Ethics and Compliance Manual

September 2026

Contents

Message from the Chairman of the Board of Directors

Dear Logicom Employees,

In today's fast-paced and constantly evolving business environment, compliance plays a pivotal role in the effective management of modern organizations. Rapid changes in laws and regulations affecting our operations—combined with increased scrutiny from regulatory authorities—require our constant vigilance and unwavering commitment to compliance.

At Logicom, we adopt and promote the highest standards of business and professional conduct. Our culture is built on open communication, integrity, adherence to applicable laws and internal policies, sound corporate governance, trust in our people, and respect for our customers, partners, and society at large. These principles form the foundation of the continued trust our customers, partners, and stakeholders place in our solutions and professional services worldwide.

The Logicom Ethics and Compliance Manual reflects our strong commitment to upholding our policies, complying with laws and regulations, and conducting business with integrity. Together with our Code of Business Conduct, it serves as a practical guide to support informed, ethical, and compliant decision-making across the organization.

Each of us shares the responsibility of protecting and strengthening Logicom's reputation for integrity, compliance, and professional excellence. Every decision we make directly impacts our ability to create meaningful value for our customers and partners.

Thank you for your continued commitment to upholding the compliance standards and ethical values that define our organization.

Dr Christoforos Hadjikyprianou

Chairman, Board of Directors

Message from the Managing Director

Dear Logicom Employees,

Logicom is committed to conducting business in an ethical, legal and compliant manner, placing these principles at the core of its core priorities and values. Adherence to applicable laws and regulations, compliance with our internal policies and ethical decision-making are of paramount importance to the Company's long-term success.

The Logicom Ethics and Compliance Manual provides summaries of our key policies and includes links to the full policy documents, key compliance areas, and ethical guidelines. It should therefore be used, together with our Code of Business Conduct, as a guided document to support sound decision-making and ensure continuous adherence to our core compliance obligations.

Our Ethics and Compliance Manual reinforces both the right and the responsibility of employees to report any wrongdoing they observe through multiple available channels, with a firm commitment to non-retaliation for good-faith reporting. Earning Trust is a fundamental principle achieved by consistently adhering to the standards set out in the Ethics and Compliance Manual.

We rely on every employee to ensure that decisions are made in line with our values, and in an ethical, compliant and lawful manner at all times.

Varnavas Irinarchos

Group Managing Director

1. Introduction to Ethics and Compliance

In a fast moving and continuously evolving business and regulatory environment, compliance has become a critical function for modern organisations worldwide. International businesses face increasing challenges in keeping up with regulatory changes that affect their operations, as laws become more complex, difficult to interpret and sometimes contradictory.

Authorities across jurisdictions are raising compliance expectations, often extending beyond territorial boundaries and impacting entities and individuals in other locations. Non-compliance can result in significant financial and, in some cases, criminal penalties. Key regulatory areas include export controls, anti-trust and competition laws, anti-bribery and corruption laws and data privacy regulations.

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

As penalties continue to increase, ranging from substantial fines to blacklisting and potential criminal liability, compliance has become an essential factor in business decision-making. Regulators increasingly stress the importance of effective compliance programs tailored to the risks faced by each organisation and capable of adapting quickly to regulatory changes.

For international businesses, designing and maintaining a cross-border, multi-jurisdictional compliance program remains a major challenge. Success lies not only in monitoring transactions but in embedding a strong culture of compliance within the organisation through targeted changes in governance, systems, processes and people.

"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 essential that we, in Logicom Group ("Logicom"), continue to strengthen our compliance culture by investing in training and development, improving our processes and reinforcing our compliance efforts to address the complexities of the evolving regulatory environment. Key areas covered in this Manual include export regulations, data privacy and protection, inclusion and diversity.

In recent years, the global focus on ethical business practices has increased significantly, with stricter approaches to transactions and greater emphasis on anti-bribery measures, corporate social responsibility and human rights.

This manual summarizes key policies that Logicom employees must comply with and provides references to the relevant full policy statements where appropriate. It should serve as guide for all Logicom employees in understanding their obligations under their employment contracts.

2. Speak Up and Whistleblowing

At Logicom, we are committed to the highest standards of integrity, transparency, and accountability.

If you see or suspect wrongdoing, you are encouraged to speak up so the Company can review the matter and take appropriate action. Raising concerns helps protect our people, our business, and our reputation.

When should you speak up?

You should report concerns if you become aware of possible misconduct or wrongdoing, such as:

- fraud, corruption, or unethical behaviour
- breaches of Company policies or procedures
- violations of laws or regulations
- misuse of Company assets or confidential information
- behaviour that could harm the Company's reputation

Whistleblowing is intended for genuine concerns. It is not meant to challenge business decisions or to revisit matters already addressed through grievance, disciplinary, or harassment procedures.

You are protected

Logicom does **not tolerate retaliation** against anyone who raises a concern in good faith.

You are protected when reporting a concern if you:

- act **in good faith**, and
- have a **reasonable belief that wrongdoing may have occurred**.

Protection applies even if the concern is not ultimately confirmed. However, knowingly making false or malicious allegations may lead to disciplinary action.

All reports will be handled **confidentially, fairly, and professionally**.

How to report a concern

Concerns should be reported as soon as possible to the **Disclosure Reporting Officer**, as defined in the Disclosure (Whistleblowing) Policy.

You may also report concerns to:

- the **Group Human Resources Manager**
- the **Group Compliance Officer**
- the **Head of Group Internal Audit**

Reports can be made:

- in person
- in writing
- by telephone
- by email
- through the Group website

Anonymous reports are accepted. However, providing your identity may help the Company investigate the matter more effectively.

Logicom Employees can find our Disclosure (Whistleblowing) policy here

3. Our responsibilities to each other

Building trust

Trust is essential to strong working relationships and successful business practices. At Logicom, trust is built every day through our actions, integrity, and respect for others.

We all have a responsibility to act ethically, make responsible decisions, and follow the principles below to maintain trust within our teams and with our partners.

Inclusion and Diversity

Logicom is committed to maintaining a workplace that promotes respect, dignity, equality, and inclusion for everyone.

We do not tolerate bullying, harassment, victimisation, or unlawful discrimination based on characteristics such as race, gender, religion, nationality, disability, sexual orientation, or age.

All employees are expected to treat others with respect and contribute to a safe and inclusive working environment.

Any allegations of harassment, discrimination, or inappropriate behaviour will be taken seriously and investigated in accordance with the Company's policies. Serious breaches may result in disciplinary action, including dismissal.

Logicom also supports equal opportunities for training, development, and career progression for all employees.

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

The role of Leaders

Leaders play an important role in building trust and supporting an ethical culture.

Leaders at Logicom are expected to:

- communicate clearly and set a positive example
- support and motivate their teams
- listen to employees' concerns and encourage open communication
- treat employees fairly and with respect
- create a positive and productive work environment

Leadership at Logicom is not limited to management roles. We encourage leadership and accountability at all levels of the organisation.

Our people's Health and Safety

Logicom is committed to protecting the **health, safety, and wellbeing** of our employees, customers, and visitors. We aim to minimise risks in the workplace and promote safe working practices across all our operations.

Health and safety is a shared responsibility. Managers, employees, and health and safety specialists work together to promote safe practices, identify risks, and continuously improve our working environment.

Employees receive appropriate **training and guidance** on health and safety matters, particularly when new risks arise due to technological changes, environmental conditions, or new work activities.

Employees must also:

- follow all health and safety procedures
- use equipment and machinery responsibly
- wear required protective equipment where applicable
- immediately report any health and safety risks or incidents to their **Health and Safety Officer or General Manager**

Logicom takes appropriate measures to prevent accidents and ensure safe working conditions. These measures include:

- providing necessary **protective equipment** where required
- maintaining equipment so that it operates safely
- ensuring protective equipment is regularly checked and replaced when necessary
- providing appropriate **hygiene and storage facilities**
- informing employees about potential workplace risks
- restricting eating, drinking, or smoking in areas where safety risks may exist (smoking is permitted only in designated areas)

Our employees are our most valuable asset, and we are committed to protecting their health and safety at all times

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

Behaviour outside work

Logicom respects employees' personal freedom outside working hours. However, our behaviour outside work may still reflect on the Company. Employees are therefore expected to act responsibly and avoid conduct that could harm Logicom's reputation.

This includes behaviour in everyday life, when socialising, and when using social media platforms. Employees should always consider the potential impact of their actions on the Company's image.

Personal activities during work time

Working hours should be dedicated to your professional responsibilities. Personal activities, personal business, or the solicitation of business for personal purposes must not take place during Logicom working hours.

Social media

Social media includes platforms such as Facebook, X (Twitter), LinkedIn, blogs, forums, review sites, and other online platforms.

Employees may use social media for personal purposes, but they must do so responsibly and ensure that their online activity does not harm Logicom's reputation.

When using social media, employees must not:

- disclose confidential or sensitive Company information
- damage the Company's reputation or brand
- breach copyright, data protection laws, or Company policies
- post defamatory, offensive, illegal, or inappropriate content
- engage in bullying or harassment
- interfere with work commitments
- use the Company's name to promote products, services, or political views

Employees are also encouraged to use appropriate privacy settings on their personal accounts.

Breaches of this policy may result in investigation and disciplinary action in accordance with Company policies. When leaving the Company, employees must update their professional profiles and remove any access to Company social media tools.

Political activities

Employees may exercise their political rights in their private time. However, personal political views must not be presented as those of Logicom.

Political activities must not interfere with work responsibilities, and employees may not hold official positions in political party committees.

Furthermore, Logicom employees are not permitted to stand as candidates in political elections, be elected to public office, or hold any political position.

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

Managing Conflicts of Interest

A conflict of interest occurs when personal relationships, financial interests, or outside activities could influence — or appear to influence — decisions made in your role at Logicom.

Employees should always act in the best interests of the Company and avoid situations that could create a conflict.

To manage conflicts of interest:

- Avoid personal or financial relationships that may influence your work decisions.
- Do not engage in external business activities that compete with or conflict with Logicom's interests.
- Disclose any actual or potential conflict of interest promptly.
- Obtain approval before undertaking any external work or business activity.
- Report potential conflicts to the HR Manager in accordance with the conflict of interest Disclosure process.

Even if you believe your judgment will not be affected, a conflict may still exist and must be disclosed.

4. Protecting company assets and information

Email and Internet use

Internet and email systems are essential tools for conducting Logicom's business and must be used **responsibly, professionally, and in accordance with Company policies**.

Employees are provided with internet and network access appropriate to their role. Access is protected by individual passwords, which must **never be shared**. Passwords must be changed regularly in accordance with the **Group IT Policy**.

Employees must use internet access responsibly and primarily for work-related purposes.

The following types of websites or online content must **not be accessed or used** through Company systems:

- sexually explicit material
- violent or offensive content
- discriminatory material
- illegal activities or violations of intellectual property rights
- streaming or entertainment services that consume excessive bandwidth unless required for work

Company email accounts are **Company assets** and should be used for work-related purposes only. Employees must not:

- send confidential information without proper authorization
- export Company data outside the organisation
- send offensive or inappropriate messages
- use Company email for illegal or improper activities
- use email for personal matters

Failure to comply with these rules may result in **disciplinary action, including termination of employment**.

To protect Company systems and comply with legal obligations, Logicom may access or monitor business email accounts and internet usage when necessary, including:

- verifying compliance with Company policies
- investigating potential misconduct
- meeting legal or regulatory requirements
- ensuring business continuity and operational needs

Such access will be carried out in accordance with the **Data Privacy Policy**.

Logicom employees can find our full Data Privacy Policy here
Logicom employees can find our full Acceptable Use Policy here

Confidential information

Confidential information is essential to our business and must be protected at all times.

Employees must not disclose or share sensitive or confidential information about Logicom, its employees, customers, or partners unless there is a legitimate business reason and appropriate authorization.

If you are unsure whether information is confidential, consult your **manager or the Group Compliance Officer** before sharing it.

Unauthorized disclosure of confidential information may result in disciplinary action.

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

Insider dealing

Insider dealing occurs when someone trades in a company's shares using **material, non-public information** that could influence the share price.

This practice is illegal in many jurisdictions and strictly prohibited at Logicom.

Employees must never:

- buy or sell Logicom shares while in possession of confidential or non-public information
- share such information with others who may use it for trading purposes

Employees who have access to sensitive information must ensure that it is protected and not misused.

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

Approvals and Commitments

Employees must obtain the appropriate approvals before making commitments on behalf of the Company.

This includes agreements with customers or suppliers, pricing decisions, contract changes, employment commitments, or any action that may bind the Company or its assets.

Employees must follow internal approval procedures and ensure commitments are properly recorded and reported.

Unauthorized commitments may lead to disciplinary action and the Company may seek compensation for any resulting damages.

Logicom employees can find our Group Policies and Procedures Manual here

5. Integrity in the Marketplace

Integrity and Anti-Bribery

Logicom is committed to conducting business with **honesty, integrity, and transparency**. We comply with all applicable laws and regulations relating to **bribery and corruption** in every country where we operate.

Bribery, corruption, and improper payments are strictly prohibited. The prevention, detection, and reporting of such activities is the responsibility of everyone working for or on behalf of Logicom.

The **Anti-Bribery and Corruption Policy** applies to all employees, directors, officers, consultants, contractors, and other individuals working with the Group. Employees receive regular training and are expected to follow the requirements of this policy at all times. Any breach may result in disciplinary action, including dismissal.

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

Gifts and Hospitality

Business gifts and hospitality may sometimes be appropriate in building professional relationships. However, they must always be **reasonable, proportionate, and transparent**, and must never be intended to improperly influence a business decision.

Employees should always consider the purpose and value of any gift or hospitality offered or received. The limits and rules governing gifts and hospitality are defined in the **Anti-Bribery and Corruption Policy**.

Facilitation Payments and Donations

Logicom **does not allow facilitation payments or kickbacks** of any kind.

Charitable donations and sponsorships may only be made for legitimate charitable, marketing, or corporate social responsibility purposes and must comply with applicable laws and company procedures.

Working with Third Parties

We expect our business partners, suppliers, and other third parties to follow ethical standards consistent with our policies. Logicom may terminate relationships with any third party involved in bribery or corruption.

Reporting Concerns

Employees are encouraged to report any suspected or actual bribery, corruption, or unethical behaviour as soon as possible through the available reporting channels.

Logicom does **not tolerate retaliation** against anyone who raises a concern in good faith or refuses to participate in bribery or improper conduct.

Logicom employees can find the Anti Bribery and Corruption Policy here

Compliance with applicable laws and regulations

Logicom operates across multiple countries and regions, employing local citizens. We must comply with the laws of the countries where we do business, as well as certain international regulations, such as U.S. laws on imports/exports, anti-bribery, and anti-money laundering.

All employees are responsible for following applicable laws in their work and when dealing with third parties. Before any transaction, compliance must be ensured. If there is any uncertainty, employees must promptly seek guidance from their manager 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 (**"EAR"**), administered by the US Department of Commerce; (b) the International Traffic in Arms Regulations (**"ITAR"**) 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, 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 regulations are 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, such as Belarus, Crimea and Russian occupied Ukraine Cuba, Iran, North Korea and Syria ("**Embargoed Countries**"), OFAC's prohibitions can 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. In addition, SDNs may also be designated under US thematic sanctions programs not targeting a specific country or territory.

The above-referenced OFAC sanctions impose compliance obligations on US Persons. Iran and Cuba sanctions require compliance also 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 Belarus, Crimea/ Russia occupied Ukraine, Cuba, Iran, North Korea and Russia, 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, software, 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 Defense Trade Controls (**"DDTC").** Under the 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. Often, the specific EAR restrictions that may be applicable depend on the Export Control Classification Number ("**ECCN**") of the underlying US-Origin Goods. Some US-Origin Goods classified in restrictive ECCNs may require BIS authorization to many different countries and/or end users, and some in less restrictive ECCNs may require BIS authorization to only few countries and/or end users.

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, , Military End-User List and Military Intelligence End-User List (along with the OFAC SDN list, EU and UN sanctions/restricted lists and other similar lists, persons/entities listed on these lists are collectively referred to as "**Restricted Parties**").

The EAR also contain a range of end user/end use controls that often can apply to any transaction involving US-Origin Goods regardless of the country of destination. For example, the EAR has restrictions on transactions involving nuclear, chemical/biological weapons and missiles, certain military end uses and uses in certain designated countries like China. The EAR can hold Logicom responsible for proceeding in transactions with others when Logicom personnel know or have reason to know (*e.g.* when there are "red flags") these other parties will not comply with US export controls. These types of end user/end use restrictions are informally referred to as "catch all" controls.

Even more restricted are US-origin products (and related technical data and services) specifically designed or modified for military applications, which are designated as "defense articles and services" by DDTC under the US Arms Export Control Act and the 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 defense 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/UN/EU Sanctions and Export Control Compliance Policy, and all other relevant procedures.

Logicom employees can find the full US Sanctions Policy here.

Anti-Money Laundering and responsible Business Partners

Logicom is committed to conducting business in a transparent and lawful manner. We comply with all applicable anti-money laundering (AML), sanctions, and export control laws in the jurisdictions where we operate.

Money laundering is the process of disguising the origins of illegally obtained funds to make them appear legitimate. Logicom does not tolerate any activity that may support or facilitate money laundering or other financial crime.

Employees must remain alert to suspicious transactions or unusual business activities and must report any concerns to their manager or the Group Compliance Officer immediately.

Working with the authorities

Logicom maintains open and transparent cooperation with regulatory and law enforcement authorities. Where required by law, the Company will fully cooperate with investigations and regulatory requests.

Employees must ensure that any contact with authorities relating to investigations, regulatory inquiries, or sensitive matters is handled in coordination with management, the Group Compliance Officer, or Group Internal Audit.

Knowing our business partners

Conducting business with reputable partners is an important safeguard against financial crime, sanctions violations, and other regulatory risks.

Before establishing business relationships, Logicom performs appropriate **client and partner due diligence** in accordance with the Group's policies. This helps ensure that we understand who we are doing business with and that we do not engage with sanctioned, illegal, or unethical entities.

This due diligence includes understanding:

- the **resellers and partners** we transact with directly, and
- where required, the **end users of the products or services** we provide.

In some cases, particularly where export regulations apply, Logicom must ensure that its products and services are not supplied to restricted parties or used for prohibited purposes.

Employees must follow the **Client On-Boarding and Due Diligence procedures** and report any concerns identified during this process to the **Group Compliance Officer**.

Fair competition

Logicom is committed to competing fairly, ethically, and in full compliance with applicable competition and antitrust laws in all markets where we operate.

Competition laws are designed to promote open and honest markets and to prevent practices that restrict competition. Employees must ensure that their conduct always reflects the principles set out in this Ethics Manual and the Code of Business Conduct.

Employees must never engage in discussions or agreements with competitors that could improperly influence the market. In particular, employees must not discuss or agree with competitors on matters such as:

- prices, pricing strategi es, or discounts
- allocation of customers, markets, or territories
- coordination of bids or tenders
- limiting production, supply, or competition

Interaction with competitors may occur in legitimate contexts, such as industry events, trade associations, or regulatory consultations. However, employees must exercise caution and avoid any discussions that could be interpreted as anti-competitive.

If a conversation with a competitor raises concerns about competition law, employees must end the discussion immediately and seek guidance from their manager or the Group Compliance Officer.

If we fail to follow these principles and choose shortcuts that damage our corporate reputation, rebuilding our brand may require significant time and effort. We should never pursue quick profits at the expense of our integrity. Instead, we must always choose the right path, even if it requires more time and effort, and move forward step by step with honesty and responsibility.

Failure to comply with competition laws may expose both the Company and the individuals involved to significant legal penalties, financial fines, and reputational damage.

Logicom employees can find the Code of Business Conduct here

Dealing with Public Sector

Working with government entities and public sector organisations requires strict compliance with applicable laws, procurement rules, and ethical standards.

Interactions with **public officials** present a higher risk of bribery and corruption because many jurisdictions impose strict legal restrictions on providing gifts, hospitality, or other benefits to government representatives. Violations can result in severe penalties for both the individual and the Company.

Employees involved in public sector contracts must therefore exercise particular care and ensure that all interactions are **lawful, transparent, and properly documented**.

When dealing with public officials, employees must:

- comply with all applicable **government procurement laws and regulations**
- avoid any **conflicts of interest or improper influence**
- never offer, promise, or provide **bribes, facilitation payments, or improper advantages**
- ensure that any **gifts, hospitality, or business courtesies** are lawful, reasonable, and in line with the **Anti-Bribery and Corruption Policy**
- follow all relevant Company procedures and seek guidance when unsure

Logicom expects the same high standards from **subcontractors, vendors, and other partners** involved in public sector projects.

Failure to comply with anti-corruption or public procurement laws may result in **criminal penalties, significant financial fines, exclusion from public contracts, and reputational damage**.

Employees should seek guidance from **management or the Group Compliance Officer** if they are unsure about the appropriate course of action when dealing with public officials.

Red Flags When Dealing with Public Officials

Be alert to situations that may indicate a risk of bribery or improper conduct, such as:

- Requests for **unusual payments, commissions, or facilitation payments** to speed up approvals or permits.
- Requests to provide **gifts, hospitality, travel, or other benefits** to public officials outside normal business practice.
- Pressure to **use a specific intermediary, consultant, or agent** who has close connections with government officials.
- Requests to **hide the true purpose of a payment** or to make payments through unofficial channels.
- Lack of transparency in procurement processes or attempts to **influence a public tender unfairly**.

If you encounter any of these situations, **do not proceed without guidance** and report the matter to your **manager or the Group Compliance Officer**.

Logicom employees can find the Anti Bribery and Corruption Policy here and the Code of Business Conduct here

Choosing our suppliers and business associates wisely

Our suppliers and business partners play an important role in delivering quality services to our customers.

Logicom expects its suppliers, consultants, and other business associates to operate with **integrity and in compliance with applicable laws and ethical standards**.

Before entering into business relationships, Logicom performs appropriate **due diligence** to ensure that our partners are reputable and aligned with our values. Employees involved in selecting or managing business partners must follow the relevant Company procedures.

Logicom may terminate relationships with business partners who engage in **illegal, unethical, or improper conduct**.

Logicom employees can find our Business Associates Onboarding policy and procedures here

Respecting our contractual obligations

Logicom works with a wide range of vendors, suppliers, and business partners across many countries. Maintaining trust with our partners requires that we **honour the commitments we make in our contracts**.

Employees must ensure that all contractual obligations with vendors, customers, and other partners are respected. Failure to comply with contractual terms may result in penalties, damage to business relationships, and reputational harm.

General Managers and Business Unit Managers of each country are responsible for ensuring that their teams understand and comply with the contractual commitments that apply to their work.

6. Responsibility to Society

Corporate Social Responsibility

Corporate Social Responsibility (CSR) is an integral part of Logicom's values and business practices. As a responsible corporate citizen, we are committed to conducting our business in a way that promotes accountability, transparency, and ethical behaviour while considering the interests of our stakeholders and the communities in which we operate.

Logicom believes that sustainable business success goes hand in hand with responsible corporate conduct. Our CSR initiatives support our goal of being a trusted technology leader while contributing positively to society.

Our main CSR priorities include:

Organizational Governance
Strong corporate governance is the foundation of our long-term success. Logicom's Board of Directors sets high standards of integrity, accountability, and ethical conduct across the Group.

Labour Practices
Our employees are the driving force behind our success. Logicom is committed to providing a safe, respectful, and inclusive working environment and operates as an equal opportunity employer.

Human Rights
Logicom supports and respects internationally recognized human rights. We believe technology can contribute positively to society when used responsibly, including the ethical use of artificial intelligence and responsible data privacy practices.

To support these priorities, Logicom promotes stakeholder engagement, employee training, and responsible business practices across the Group.

We care for our environment

Logicom is committed to protecting the environment and minimizing the environmental impact of its operations. We aim to conduct our business responsibly by promoting sustainable practices and encouraging employees to contribute to environmental protection in their daily activities.

The Company maintains an **Environmental Management System aligned with ISO 14001 Standard**, focusing on responsible resource use, waste reduction, and continuous improvement of environmental performance.

Our environmental practices include:

- **Complying with environmental laws and regulations** in all countries where we operate.
- **Reducing our environmental footprint**, including energy consumption, emissions, and waste generated from our operations.
- **Promoting responsible waste management and recycling**, including electrical and electronic equipment, packaging materials, batteries, ink cartridges, and plastic, metal drink cartons
- **Reducing paper consumption** through digital processes and responsible printing practices.
- **Using energy, water, and natural resources efficiently** across our offices and operational activities.

- **Encouraging sustainable logistics and transportation practices** to reduce environmental impact.
- **Selecting environmentally responsible products and suppliers** whenever possible.
- **Ensuring proper disposal of electronic and hazardous waste** through approved recycling or disposal channels.
- **Supporting climate responsibility initiatives** aimed at reducing carbon emissions and improving environmental sustainability.
- **Promoting sustainability across our supply chain** by encouraging suppliers and business partners to adopt responsible environmental practices.
- **Raising environmental awareness among employees** and encouraging environmentally responsible behaviour in the workplace.
- **Continuously improving our environmental performance** through monitoring, evaluation and the setting of environmental objectives and targets.

Employees are encouraged to support these efforts by adopting environmentally responsible practices in their daily work and by contributing ideas that help reduce the environmental footprint of our operations.

Logicom employees can find our full Cyprus Environmental Policy here

Quality

Logicom is dedicated to delivering high-quality products and services to our customers. Upholding a culture of quality and excellence is vital to preserving our leadership position across all the markets we serve.

Quality is built through careful planning, attention to detail, and continuous improvement at every stage of our operations. Every employee plays a role in maintaining these standards and is expected to follow the Company's policies and procedures relevant to their responsibilities.

"Quality means doing it right when no one is watching."
Henry Ford.

Logicom's quality management systems, including ISO 9001 certification for the Cyprus (Logicom Public, Logicom Solutions, Newcytech Business Solutions and Newcytech Distribution) and Greek (ICT Logicom Solutions) entities, support our commitment to consistent service excellence and enhanced customer satisfaction.

The management of Logicom continuously sets quality objectives and targets, assesses the performance of the company through quality performance indicators and reviews and revises its objectives and targets on a systematic basis with the aim of continual improvement of the policies, procedures, practices and the corporate performance.

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

7. Data Privacy and Cybersecurity

We respect personal data

Protecting personal data is a key priority at Logicom. We are committed to respecting the privacy of our employees, customers, suppliers, shareholders, and other individuals whose personal data we process.

Logicom strives to maintain high standards of **data protection and privacy** and complies with applicable data protection laws, including the **General Data Protection Regulation (GDPR)**.

Employees must ensure that personal data is:

- collected and used only for **legitimate business purposes**
- handled **securely and confidentially**
- accessed only by those who are **authorized to use it**
- retained and disposed of in accordance with Company policies and legal requirements

All employees have a responsibility to protect personal data and to follow the requirements set out in the **Logicom Data Privacy Policy**.

Data Privacy Policy

Logicom has implemented a **Data Privacy Policy** that establishes the framework for protecting personal data across the Group.

The policy aims to ensure that:

- personal data is protected against unauthorized access, loss, or misuse
- employees understand their responsibilities regarding privacy and data protection
- personal data is processed only for legitimate and clearly defined purposes
- third parties processing data on behalf of Logicom maintain appropriate data protection standards
- applicable laws and contractual obligations regarding personal data are respected

Data Protection Governance

Logicom has established a data protection governance structure to ensure compliance with applicable data protection laws.

The **Group Data Protection Officer (DPO)** oversees the Company's data protection framework, monitors compliance with privacy laws and Company policies, and acts as the main contact point for data protection authorities.

To support the DPO, **Data Privacy Coordinators (DPCs)** are appointed in local entities to assist with the implementation of data protection practices and to act as local points of contact for employees.

In addition, designated **Data Controllers** within business areas are responsible for ensuring that personal data is processed in accordance with applicable laws and Company policies.

Employees should seek guidance from their **manager, the local Data Privacy Coordinator, or the Data Protection Officer** if they have questions about the handling of personal data.

Data Protection Officer (DPO)

Logicom has appointed a **Group Data Protection Officer (DPO)** who oversees the Company's data protection framework and ensures compliance with applicable data protection laws.

The DPO:

- advises the Company and employees on data protection obligations
- monitors compliance with privacy laws and Company policies
- provides guidance on data protection impact assessments
- cooperates with supervisory authorities and acts as the contact point for data protection matters

Employees may contact the **Data Protection Officer** for guidance on privacy-related matters.

Reporting Data Breaches

Any suspected **personal data breach** must be reported immediately to the **Data Protection Officer** so that appropriate action can be taken and, where required, the relevant authorities and affected individuals can be notified. Employees can raise their data privacy concerns through the Suggestion/Incident Request workflow or by directly contacting the DPO.

Logicom employees can find our full Data Privacy Policy here

Cybersecurity Framework

Logicom has implemented an Information Security Management System (ISMS) framework that establishes the principles, governance arrangements and control standards for protecting the Group's information assets, systems and services. The framework is designed to safeguard the confidentiality, integrity and availability of information and to support compliance with applicable legal, regulatory and contractual obligations. It is built around the Group Information Security Policy and is supported by a set of related policies, standards and procedures covering key cybersecurity domains, including identity and access management, acceptable use, change management, cloud security, incident management, backup and recovery, vulnerability and patch management, mobile device security, email security, network security, cryptographic controls, privileged access management, endpoint security and system development and maintenance.

Logicom Group, together with Logicom Solutions Ltd, Newcytech, Newcytech Distribution Ltd, and ICT Logicom Solutions, is certified against the latest version of ISO/IEC 27001 and undergoes annual external audits to maintain certification. This reflects the Group's commitment to applying a structured, risk based and continuously monitored approach to information security governance and control.

In support of this framework, the Group carries out a range of cybersecurity activities and assurance measures, including penetration tests, security reviews, phishing campaigns, dark web monitoring, 24x7 security operations monitoring, risk assessments, vulnerability assessments and other initiatives designed to strengthen resilience, identify weaknesses and enhance the overall security posture of the Group.

The cybersecurity framework aims to ensure that:

- information and systems are protected against unauthorized access, misuse, disruption, alteration or loss
- employees understand their responsibilities in maintaining a secure working environment
- cybersecurity risks are identified, assessed and managed through appropriate controls and processes
- incidents are detected, reported, investigated and addressed in a timely and coordinated manner
- vulnerabilities and emerging threats are proactively identified through testing, monitoring and assessment activities
- third parties and connected entities are subject to appropriate security expectations where required
- the Group maintains resilience and preparedness to respond to cyber threats and operational disruptions

Cybersecurity Governance

Logicom has established a cybersecurity governance structure to provide oversight of the Group's information security framework and related risk management activities. The Cybersecurity Committee is the body responsible for the overall governance of cybersecurity across the Group. It oversees the cybersecurity strategy, reviews key risks and incidents, monitors the effectiveness of the control environment and supports the continuous improvement of the Group's security posture.

The Cybersecurity Committee also provides oversight in relation to the Group's Information Security Policy, supporting standards and procedures, security assessments, awareness initiatives and preparedness for incident response and business continuity.

The Group's Information Security Policy forms the core of the cybersecurity governance framework and is supported by linked standards, policies, and procedures that define the control requirements to be followed across the organization. The framework is reviewed and maintained as part of the Group's formal governance processes and is supported by defined roles and responsibilities across management, IT, internal audit and employees.

Employees should seek guidance from their manager, Group IT or the appropriate internal stakeholders if they have questions about cybersecurity requirements or the secure handling of information and systems.

Information Security Policy

Logicom has adopted an Information Security Policy that establishes the overall framework for protecting the confidentiality, integrity and availability of the Group's information assets. The policy applies across the Group's business processes, systems, services, personnel, and supporting technologies, including infrastructure, cloud environments, applications, communication services, and employee devices. It also applies to contractors, consultants, and third parties who access or process information on behalf of the Group.

The Information Security Policy aims to ensure that:

- information assets are protected through appropriate technical and organizational measures
- security requirements are clearly defined and communicated to employees and relevant third parties
- access to systems and data is authorized, controlled, and monitored
- vulnerabilities and weaknesses are identified and addressed in a timely manner
- the Group maintains appropriate safeguards to support secure operations, resilience, and recovery
- information security practices remain aligned with legal, regulatory, and contractual obligations

Reporting Cybersecurity Incidents

Any suspected or actual cybersecurity incident must be reported immediately through the Group's defined incident reporting channels so that appropriate action can be taken. Prompt reporting is critical to enable timely investigation, containment, response, recovery and escalation where required.

Cybersecurity incidents should be reported through the following channels:

- Email: security-incidents@logicom.net
- Phone: 1111 – Group IT Department
- Ticket: Select type = incident

Upon receipt of a reported incident, the responsible Group IT Administrator performs a preliminary investigation to validate the incident and initiate the required response actions. Where appropriate, the matter is escalated to Group IT management and recorded in the Cybersecurity Incident Register, while the representative of the Cybersecurity Committee is informed and oversees the investigation as needed.

Employee Responsibilities

All employees have a responsibility to contribute to the protection of Logicom's information, systems and services. Employees are expected to comply with the Information Security Policy and related standards, follow secure working practices, protect Group's information from unauthorized disclosure or misuse and report any suspected incidents, weaknesses or suspicious activity without delay. The effectiveness of the Group's cybersecurity framework depends on the active participation and awareness of all personnel.

8. Governance, Financial Integrity and Compliance

Building trust with our shareholders, customers, partners, and communities is essential to Logicom's long-term success. We achieve this by acting with integrity, maintaining transparency, and complying with all applicable laws and regulations.

Corporate Governance

Logicom maintains a strong corporate governance culture that promotes fairness, transparency, accountability, and responsible management.

As a company listed on the Cyprus Stock Exchange, Logicom follows the Corporate Governance Code and implements governance practices designed to ensure effective oversight, responsible decision-making, and sustainable growth.

These principles guide how our Board of Directors, management, and employees work together to achieve the Company's objectives while protecting the interests of our stakeholders.

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

Accurate Records and Responsible Tax Practices

Logicom is committed to maintaining **accurate books, records, and financial reporting**. As a listed company, we follow all applicable accounting standards and ensure that all transactions are properly recorded.

Accurate financial information is essential for maintaining the trust of our stakeholders and supporting responsible decision-making.

Logicom also complies with all applicable tax laws in the countries where it operates and is committed to meeting its tax obligations responsibly and transparently.

Our Group Financial Statements can be found here

Group Compliance function

Logicom is committed to maintaining a strong Ethics and Compliance culture across the Group. We strive to ensure compliance with all applicable laws, regulations, and internal policies in every jurisdiction where we operate.

To support this commitment, Logicom provides regular training, raises awareness through ongoing communication and learning initiatives, and continuously improves its monitoring and reporting mechanisms.

The **Group Compliance function** is responsible for:

- Promoting and supporting a strong culture of ethics and compliance throughout the organization.

- Establishing mechanisms aimed at preventing, detecting, and addressing non-compliance with applicable laws, regulations, and internal policies.
- Conducting or supporting compliance investigations when required, including special investigations as directed by senior management.

Responsibilities of Employees:

All employees play an important role in maintaining Logicom's ethical culture. Employees are expected to:

Read, understand, and comply with all applicable laws, regulations, and Company policies relevant to their roles.

Speak up and report any suspected wrongdoing or unethical behaviour through the appropriate reporting channels, including the **Whistleblowing Policy**.

Cooperate fully with internal reviews or investigations when required.

By acting with integrity and responsibility, each employee contributes to maintaining Logicom's reputation as a trusted and ethical business partner.

How to Contact the Group Compliance Officer

If you have questions about this Code, need guidance, or wish to report a concern, you may contact the **Group Compliance Officer**:

How to reach the Group Compliance Officer:

Group Compliance Officer: Foivia Charalambous

Telephone: 00357 22 551 026 Ext: 1026

Email: groupcompliance@logicom.net

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

Failure to comply with this Code may result in disciplinary action in accordance with Company policies.

A strong ethics and compliance culture is essential to sustainable business success. At Logicom, this culture is built through the actions and commitment of every employee.

By acting with integrity, making responsible decisions, and speaking up when concerns arise, we protect our reputation and strengthen the trust placed in us by our colleagues, customers, partners, and communities.