of its core priorities and values. Adhering to applicable laws and regulations, abiding to our internal policies and making decisions in an ethical manner is of paramount importance for the long-term success of the company.

The Logicom Ethics and Compliance Manual includes summaries of our key policies and associate links to the full policies, key compliance areas, and ethical guidelines. It should be therefore used as the guiding document, along with our Code of Business Conduct, to help us make the right decisions but also guide us though key compliance areas that we need to ensure we adhere to on a continuous basis.

Our Ethics and Compliance Manual also solidifies the right but also responsibility of employees to report any wrong-doing they observe though multiple channels, with a commitment to no-retaliation for such proper reporting. Earning Trust is a fundamental principle achieved by following the principles of the Ethics and Compliance Manual.

We count on every employee to make sure that the right decisions are taken based on our values, and in an ethical, compliant and legal manner at all times.

Varnavas Irinarchos

Managing Director

1. Introduction to Ethics and Compliance: A complex new world

In a fast moving and continuously evolving business and regulatory environment, compliance has gained a pivotal role in the management of modern organisations around the globe. International players face increasing difficulties in keeping up with changes in regulations that directly or indirectly affect their business operations. Laws and regulations are becoming more complex, harder to understand and contradicting in some cases.

Authorities from different areas of the globe are raising expectations with regards to compliance requirements which many times cross territorial boundaries and apply to individuals and/or entities in other geographical locations with direct and significant impact on their business activities and carry financial and in some cases criminal penalties for non-compliance. Such regulations include but are not limited to: Export compliance regulations, Anti-trust and competition laws, Anti-Bribery and Corruption laws and Data Privacy laws. The compliance stakes are becoming increasingly relevant in decision making as potential penalties arising are exponentially growing and include monetary penalties, being listed in "black lists" and therefore being unable to work with specific countries or currencies and in some cases criminal actions against individuals involved.

If you think compliance is expensive, try non-compliance.

Global regulators emphasize the importance of establishing effective compliance programs which are directly linked with risks faced by their local presence and swift adapting to changes thereafter. Designing, building and maintaining a cross border, multi-jurisdictional compliance program has become a huge challenge that international businesses are called to address. And the challenge is not focused on merely building armies of compliance "policemen" to audit and follow every single transaction entered into but rather focusing on evolving the business culture. Embodying a culture of compliance in an organisation is a gradual and many times painstaking process that involves surgical changes in human resources management, systems and processes.

It is not only for what we do that we are held responsible but also for what we do not do.

Moliere

It is therefore critically important that we, in Logicom Group ("Logicom"), focus on our compliance culture and build on our training and development, evolving our processes and continuously strengthen our compliance efforts to address the complexities of this new world. Export regulations, data privacy and protection, inclusion and diversity are examples of key areas addressed by the Manual.

Moreover, the global community's focus on ethical business practices has grown exponentially in the last years with the adoption of much stricter approach in transactions with emphasis in bribery suppression, corporate social responsibility and human rights.

In this manual, we are summarizing important policies that Logicom employees have to comply with and provide links to the relevant full policy statements where appropriate. This Policy should be used as a mind map for all Logicom employees in understanding their obligations under their employment contracts.

2. Speaking Up

We are a live and fast-growing organisation. It is our strong belief that our staff feel comfortable to speak up openly with management about any concern. You can freely report any matter for which you have an ethical, legal or integrity related concern. The report will be treated in a fair manner and timely, and actions may be taken based on this report.

Whistleblowing

Logicom is committed to the highest standards of openness, probity and accountability. For this reason, a formal Disclosure (Whistleblowing) Policy has been established to ensure that employees are able to speak up without fear of retaliation. Logicom is committed to this policy and to all related applicable laws and regulations including Data Protection Laws. All disclosures will be treated in confidence, consistently, fairly and in a professional manner.

It should be emphasized, that this policy is intended to assist individuals who believe they have genuinely discovered malpractices, impropriety or a breach of Company policy or a legislation or regulation governing the Logicom's operations. Whistleblowing is neither a means to question financial nor business decisions taken by the Company nor should it be used to reconsider any matters that have already been addressed under harassment, grievance, disciplinary or other HR procedures.

It is expected that staff will use this policy to avoid the necessity to air their complaints publicly, inside or outside the Company but to report their concerns directly in good faith and on the basis of reasonable belief so action can be taken.

"Whistleblowing" is a term used when an individual – the "Whistleblower" discloses information concerning an alleged wrongdoing including reasonable suspicions of a wrongdoing. This may be something they have witnessed at work or while doing business with or on behalf of Logicom.

Non-retaliation

Victimization of or retaliation against a whistleblower is wholly unacceptable provided they have disclosed their concerns:

- In good faith, and;
- In the reasonable belief that malpractice or impropriety has actually occurred.

A whistleblower making a disclosure under these conditions, whether founded or not, is protected. However, if the disclosure is proven to be malicious or a purposely false allegation, the Company may take disciplinary action.

Reporting wrongdoings

The Company respects anonymous reporting and will treat all disclosures in a confidential and sensitive manner. Disclosed information must be very specific for the case to be investigated. The identity of the whistleblower may be kept confidential so long as it does not hinder or frustrate any investigation. However, the investigation process may reveal the source of the disclosure and the identification of the whistleblower who may therefore be asked to provide a statement.

Staff raising concerns retain the right to remain anonymous provided always that (i) the Company will not be in breach of any applicable law, rule or regulation by maintaining the anonymity and (ii) the issue raised does not concern a criminal offence.

If an employee sees, has reasonable suspicion of any wrongdoing or receives a complaint of malpractice, the employee must pass this information as soon as is reasonably possible, to the designated Disclosure Reporting Officer as defined in the Disclosure (Whistleblowing) policy.

It is expected that all stakeholders duly report such wrong doings. You have an ethical and business obligation to report wrong doings and not to cover such behavior, which can damage the company's reputation and business. Failure to report a suspected wrongdoing may lead to disciplinary actions.

Alternative reporting channels are the Group Human Resources Manager, Group Compliance Officer, and/or the Head of Group Internal Audit .

The contact may be made in person, in writing, by telephone, email or through the group website.

Logicom Employees can find our Disclosure (Whistleblowing) policy here

3. Your Private Time

While on Your Private Time

Logicom expects that during your private time, you will act in a responsible manner. Our behaviour outside working hours may reflect on Logicom. In this respect we all need to be cautious, follow common logic, and act in a responsible manner similar to how you would act if you would be representing Logicom. Our behaviour outside Logicom should include our presence in social media, even for personal purposes, our behaviour when socializing, and generally our behaviour in our everyday life. We should therefore be continuously cautious in presenting a proper image. While you maintain your personal freedom for your actions, you need to always consider the impact of your personal actions to the reputation of the company.

Personal Use of Logicom's time

During our work time at Logicom, we are not allowed to do personal activities whether this represents a conflict of interest or not. Moreover, we cannot solicit business for personal purposes during Logicom time and must not perform any other business. We operate in a complex and fast-moving business environment and our focus should be on the performance of our obligations during business working hours.

Social networking

Social networking includes profile pages and other resources maintained by employees on networking sites including, but not limited to, Facebook, Twitter and LinkedIn, as well as blogs, forums, message boards, review sites and online polls ("Social Media Tools") used for personal or professional reasons.

It is important that employees using social networking sites in the workplace use it in a way which does not affect Logicom's reputation.

Social Media Tools usage for work purposes is controlled by the Group IT Department and usage for personal reasons does not need approval by the Company, however, when using these tools, either in a personal or work capacity, during times allowed by Logicom or outside working hours, posts must not:

- compromise the Company, disclose confidential data or disclose sensitive data
- damage the Company's reputation or brand
- breach copyright or the Data Protection Laws or the Data Privacy Policy
- contain libel or defamatory content
- must not engage in bullying or harassment

- be of illegal, sexual or offensive content
- interfere with your work commitments
- use/ disclose the name of the Company in any way to promote products or express political opinions and views

It is also recommended that all employees use strict privacy settings on their social network profiles.

Social media or blog content attributable to you which breaches the terms of this Policy, or the other related policies, may result in an investigation and disciplinary action in accordance with the Company's Disciplinary and Grievance Policies and Procedures.

Upon leaving the organization, employees must update all their professional and personal social media accounts to reflect their updated status and rescind access to any company social media tools they may have had access to.

Logicom staff can find the Disciplinary and Grievance Policies and Procedures here

Political considerations

When exercising our political rights in our personal time we need to take special care to ensure that our individual views are not presented or perceived as Logicom views. No employee may hold any political party office position such as member of a political party committee. Any and all political actions are expected to be performed solely in your private time and should never interfere with your employment performance.

4. Building Trust with each other

Building Trust

Trust plays a crucial role in successful business relations. Trust is a fundamental pre-requisite for ethics and compliance. It is earned every day and not considered as granted. We therefore need to follow the principles listed below in building Trust with each other to win the trust vital for building strong professional relations.

Managing Conflicts of Interest

Conflicts can exist in various situations, for example when a Logicom employee participates in a competing, complementary or otherwise associated business therefore attaching natural bias to his/her decisions when wearing the Logicom hat. It is therefore important for Logicom employees to completely refrain from being involved in any business outside their normal Logicom employment duties.

Conflicts may be managed by:

- always working for the best interest of Logicom
- avoiding situations where a personal relationship or financial interest in another company might influence how we make decisions in our jobs.
- understanding that a conflict of interest can exist even if we feel comfortable that our decisions will not be affected by an outside relationship.
- promptly disclosing any conflict of interest and acting to immediately resolve it.
- before entering into any kind of external work/business arrangement, we ensure that such work does not affect Logicom's business interests or violate any employee terms we have signed and it is in accordance with the Conflict of Interest Disclosure Form which is signed by all employees.
- Report any potential conflicts to the HR Manager immediately.

Inclusion and Diversity

Logicom commits to encourage equality and diversity in the workplace and strives to create a working environment free of bullying, harassment, victimization and unlawful discrimination, promoting dignity and respect for all, and where individual differences and the contributions of all staff are recognized and valued.

As part of this commitment, Logicom is devoted to educating all employees about their rights and responsibilities for inclusion and diversity under the Equality and Diversity Policy.

Logicom commits to thoroughly investigate any allegations of bullying, harassment, victimization and unlawful discrimination by fellow employees (including managers), customers, suppliers, visitors, the public and any others in the course of the organization's

work activities with regards to discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age.

Allegations regarding such acts will be dealt with very seriously and may result in findings of misconduct under the organization's Grievance and Disciplinary Policies and Procedures, resulting in appropriate action. Findings of particularly serious breaches of the corporation's Equality and Diversity Policy may be considered as gross misconduct and may lead to summary dismissal.

Further, sexual harassment may amount to both an employment rights matter and a criminal offence, such as in the case of sexual assault.

Opportunities for training, development and progress are made available to all staff, who will be helped and encouraged to develop their full potential.

Management commits to review and update employment practices, procedures and the policy when necessary to ensure fairness and to consider changes in the respective laws and regulations but also monitor the composition of the workforce in relation to demographics such as age, gender and disability in order to encourage equality and diversity in the workplace.

Monitoring will also include assessing how effective the equality policy and any supporting action plan are, reviewing them as necessary and taking any action to address the relating issues.

Logicom employees can find the Equality and Diversity policy here and our Anti-Harassment Policy here

The role of the Leader

Leadership is an important function of management that helps us maximize efficiency and achieve organizational goals. The attributes of the leader may be summarized but not limited to the following:

1. Starts the work by communicating policies and plans to subordinates.
2. Plays an incentive role in the concern's working. He/she motivates the employees with economic and non-economic rewards and thereby gets the work from the subordinates.
3. Supervises and guides the subordinates. Guidance here means instructing subordinates the way they have to perform their work effectively and efficiently.
4. Creating confidence through expressing the work efforts to subordinates, clearly defining their role and giving them guidelines to achieve their assigned goals effectively. It is also important to listen to employees' opinion, with regards to their complaints and problems.

5. Building morale of employees towards their work execution and getting them into confidence and winning their trust. A leader can be a morale booster by achieving full co-operation so that they perform to the best of their abilities as they work towards achieving their goals.
6. Builds work environment in getting things done from people. An efficient work environment helps in sound and stable growth. Therefore proper, human relations should be kept into mind by a leader. He/she should have personal contacts with employees and should listen to their problems and solve them. He/she should treat employees humanly.
7. Achieves coordination through reconciling personal interests with organizational goals. This synchronization can be achieved through proper and effective co-ordination which should be primary motive of a leader.

In Logicom we aim to build our leadership culture at all levels and within every team to promote effective management of our resources and achievement of our goals.

Obtaining Approvals and Making commitments

Before taking any commitment or an action that will bind the company or its assets, whether that is a supplier agreement, a customer agreement, special pricing or anything else, the appropriate level of approval much be secured depending on the case.

Modifications of contract terms, purchase orders, invoicing terms, and commitments for employment of staff, etc. need the appropriate level of management approval to be in place as per company practice. You cannot make a commitment on behalf of the company without previously obtaining the appropriate level of approval.

Any authorised commitments need to be reported to the appropriate function for tracking and to ensure that our financial statement reflects these commitments and the right level of approval is obtained as described in the respective procedures.

Any unauthorized commitments may lead to disciplinary action including dismissal. The company reserves the right also require financial compensation for the damages caused by that unauthorized commitment.

Logicom employees can find our Group Policies and Procedures Manual here

Our people's health and safety

Logicom is very sensitive in the health, safety and welfare of its employees and customers. As such, Logicom aims to minimise the risk of accidents and takes appropriate actions to protect and sustain the health of all personnel.

The majority of our health and safety regulations initiatives and activities revolve around workplace practices and behaviour and the proper use of machinery, tools and equipment.

Teams of managers, employees, health and safety specialists and other interested parties work together to establish best practice, share experiences and expertise and find ways of promoting health and safety matters throughout all levels of the company.

Our employees are our most valuable assets, and we will continue to do everything in our power to protect their health and safety.

Logicom global operations is committed to respect all elements and follow all principles stated within this Policy.

The training of the employees is adapted to the evolution of risks and updated in case new risks may occur due to the technological evolution, to environmental situations, etc. and, therefore, such training is repeated periodically. The employees are prevented from using dangerous equipment or material and there are provided specific instructions and training for the use of any non-regularly used equipment.

The employees are required to report any health and safety risk they identify in writing to their health and safety officer and/or their General Manager.

Logicom is extremely careful and takes all necessary action in order to prevent accidents from the use of equipment and provides all necessary protective equipment to its employees when applicable.

More particularly, Logicom takes all appropriate measures so as:

- Employees do not eat or drink in activity areas where there is any possibility of risk. Smoking is only permitted in designated areas outside the buildings.
- Employees, depending on the situation and the activities, are provided and obliged by the company to use appropriate protective or other special equipment. The company provides separate spaces to store the regular clothing separately from special equipment.
- Employees are provided with appropriate hygiene spaces.
- The protective equipment, is properly placed in specific locations, checked prior to any use and replaced or repaired when damaged.
- Logicom maintains the equipment so that the health and safety of employees is not in danger.
- Employees are updated regarding possible risks in relation to their activities.

Logicom employees can find our Health and Safety Policies (located in our Code of Conduct) here

Email and Internet use

Internet communication plays an essential role in the conduct of Logicom's business. Communication tools must be used sensibly, professionally, lawfully and to the extent necessary for us to perform our duties in accordance with this policy and other rules and procedures.

Every employee is given access to the intranet and/or internet as appropriate to their duties and responsibilities. All PC/network access is done through passwords, and employees are not permitted to share their password with anyone inside or outside the company. Individuals will be allowed to set their own passwords and must change them at the latest on a 60-day frequency following the instructions of Group IT and as per the Group IT policy.

Employees have a duty to use the Internet responsibly. Only websites directly related to work purposes for the execution of work are permitted to be accessed. Employees should not at any time access or seek to access websites which promote any of the following:

- sexually explicit materials.
- violence.
- discrimination based on race, sex, religion, nationality, disability, sexual orientation, or age.
- illegal activities or violation of intellectual property rights.
- access to streamed or real-time audio, data, graphics, video or any other data that uses a large amount of bandwidth or system resources is not allowed either during work time or break or rest periods unless access to such services is directly related to your work. This includes accessing entertainment services such as, "reality TV" shows and sports events.

Corporate emails are powerful tools that help employees in their jobs and are strictly a company asset. Employees should use their company email solely for work-related purposes. Employees are not allowed to use their company email for personal purposes. Employees are not allowed to export company data outside the company. Non-compliance may lead to disciplinary action.

Employees who don't adhere to the present policy will face disciplinary action up to and including termination. Example reasons for termination are:

- Using a corporate email address to send confidential data to anyone without authorization.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.
- Using a corporate email for an illegal activity

Logicom (through its Internal Audit, Compliance function, and/or other authorized personnel), as per the Data Privacy Policy, may access the business email accounts of any employee for the following reasons:

- to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy (and employees acknowledge that the Company can use software to monitor the identity of senders and receivers of emails);
- to assist in the investigation of possible wrongful acts; or
- to comply with any legal obligation.
- for execution of work
- for any operational reason for the company's purposes

Logicom employees can find the Group User Policy here
Logicom employees can find our full Data Privacy Policy here

5. Enhancing trust with our stakeholders

We have a strong Corporate Governance culture

The purpose of corporate governance is to help build an environment of trust, transparency and accountability necessary for fostering long-term investment, financial stability and business integrity, thereby supporting stronger growth and more inclusive societies. Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.

On 6 March 2003, the Company's Board of Directors resolved to implement all of the provisions of the Corporate Governance Code ("the Code") of the Cyprus Stock Exchange. The Code through its evolution over the years provides detailed guidance as to the effective operation of the Board of Directors and has at its core the principles of:

1. Fairness,
2. Transparency,
3. Accountability,
4. Responsibility,
5. Corporate stewardship
6. Inclusion
7. Diversity

Through the Code Committees, the Company also implements the provisions of the Code for all its subsidiary companies, with the exception of the provisions concerning the composition of the boards of directors, where it is deemed that their composition is more effective by Executive directors.

Logicom's Corporate Governance reports and information about Board committees and officers can be found here

Insider dealing

Insider dealing is the trading of a public company's shares or other securities by individuals with access to non-public information about the company which provides a financial advantage. Generally, trading based on insider information is considered illegal. This is because it is seen as unfair to other investors who do not have access to the information, as the investor with insider information could potentially make larger profits than a typical investor could make. The rules governing insider dealing are complex and vary significantly from country to country. The extent of enforcement also varies from one country to

another. The definition of insider dealing can be broad, and may cover not only insiders themselves but also any persons related to them, such as brokers, associates and even family members. A person who becomes aware of non-public information and trades on that basis may be guilty of a crime.

Logicom strictly prohibits all employees from trading on material non-public information or sharing such information with others. This is illegal in most countries and Logicom does not accept such insider dealing. Such information can be used by investors to trade on the stock exchange or can have an impact on the company's stock price.

Logicom employees in possession of any non-public information must never enter into any trading transactions in the company's shares in the Cyprus Stock Exchange

Logicom employees can find more information in the Code of Conduct here

Protecting Confidential Information

Disclosing confidential information within or outside our organisations can be dangerous and could adversely affect the achievement of our goals and the continuity of our business. It is therefore important for all of us to keep business related information to ourselves and refrain from discussing business related matters with third parties outside Logicom unless there is a clear business reason for doing so. We should also be very careful in communications we have with our colleagues within Logicom to not disclose any sensitive and/or confidential information. If in doubt about what information is sensitive or confidential you must consult with your manager or the Group Compliance Officer. Any unauthorized distribution of confidential or sensitive information may lead to disciplinary action.

All Logicom salary information is confidential and should not be disclosed for any reason, other than as required for appropriate financial reporting purposes. Logicom requests that all employees keep their remuneration package confidential, and avoid providing or otherwise broadcasting this information with other Logicom employees, or with any other third party. Any unauthorized disclosure of salary information by employees may create unnecessary conflict and disputes therefore should be avoided. The Salary Confidentiality Policy which is signed by all employees must be strictly followed. Any un-authorized distribution of confidential salary information may lead to disciplinary action.

Logicom's Staff Handbook containing relevant guidance can be found here and the Salary Confidentiality policy here

We keep accurate books and records and pay our taxes

Logicom, being listed on the Cyprus Stock Exchange, places great emphasis on keeping proper books of account and accurately record all transactions it enters into. This is of vital importance to provide the Group stakeholders with accurate information to make informed decisions. Logicom complies with all applicable International Financial Reporting Standards.

Paying tax is part of the legal and social responsibility of any organisation. Logicom benefits from infrastructure, security, education, health, use of resources, etc so paying taxes is important to be able to maintain the services that make business possible at all. Maintaining accurate books and records is also part of our corporate social responsibility and in order to comply with our legal obligations in relation to paying taxes in all countries we work in. Logicom is committed to pay its fair share back to the communities in which it operates in and wishes to be fully transparent in terms of its tax obligations.

Our Group Financial Statements can be found here

6. In the Market

We act with integrity

Logicom will uphold all related laws relevant to countering bribery and corruption in all the jurisdictions in which it operates. The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for Logicom or under its control.

The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for Logicom

Our Anti Bribery and Corruption Policy applies to all staff members working at all levels and grades, including the Board, directors, senior managers, officers, employees, consultants, contractors and trainees in all countries we have operations. Our staff receive regular training on our Anti Bribery and Corruption Policy, and are bound to conduct their tasks and responsibilities in accordance with the relevant requirements as part of their ongoing employment assessment process or contractual or other relationship with the Group. Any employee who breaches this Policy, whether or not such breach is intentional, may be subject to disciplinary action, which could result in dismissal for gross misconduct.

Third Parties we transact with are expected to have ethical standards that are compatible with this Policy and we reserve the right to terminate our contractual relationship with third parties if they breach this Policy and the right to initiate legal proceedings against staff or third parties for recovering any losses incurred as a result of such breach.

Third Parties we transact with are expected to have ethical standards that are compatible with this Policy and the Code of Conduct

To maintain trust and integrity with our business associates and avoid any unethical or illegal conduct or a potential conflict of interest, we are prudent when accepting or giving gifts and hospitality. Logicom understands that the practice of giving business gifts and hospitality varies between countries and regions. What may be normal and acceptable in one region may not be in another. The test to be applied is whether in all the circumstances the gift or hospitality is reasonable, proportionate and justifiable. The intention behind the gift or hospitality should always

be considered. More information as regards the allowed limits of gifts and hospitality can be found in the Logicom Anti Bribery and Corruption Policy in the link below.

Logicom does not make, and will not accept, facilitation payments or "kickbacks" of any kind. We only make charitable donations to bona fide charities that are ethical and legally constituted under local laws and regulations. Logicom may provide sponsorship for normal marketing and corporate social responsibility purposes.

When you are faced with a choice between integrity and profit, choose integrity without hesitation.

All staff are encouraged to raise concerns in good faith and based on reasonable belief about attempted, suspected or actual bribery or any issue or suspicion of malpractice, at the earliest possible stage.

Staff who refuse to accept or offer a bribe, or those who raise concerns or report another's wrongdoing should not be concerned about repercussions. Logicom encourages openness and will support anyone who raises genuine concerns in good faith under this Policy, even if they turn out to be mistaken.

We are committed to ensuring that no one suffers any detrimental treatment or adverse consequences as a result of refusing to take part in bribery, corruption, improper payment activity, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place, or may take place in the future, or misconduct happens. Detrimental treatment includes dismissal, disciplinary action, threats, negative impact on the professional career or other unfavourable treatment connected with raising a concern.

There are clear reporting channels to Group Compliance available in the Anti Bribery and Corruption policy.

Logicom employees can find the Anti Bribery and Corruption Policy here

We comply with Laws and Regulations wherever we do business

Following applicable laws

Logicom is conducting business in several countries and diverse geographical regions. Our employees are citizens of those countries. We have a responsibility to comply with the laws and regulations of the countries we perform business in. At the same time, we need to comply with laws that are beyond the borders of the countries we operate in. For example, we need to comply with specific US laws that deal with imports and exports of goods and services, anti-bribery, anti-money laundering etc. All Logicom employees have the responsibility to follow all applicable laws that relate to our business. The same applies for dealing with third parties. We have responsibility to follow all applicable laws before making any transaction with a third party.

If there is any doubt at any time for anything relating to complying with related laws for the Logicom business or for dealing with any third party, you have the responsibility to immediately seek support from your manager and/or the Legal department.

Logicom's US Sanctions Policy

The global nature of our business means that we are subject to complex regulation by governmental authorities in the United States among other countries in which we operate, including in regard to economic sanctions and export controls. The policies and procedures set out, which have been adopted by Logicom, as a minimum standard, are designed to ensure compliance with applicable US sanctions and embargoes.

Failure to comply with applicable US Sanctions laws may expose Logicom and individual employees to significant adverse business consequences and/or civil and criminal liability, including criminal prosecution, heavy fines, imprisonment, civil penalties, property forfeitures, loss of export trading privileges, debarment and serious damage to Logicom's name and reputation.

Compliance with this Programme by all employees, regardless of their role or location, is therefore essential. Non-compliance with the Programme will be dealt with promptly and may result in disciplinary measures up to and including termination of employment.

All Logicom employees, contract workers, officers and directors, as well as consultants, representatives, agents, brokers and other intermediaries when they are acting on behalf of Logicom or any Logicom company, shall comply fully with all applicable US laws and regulations. These include, but are not limited to: (a) the Export Administration Regulations, administered by the US Department of Commerce; (b) the International Traffic in Arms Regulations administered by the US Department of State; (c) all sanctions programs administered by the US Treasury Department's Office of Foreign Assets Control, as well as all UN resolutions and trade embargoes.

US Economic Sanctions

The major jurisdictions in or with which Logicom generates business, including the United States, administer economic sanctions laws and regulations targeting individuals, entities, vessels and certain countries/territories. In addition, export controls prohibit unauthorized or unlicensed exports, transfers and sales of certain specified commodities, technology and technical data to certain countries, companies and individuals, as well as (in some cases) re-exports from one third country to another. Due to the extraterritorial reach of US Sanctions requirements, the Logicom has developed this Programme to facilitate compliance and mitigate risk.

The Office of Foreign Assets Control of the US Department of Treasury ("OFAC") administers and enforces laws and regulations that impose economic and trade sanctions based on US foreign policy and national security goals. Relevant regulation is also included in the US Treasury's Countering America's Adversaries Through Sanctions Act ("CAATSA").

OFAC sanctions prohibit trade or commerce with certain US embargoed countries, entities and individuals. In some cases, OFAC sanctions target entire countries and their governments; in other cases, they target only certain government officials and/or other persons or entities associated with sanctioned activity in particular countries or regions. Sanctions targets also include OFAC-designated terrorists, international narcotics traffickers, and persons linked to the proliferation of weapons of mass destruction.

For certain target countries and territories, presently including Crimea, Cuba, Iran, North Korea, and Syria ("Embargoed Countries"), OFAC's prohibitions extend to essentially all unlicensed economic or trade contact with the country, its government, and associated OFAC sanctions targets.

In addition to these comprehensive country/territory-wide sanctions, OFAC also maintains lists of individuals and entities designated as Specially Designated Nationals ("SDNs") to which a blocking requirement applies and with whom transactions are prohibited. This list includes SDNs designated under OFAC sanctions against the Embargoed Countries, but also includes SDNs associated with the countries listed in https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. This list of countries is updated on a regular basis and it is advised that all employees involved in direct client affairs to be familiar with the countries that are included on this list.

The above-referenced OFAC sanctions impose compliance obligations on US Persons. Iran and Cuba sanctions require compliance by all US owned or controlled non-US entities, e.g., non-US subsidiaries of US companies. Non-US domiciled and non-US owned/controlled entities such as Logicom do not have compliance obligations under OFAC's jurisdiction-based sanctions except to the extent of their activity in or through the United States or otherwise involving US Persons, US territory, the US financial system and/or US-Origin Goods. Thus, a non-US person potentially violates OFAC sanctions by involving the US

financial system (including US intermediary banks when paying in US$s) or other US Elements in transactions with the Embargoed Countries, SDNs or other US Sanctions targets, unless OFAC has authorized that transaction. OFAC continuously updates its designations of sanctions targets in response to US law enforcement, foreign policy and national security objectives.

The United States also imposes extraterritorial sanctions, primarily directed against Iran, North Korea, Russia and Syria, under a number of different statutes, executive orders and regulations that seek to deter non-US persons from engaging in a range of sanctionable activity. OFAC refers to these measures as "secondary sanctions" because, unlike the above-referenced "primary" sanctions, they operate beyond US jurisdiction and operate through a designation mechanism rather than traditional methods of US law enforcement. The sanctions that the US State Department and OFAC have authority to impose in response to sanctionable activity range in severity, but could include a requirement on US banks and other US Persons to block all funds and other assets of the designated non-US person in their possession and undertake no further business directly or indirectly with such person, thereby cutting off the designated non-US person's access to the US economy and US financial system.

US Export Controls

The US Government applies export controls to US-Origin Goods on a global basis, including by prohibiting most exports, reexports, or transfers of US-Origin Goods to Embargoed Countries. The range of applicable controls varies depending on the goods, technology, end use, end user, other transaction parties, and destination country.

In addition to the trade embargos imposed by OFAC, the US government agencies with primary responsibility for export compliance are: (i) the US Department of Commerce, Bureau of Industry and Security ("BIS"); and (ii) the US Department of State, Directorate of Defence Trade Controls ("DDTC").

Under the Export Administration Regulations ("EAR"), BIS primarily regulates exports and reexports of US-Origin Goods that have potential strategic significance as well as so called "dual-use" goods, which can be used for both civilian and military applications. BIS controls exports on a case-by-case basis, by examining the nature of the product, the destination, the end-user and the end-use. The EAR prohibits the unlicensed export of nearly all types of US-Origin Goods and technology to certain specified countries, end uses and end-users. BIS and the State Department also administers several lists that restrict certain exports, reexports, or transfers of US-Origin Goods to specific individuals and entities, such as the BIS Entity List, Denied Persons List, and Unverified List (collectively, "Restricted Parties").

Even more restricted are US-origin products (and related technical data and services) specifically designed or modified for military applications, which are designated as "defence articles and services" by DDTC under the US Arms Export Control Act and the International

Traffic in Arms Regulations ("ITAR"). ITAR licensing requirements apply to virtually all exports from the United States (and subsequent re-exports) of defence articles and services. The ITAR also imposes registration and licensing requirements on US Persons engaged in the business of manufacturing, exporting or importing defence articles and services or any related "brokering activities".

When entering into any transaction or accepting any new client, you are required to follow the procedures included in the Client on boarding policy and the US Sanctions policy.

Logicom employees can find the full US Sanctions Policy here.

Anti-Money Laundering

Working closely with the authorities

Money laundering is the process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions.

Illegal arms sales, smuggling, and the activities of organised crime, including for example drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to "legitimise" the ill-gotten gains through money laundering.

At Logicom, we strongly believe in transparency in all affairs with local authorities in the jurisdictions we are operating in. Failure to do so could expose the Logicom in penalties but also loss of goodwill and a damage to our brand image. It is therefore vitally important to cooperate with all local authorities in day to day operations, transactions, investigations, etc. always in consultation with the local General Manager, the Group Compliance Officer or the Head of Group Internal Audit to help combat and avoid Money Laundering. Logicom employees must inform their management and the Group Compliance Officer if they come across any transaction that is attempting to push Logicom to legitimize proceeds of a crime.

We choose well who we do business with

While client due diligence (CDD) is not a legal requirement on Logicom, many regulations like the US and EU Export regulations and the Anti-Bribery and Corruption regulations oblige us to carefully consider who we do business with. Group Compliance has therefore introduced a new customer on-boarding process and a new client application tool to streamline the way we accept clients across the Group. To ensure compliance with relevant

export regulations (as stated above), focus is placed on 2 main players in our sales chain: resellers and end-clients.

Resellers are our distribution customers, the persons/entities we directly transact with in our sales cycle. We need to have good visibility on (i) the entities we transact with, (ii) their management and control and, (iii) their ownership structure. This is important to ensure that we are dealing with honest and truthful businesses and to reduce the risk of working with sanctioned or money laundering entities. This obligation is included in the Client on-boarding policy.

End-customers are the persons/entities who are actually using the goods/services we are selling. These are usually our distribution resellers' or the Services' direct customers. We have strict obligations under US export regulations to know the end users of our products primarily in back to back transactions. For products which are being sold to retailers these obligations are generally less strict but we still need to do our due diligence on the retailers. We therefore have to get information about end users early on in the ordering process. This information will need to be entered into our ERP system. A second screening should be done through the Red Flags checklist available in the ERP system for every order and through our access to screening tools which we are using for screening client information against Sanctions lists and other sources of information. Our Client Due Diligence program contains:

1. Full identification of customer and business entities
2. Development of transaction and activity profiles of each customer's anticipated activity
3. Definition and acceptance of the customer in the context of specific products and services
4. Assessment and grading of risks that the customer or the account presents
5. Account and transaction monitoring based on the risks identified
6. Investigation and examination of unusual customer or account activity
7. Documentation of findings

Knowing our clients is a key defence in case we need to answer to any questions to us by the Regulators therefore it is expected that we all abide very carefully to the Customer on boarding as well as the US Sanctions policies and report to the Group Compliance Officer any issues identified during the Client on boarding process.

Dealing with Public Sector

Working with Public Sector Contracts

Government contracting requires strict adherence to the local government procurement laws and regulations. Such commitments usually have much stricter rules of engagement. All persons dealing with public sector contracts need to understand the specific rules of engagement and be particularly careful in dealing with public sector clients. These requirements also apply to Logicom's subcontractors, vendors, and other partners working with Logicom in such contracts. They apply to interactions with all Government-Owned Entities (GOE) (including government and semi-government organizations).

Conflicts of Interest

We should avoid all cases of conflict of interest that could influence business decisions. Situations which can have a conflict of interest include using a business or personal relationship to influence the outcome of a decision. This is particularly problematic in the case of public sector proposals and contracts, especially if using political relations to influence a decision.

Anti-Bribery and Business Amenities and Gifts

Logicom is fully firm in not providing or accepting bribes or corrupt payments. Never offer or receive either through Logicom or personally bribes or "facilitation payments" either directly or indirectly through third parties e.g. business partners, vendors, or consultants. Any such action, apart from being illegal, is not acceptable by Logicom as it can damage our long-term reputation. We need to conduct all our business with full integrity and in an absolute legal manner.

Dealing with Public Sector Officials

Dealing with public officials poses a particularly higher risk in relation to bribery due to strict rules and regulations in many countries. Bribery of a public official is a criminal offence in many jurisdictions. Be particularly careful when providing expected-by the local culture normal business amenities e.g. lunch, dinner, small customary branded gifts, to ensure that such amenities are considered legal, are perceived as ethical, and are fully in-line with our Anti-Bribery and Corruption policy. Logicom will not provide gifts or hospitality with the intention of persuading anyone to act improperly or to influence a public official in the lawful performance of their duties.

Bribery and corruption by individuals is punishable by law. If Logicom is found to have taken part in corruption it could face a fine, sustain serious damage to its supply chain, be excluded from tendering for public contracts and face serious damage to its reputation. Logicom takes its legal responsibilities very seriously. Special care should be given to facilitation payments, the giving and receiving of gifts and hospitality, charitable donations and sponsorships.

What is not acceptable?

It is not acceptable for you (or someone else on your behalf) to:

- give, promise to give, offer, or accept a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;
- give, promise to give, offer, or accept a payment, gift or hospitality to or from a public official, agent or representative to "facilitate" or expedite a routine procedure.

Logicom employees can find the Anti Bribery and Corruption Policy here

and the Code of Conduct here

We compete fairly

Competition laws help foster and preserve fair and honest competition in the market place. Laws are complex and sometimes unique in specific countries, so all Logicom employees need to take special care in complying with these laws. Be very careful when dealing with competitors as sometimes there are laws that deal with such cooperation if that limits competition in that market or result in monopolies.

Meetings and/or any other kind of communication with competitors is inevitable. Commercial life could not function without meeting our competitors in certain circumstances, such as at trade association meetings, where companies need to tender for a project that could not be performed individually or even when regulators and government agencies invite industry representatives to canvass the views of the industry. While there is no legal prohibition on competitors meeting / communicating with each other, especially when employees are socially related to the competitors, there are strict competition law rules that must be adhered to and penalties may be imposed where such meetings result in a breach of competition law.

If we do not follow this direction and choose an easy option that results in our corporate brand being damaged, it will take a long time and a lot of energy to restore our brand. We shall not take short-cuts in the pursuit of a quick profit, rather we shall choose the right pathway even if it involves a detour, taking one step at a time.

Logicom recognizes that its members operate in a competitive business environment. We would like to caution our employees that all discussions held at meetings or events with Competitors must be conducted in strict compliance to all applicable local Anti-trust or Competition Laws and in accordance with the Company's Policies.

The purpose of this section of the Code of Conduct is to set out Logicom's procedures and policies for compliance with competition law and to provide appropriate guidelines to all employees, wherever located, with regard to competition law and to assist them in complying with it. This policy does not provide a detailed description of the local competition laws in all the countries where Logicom operates; rather it summarises the general principles that underlie most competition laws around the world and provides a practical overview of the rules likely to apply.

Logicom employees can find the Code of Conduct here

We respect the communities we operate in (Corporate Social Responsibility)

Corporate social responsibility ("CSR") is integral to our values and practices. The implementation of CSR practices helps empower accountability, transparency and ethical behaviour, all while taking into account our stakeholders' interests.

Logicom's successful growth comes with a lot of responsibility. As a committed corporate citizen, we cannot overlook the importance of our accountability to society. It is our strong belief that undertaking corporate social responsibility initiatives reinforces our goal of being the leading technology authority in our region, whilst also operating a sustainable business.

CSR Areas of Priority

In the course of a stakeholder survey, the priority areas identified are: Organizational Governance, Labour practices and Human Rights.

Organizational governance: Strong corporate governance is the foundation of our long-term success. The Logicom Board of Directors sets high standards for the Group's employees, officers, and directors.

Labour practices: Our employees are the driving force behind our success and our diverse workforce is the source of our strength in achieving our objectives. Logicom treats its employees with dignity and respect and is an equal opportunity employer.

Human Rights: Logicom strongly supports human rights. We believe that technology is the medium to help human rights proliferation. Moreover we believe that ethical handling of artificial intelligence and data privacy are becoming fundamental human rights.

CSR Actions

- Stakeholder engagement: In this changing world, we recognise the fact that every decision and activity impacts individuals and groups more than ever before, either directly or indirectly. There is a requirement for a systematic stakeholder mapping and engagement plan alongside with a communication plan that will help the company identify all of its stakeholders and risks in a proactive manner, allowing us to mitigate them in a strategic manner.
- ISO 37001:2016 "Anti-bribery management system". The management of Logicom recognizes the importance of working in a transparent and ethical way. For this reason, the decision was made to set up, implement and certify with this standard.
- Employee trainings on CSR and business-related topics are conducted on regular basis.

Our full CSR information and relevant reports here

We believe in Quality

It is the policy of Logicom to create and maintain a culture of excellence with the objective of delivering world-class quality products and services to its customers. This will help the company to maintain its leading position in the markets where it operates.

An important feature of this Policy is that quality can be built into our products and services by following a careful approach, effected with good planning, attention to detail and commitment to quality at each step of the product life cycle process. No amount of post inspection or checking will improve the quality of a product or service. All staff is encouraged to strive towards maximising the quality levels and minimizing the cost of quality, which is the price we pay for not getting things right first time.

Quality means doing it right when no one is watching.

Henry Ford.

Careful consideration is given to the suppliers of equipment to be incorporated into the final product or passed on to our customers.

Every member of staff is expected to be fully conversant with this Policy and the detailed procedures, which apply to one's area of responsibility, and to work consciously to its realisation.

Systems and procedures per the Group Policies and Procedures Manual are mandatory for all employees in order to ensure this Policy and supporting systems and procedures remain effective, and they are reviewed on a regular basis. Moreover, the Cyprus entities have been certified with ISO 9001:2015 Quality Management System Standard.

Logicom employees can find the full Quality Policy in the Employee Handbook here and our Group Policies & Procedures Manual here

We observe and respect our obligations based on our contractual arrangements

Logicom works with a large number of vendors and other business associates in a growing number of countries. It is important to ensure that we remain compliant with our contractual obligations with each and every third party we work with. This is the responsibility of each country manager under the supervision and control of the Group Compliance Department. Failure to comply with our contractual obligations could lead to penalties under the contracts, loss of goodwill and damage to our relationship with our vendors and business associates.

It is therefore very important that country managers and Business Unit Managers train their teams to follow and respect all vendor contracts to reduce the risk of having penalties imposed by our vendors for non-compliance. Failure to comply with vendor and other third-

party contracts may lead in loss of goodwill with our business associates, penalties and loss of business.

We respect personal data

Data Protection is a key priority

Logicom endeavors to meet leading standards for data protection and privacy. We protect all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

While our reasons are founded on ethical and corporate responsibility, our privacy practices as outlined in this policy facilitate the establishment of the following:

- Competitive Advantage: Our emphasis on protecting the privacy of customers, vendors, and employees distinguishes us from our competitors.
- Good Corporate Citizenship: A sound data protection policy and practice is emblematic of reliable corporate citizens that respect data subjects' privacy.
- Business Enablement: Since Logicom uses personal information, privacy notices become a prerequisite to building enduring business relationships.
- Legal Protection: Appropriate privacy notices offer an opportunity to eliminate allegations of unlawful usage of personal information.
- Comply with the General Data Protection Regulation (GDPR): failure to comply with the provisions of the GDPR may expose Logicom to fines that can be significant depending on the breach or non-compliance extend

Data Protection: It's Our Business

Data Privacy Policy

The Logicom Data Privacy Policy is in place to provide a framework for the Data Privacy and Protection implementation. The policy aims to:

- ensure that all of the personal information in Logicom custody is adequately protected against threats to maintain its security.
- ensure that Logicom employees are fully aware of the contractual, statutory or regulatory implications of any privacy breaches.
- limit the use of personal information to identified business purposes for which it is collected.
- create an awareness of privacy requirements to be an integral part of the day-to-day operation of every employee and ensure that all employees understand

the importance of privacy practices and their responsibilities for maintaining privacy.

- make all the employees aware about, the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal information.
- ensure that all third parties collecting, storing and processing personal information on behalf of Logicom provide adequate data protection.
- ensure that applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal information are adhered to.

Company data is an asset belonging to the company. Company data including employee business emails can be audited, as per the Data Privacy Policy, for potential wrong doings.

Data Protection Officer (DPO)
A Data Protection Offices is assigned at Group level and is available in all countries.
According to article 39 of GDPR, in summary the duties of the DPO include the following:

1. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
2. to monitor compliance with this Regulation, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
3. to provide advice where requested as regards the data protection impact assessment and monitor its performance;
4. to cooperate with the supervisory authority;
5. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in GDPR Article 36, and to consult, where appropriate, with regard to any other matter.

Don't think "unlikely" events will never happen.

The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Data Subjects can exercise their rights by contacting the Logicom Data Protection Officer at email dataprotection@logicom.net , telephone 22551000, 26 Stasinou Street, 2003 Strovolos, Cyprus.

Data Privacy Coordinators
Local points of contact, the Data Privacy Coordinators (DPCs), have been established in all subsidiaries in order to help/support the DPO to perform the above duties.

Data Controller
Data Controllers are defined for each business area for which data protection is performed. The responsibilities of the Data Controllers according to GDPR Article 24 include:

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in GDPR Article 40 or approved certification mechanisms as referred to in GDPR Article 42 (described in the policy linked below) may be used as an element by which to demonstrate compliance with the obligations of the controller.

A mistake you see but do not fix becomes your mistake too.

Breach Notification
Any breach involving personal data has to be immediately reported to the DPO who will lead the investigation and if needed, the breach will be reported to the relevant authorities. In this case, the data subjects might to be informed if their rights have been affected. The DPO will lead the communication with the authorities.

Logicom employees can find our full Data Privacy Policy here

Choosing our Suppliers and business associates wisely

The quality of our service and delivery to our customers relies heavily on the quality of our business associates including suppliers, consultants, lawyers, etc.

Logicom recognizes that its Business Associates are effective means of developing, expanding and maintaining its business around the world. However, without careful selection and management, the Business Associate may expose Logicom to reputational risk or criminal proceedings, even if Logicom was unaware of such impropriety.

The laws in the jurisdictions in which the company operates, requires us to do everything necessary to prevent bribery and unethical behavior by ensuring as far as possible that our Business Associates comply with applicable laws in their own jurisdictions, regardless of the business pressure and local custom and practice.

Logicom employees can find our Business Associates Onboarding policy here

We care for our environment

Environmental Management System

Logicom is committed to protecting the environment and the well-being of the communities in which it operates. For this reason, we developed and maintain an Environmental Management System (EMS) at Logicom Public Limited (Cyprus) conforming to the requirements of ISO 14001.

Logicom's EMS focuses on reducing the adverse environmental impacts of its operations by choosing products which are environmentally friendly, delivering products through well-planned routing of vehicles and proper handling of waste materials.

The above system provides the framework for:

- Monitoring and continuously improving the environmental performance of the company
- Monitoring, addressing and conforming to relevant environmental legislation and any other stakeholder and market requirements
- Setting and reviewing environmental objectives and targets
- Implementing objectives and targets through environmental implementation programmes to reduce adverse environmental impacts, pollution and waste disposal from the company's operation and by-products
- Focusing on the continuous awareness and participation of employees

Logicom participates in collective schemes for the management of electrical, electronic and waste. The purpose of this system is to collect waste for recycling and reuse. In order to comply with our environmental policy, this waste should not be disposed of as common municipal solid waste. Instead it should be segregated and disposed of at dedicated collection points.

Logicom implements the efficient use of paper in all its offices in order to minimise waste. Additionally, paper and packaging waste is collected and forwarded to relevant, approved organizations for proper handling and/or recycling.

Logicom encourages the proper collection and recycling of battery waste by approved organizations. Special battery recycle bins have been installed in all our offices and all employees are encouraged to bring their own personal scrap batteries for recycling.

The Executive Management of Logicom encourages the implementation of the aforementioned environmental practices to all countries the company has operations.

Logicom employees can find our full Cyprus Environmental Policy here

7. Group Compliance

Ethics and Compliance Commitment

Logicom is committed to its Ethics and Compliance program. We strive for ensuring compliance with applicable laws and regulations. We train our employees and raise awareness frequent communications and learnings while we continuously improve our monitoring and reporting mechanisms.

Our Group compliance function is mandated to:

- Promote and facilitate a culture of compliance within Logicom.
- Create mechanisms to prevent to the maximum possible extent non-compliance with external Laws and Regulations governing the Group's operations and internal Group policies.
- Perform special investigations, as directed by the Managing Director, for compliance purposes.

Responsibilities of Employees:

- Employees are responsible to read and understand and comply with all policies, laws and regulations in relation to their specific job.
- Must speak up, in case they notice wrong-doings, through the whistle-blowing policy.
- Cooperating in internal investigations.

How to reach the Group Compliance Officer:

Group Compliance Officer: Andreas Zenieris

Telephone: 00357 22 551 052 Ext: 1052

Email: groupcompliance@logicom.net

Address: 26 Stasinou Street, 2003 Strovolos, Nicosia, Cyprus

It is great that organisations are finally recognising the important role a positive compliance culture can have on its business. What remains now is for organisations to implement changes to encourage a positive culture to grow. Understanding that there is no quick-fix is important – widespread change within a single organisation can take time.