Code of Conduct

Core Regulation:

Corporate Culture

Relevant Company Domain:

Compliance; Human Resources

Sensitivity Classification:

Public

Related Internal Acts:

N/a

Whom it Concerns:

All employees

Effective: [insert date]

Notification:

Distribution list: *all employees*

Contents

SUMMARY OF CHANGES

Changes in force as of: *n/a*

Reasons for changes : *n/a*

1. GENERAL PROVISIONS

1.1. Introduction

This Code of Conduct (hereafter: the "**Code**") establishes a set of standards that govern the way we deal with each other, our customers, shareholders, government(s), regulators, suppliers, competitors, the media and the public at large.

While reaching our business goals is critical to Company's success, it is also important to achieve them in the right manner. Therefore, as a responsible corporation, the Company is committed to conducting its business activities and other relationships with the highest standards of ethics, integrity, honesty, fairness and professionalism – in every respect, without exception, and at all times.

Therefore, the Code sets out a common baseline of ethical and behavioural standards required of all of us.

1.2. What is the Purpose of this Code?

By following the ethical and behavioural practices outlined in the Code and incorporating elements in our day-to-day activities, we will continue to promote a culture of high integrity in the Company with the purpose to reduce any operational, reputational and/or compliance risk that may cause harm to the Company and/or other entities or persons.

1.3. To whom does this Code of Conduct apply?

The term "we" stands for every employee and every manager of the Company. Therefore, complying with the Code is part of the terms and conditions of our employment with Nexi Croatia together with its wholly owned subsidiaries, if any.

The Code also applies to all persons that are in any type of work relationship with the Company (students, third party workers, employment agency employees, seconded employees, advisors and other partners).

1.4. What is required from us?

We are expected and required to assess every business decision and every action on behalf of the organization in light of whether it is right, legal and fair and within our risk appetite. This applies at all levels of the organization, from major decisions made by the Management Board to day-to-day business transactions.

1.5. The Code as a Guidance Document

The Code intends to help employees and managers in meeting expectations set out in the Code and making assessments based on a wording of the Code that is user friendly and understandable to all.

1.6. What is the Role of Managers?

In order for this Code to be effective, the managers, as our business leaders, consistently need to demonstrate resolute integrity in complying with the Code themselves but also to promote awareness and compliance with the Code with their teams.

This is very important because employees often take their indications of behaviour from their managers.

An additional role of managers manifests in the fact that employees most frequently report any noticed misconduct to their managers first of all and, eventually, to other organisational units such as Human Resources.

Therefore, it is crucial for those who receive such information to address it promptly and with the seriousness it deserves and to notify the Human Resources and/or Head of Compliance without exception and regardless of manager's personal opinion on the matter.

1.7. How to Apply this Code?

Not every situation can be addressed specifically in the Code. We need to apply the principles outlined in the Code in exercising our judgment also in situations without clear right or wrong answers.

However, it may be helpful for us to apply a process such as the one below before making these types of decisions.

Nevertheless, if we are still uncertain, we should seek the advice and direction of a more senior manager, head of Compliance or head of Human Resources (or in the case of a head of first level unit, the Company Secretary or head of Compliance) so that all relevant interests are fully recognized and properly served.

Therefore, when we recognize that we are faced with a challenging decision that engages the principles outlined in the Code, we should:

Step 1: Collect the necessary information, and:

- Consider what is right, legal and fair, without rationalizing.

Step 2: Consider the available options, and:

- Weigh the business and ethical pros and cons
- Consider the impact of the options on Company's different stakeholders
- Think about the long-term impact of our decision

Step 3: Develop a preliminary decision and test it by asking ourselves:

- Does it strike the right balance?
- Do I think I would be able to explain the decision to those affected by it, or even to my close family members in a way that would not embarrass the Company or me?
- Might this decision harm Company's or my reputation?
- Should I get help from my manager or others to make the decision?

Step 4: Make the decision and be transparent, and:

- Acknowledge difficult ethical decisions that make us uncomfortable and may in fact require us to choose between two imperfect outcomes
- We should consider reviewing difficult decisions with our managers.

Remember that, as we commit ourselves to a course of action, our Chief Executive Officer and Management Board and Supervisory Board are expecting us to make decisions that are right, legal and fair and that it may be reflected upon their responsibility as well.

2. CONTENTS

2.1. Compliance with the Laws

Concern for what is legally and ethically acceptable should be our first consideration in all business decisions and actions, and that includes compliance with the law. Payment services and processing services are heavily regulated in all jurisdictions in which we operate. We need to be familiar with and observe all laws and regulations relating to Company in the jurisdiction(s) in or for which we work or that is/are impacted by the decisions that we make. We must avoid performing any task that could reasonably be considered legally suspect, even if it might be common practice in the country or region.

Adhering to the requirements in the Code and Company's other policies and procedures that relate to the Company as a whole, or our business segment and job function will help us fulfil these requirements.

2.2. Personal Integrity

2.2.1. Gifts and Entertainment

We may not accept, offer or give, directly or indirectly for ourselves or for anyone else, gifts, entertainment or other benefits of value (referred to as "Gifts"), having more than nominal value, from or to existing or potential customers, suppliers, employees or others seeking to do business with the Company, without following the approval procedure prescribed in Gifts Register Policy.

Nominal value of a gift means a value which is usually consistent with accepted business practices, and which can be estimated in monetary value. An inexpensive bottle of wine or free passes to the movies are token/nominal but front row seats at a big sporting match and a week at a holiday house are definitely not.

For clearance sake, any gift or entertainment/hospitality below value of EUR 50 is of nominal value and such gifts/hospitality can be accepted without following the approval procedure prescribed in Gifts Register Policy.

Furthermore, we must never accept, offer or give, directly or indirectly, Gifts of any value where they may be construed as an attempt to bribe or influence a decision or alter the provision or receipt of a service, or where it might otherwise be inappropriate in light of the underlying business relationship or the roles of the individuals involved. We must also never solicit for Gifts of any size at any time. To determine a nominal value, we should consider whether the Gift (or combination of Gifts from or to the same individual or organization) could reasonably be construed as an attempt to influence our behaviour or that of the Company. This also applies in circumstances where we are offering or giving the Gift. We should also consider the value of the Gift in relation to our personal situation (or that of the recipient). It is also important to consider the circumstances, nature and timing of the Gift. For example, Gifts should be avoided to be given or accepted during pending tender procedures or legal procedures.

If the potential recipient of a Gift or one of their family members is, or could be perceived as a Public official (domestic or foreign, or international), e.g., member of government or employee of a state-owned or state-controlled agency, we must also make sure that we are complying with the Anti-Bribery and Anti-Corruption part of

this Code and any related policies and procedures, as failure to do so could result in very serious penalties. Therefore, Gifts to public officials should be avoided.

We may accept, offer or give Gifts of nominal value as prescribed in Gift Register Policy provided that they:

- are not in cash or readily convertible to cash (such as securities, or money orders);
- are consistent with accepted business practices in our region of Slovenia and Croatia;
- cannot be construed as an attempt to bribe or influence, or as a form of payment for a particular transaction or a referral;
- do not contravene any law or regulation, and would not compromise our integrity or that of the Company itself (or, in circumstances where we are offering or giving the Gift, the integrity of the recipient or their organization); and would not adversely affect our reputation or the reputation of Company if knowledge of the Gift was to become public.

There may also be times when we are invited to attend a networking, educational, sporting or other event as a guest of an existing or potential customer or supplier. We cannot accept an offer by the third party to pay for our travel and accommodation costs, and we should be alert to the fact that attending these events often creates the appearance of a conflict of interest even when we pay for the travel costs ourselves following the Gifts Register Policy.

Here are some examples to help us interpret these rules:

- Being taken to lunch or dinner by a supplier would not normally be prohibited even though the supplier is likely trying to maintain or extend its services to the Company, provided that the lunch or dinner is consistent with accepted business practices.
- This applies also equally when taking a customer to lunch or dinner.
- We may not offer to pay the travel or overnight accommodation expenses of a customer or a potential customer without first obtaining the approval according to Gifts Register Policy.
- Taking (or being taken by) a customer or a supplier to a local sporting or other event would generally be acceptable, subject to being reasonable and consistent with accepted business practices. Giving or accepting tickets to events for personal use would be considered a Gift and would only be acceptable if they are of nominal value and according to Gifts Register Policy.
- Subject to the guidance above and according to Gifts Register Policy, giving (or accepting) a gift certificate or gift card to a local restaurant or retailer is acceptable provided the certificate or card is modest in value and not ordinarily convertible to cash.

If there is any doubt about whether a Gift is of a nominal value or may otherwise be accepted, offered or given, we should seek guidance from our manager or to the Head of Compliance. For employees at the level of 2nd line management and above, where there is doubt whether or not the Gift is of nominal value or otherwise permitted, the matter should be referred to the Head of Compliance.

We should also bear in mind that there are some more stringent business segment or jurisdiction-specific laws, policies, procedures or guidelines regarding giving and receiving of Gifts, benefits or entertainment with which we must also comply if they apply to us.

Services by client banks offering sport and recreation, corporate kindergarten, favourable loan terms, voluntary supplementary pension fund or similar are considered employees' benefits and as such are not gifts nor subject to conflict of interest under this Article.

2.2.2. Alcohol and Substance Abuse

Company is committed to providing work and business environment that is free of alcohol and substance abuse. Accordingly:

- We will not consume alcoholic beverages during working hours in quantities that affect work performance or impair conduct or judgment (maximum 0,5 ‰);
- We will not consume, possess, sell or distribute illegal substances, especially while in or around Company premises (including buildings, parking lots, surrounding grounds and in Company owned or leased vehicles), at any Company function, or at any time when one could be identified as a Company employee; and.

As we are all responsible to maintain a healthy and safe workplace, we should take reasonable steps to prevent any co-worker, customer, supplier or other guest from driving while impaired/intoxicated.

2.2.3. Human Rights, Diversity, Inclusion and Preventing Violence in the Workplace

Company is committed to conducting all of its affairs with fairness and equity and fostering a unique and inclusive culture by providing a safe and respectful work environment that is free from harassment, discrimination, violence and other unacceptable behaviour as defined in the *Collective Agreements and respective local regulations*. In support of this commitment:

- Company will not condone, tolerate or ignore any harassment or discrimination on any ground protected by applicable law,
- Company will not condone, tolerate or ignore violence or threats of violence,
- Every employee, or person acting on behalf of Company, as well as every customer, supplier or other person in a business relationship with Company must be treated with dignity and respect,
- We must immediately report to Human Resources unit and/or Head of Compliance any harassing, discriminatory or violent conduct of which we are aware or suspect so that it may be properly addressed.

2.2.4. Use of the Internet, Email and Electronic and Social Media

When we use Company electronic communication devices, communicate over Company electronic networks or discuss Company subject matter, we must comply with Company's applicable policies on rules for the protection of information, company assets and for the use of e-mail, internet and web collaboration tools.

Company's expectations apply in this regard wherever we happen to be, whether in a Company workplace or not. Our communication should be respectful, responsible and professional in tone and must not violate the Code, or other applicable policies, including customer or employee privacy. For example, we must not knowingly transmit, view, generate, print, retrieve, download, display or store any communication or material of a discriminatory, defamatory, obscene, damaging (such as viruses), threatening or harassing nature, or any material that is inappropriate for the business environment (such as sexually oriented literature or pictures).

We must not use personal email accounts for business purposes, unless we are authorized to do so, we cannot use external social media channels to communicate for Company business purposes, or to otherwise publicly comment, post or speak on behalf of Company or disclose confidential, proprietary, restricted, internal or personal

information that is not publicly known. Company will not interpret this Code or policies in a way that prevents us from engaging in lawful communications which includes expressions of personal opinions.

2.2.5. Irregular Business Conduct

Irregular business conduct (which includes any criminal, fraudulent or illegal conduct, any impropriety or dishonesty) will not be tolerated under any circumstances. Such conduct may not only be subject to internal disciplinary action, but may also lead to criminal prosecution, regulatory action or civil suit. Some of the most serious types of violations are described below:

- Anti-Competitive Behaviour – Generally, an agreement or arrangement with a competitor to fix prices (e.g., to set interest rates, fees, prices, etc.), allocate markets or restrict supply could be illegal. As competition and anti-trust laws are very complex and vary by jurisdiction, we should seek guidance from the Legal Affairs unit or Compliance unit in any circumstance that might be perceived as anticompetitive.

- Bribery and Corruption – As a general rule, “anything of value” offered, promised or given to a recipient, directly or indirectly, in order to induce or reward the improper performance of, or the failure to perform, a function or an activity, can be considered a bribe. In all instances, whether an action will be considered a bribe will depend on whether it was presented for the wrong reasons. Bribes come in many forms and activity may be construed as illegal anytime there is the giving or receiving of an undue reward to influence another party’s behaviour. The Company prohibits us (or anyone acting on their behalf) from:

    - soliciting anything of value for themselves or for any other individual from anyone in return for any business, service or disclosure of confidential information; and

    - accepting anything of value from anyone other than Company in connection with conducting Company business, except as may specifically be permitted by the Code (see Gifts section above) or in other applicable policies. The Company’s prohibition extends to “facilitation” (or “grease”) payments when dealing in particular with public administrative services. Some specific examples of undue rewards that can constitute a bribe include cash, unactable gifts, business opportunities or contracts, employment or internships, travel, entertainment and other expenses. Bribery and corruption laws are complex and violations carry very significant penalties. Accordingly, if we should become aware of or suspect a violation of rules described above please seek guidance from the Legal Affairs unit or Compliance unit.

- Due Diligence –when we are responsible for due diligence processes before committing Company to a loan or other business transaction, we must exercise due care and follow business policies, practices and procedures in carrying out these activities.

- Forgery, Falsifying Accounts, Documents and Records – improperly creating or reproducing, or falsifying a signature or initial, or otherwise creating a false document will not be tolerated under any circumstances. In addition:

    - We must not manipulate internal accounts or make entries to any account which are false, have not been properly verified or obscure the true nature of the transaction, or allow such entries to be made. We must not establish or operate, for any purpose, an account on the books of the Company that cannot withstand the closest public scrutiny of its propriety. Also, we must not manipulate or falsify any Company financial statement, record or return.

    - We must not intentionally complete inaccurate reports, forms or other documents (including marketing and client presentation material) that are relied upon by the Company to be an accurate record of the circumstances, or that are disclosed publicly or directly to third parties, including government agencies, regulators and customers or potential customers.

- Insider Trading or Tipping – If we possess material, non-public information about Company or its customers, business partners or other third parties (e.g., with whom Company may be contemplating a purchase or sale) and we are prohibited from trading in securities of those entities ("Insider Trading"). We also may not communicate material, non-public information ("Tipping") to anyone except in accordance prescribed rules of the economic group to which the Company belongs. Information is material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision, or if it would reasonably be expected to affect the value of securities of a company. Examples of material information may include (but are not limited to):
    - A significant acquisition, sale of a business, merger or takeover bid;
    - A change in the general character or nature of a company;
    - Entering into or loss of significant contracts;
    - Bankruptcy, impending insolvency, or other financial problems;
    - Significant new business opportunities (e.g., discoveries, inventions, new orders or contracts), or the loss of business;
    - A change in a company's capital structure; or
    - Earnings information or information about a dividend declaration that is not available to the public.

  If we have any questions as to whether a particular piece of information is material and/or non-public we should contact Compliance or Legal Affairs /Company Secretary units prior to taking any action that may constitute insider trading or tipping.

- Money Laundering – Company is committed to taking all reasonable and appropriate steps to prevent persons engaged in money laundering from utilizing Company products or services to do so. Making the proceeds of criminal activity appear as if they came from legitimate sources is a criminal offence, and so is knowingly failing to report transactions or activities where there are reasonable grounds to suspect they relate to money laundering. We must not knowingly initiate or be party to money laundering, and must promptly report suspected money laundering situations in accordance to Company's Compliance unit.

- Sanctions – Company is committed to complying with economic and trade sanctions imposed against countries, governments, individuals and entities specified by the competent authorities in the jurisdictions where the Company operates. Company takes reasonable and appropriate steps to ensure Company products or services are not used to violate or circumvent applicable economic and trade sanctions laws as sanctions violations can result in civil and criminal liability for Company and certain employees. We must not knowingly initiate or be party to the circumvention or facilitation of activity prohibited or restricted by sanctions, and must promptly report suspected sanctions related situations or issues in accordance with the escalation procedures established for our business segment or region. For more information, refer to the Company's Compliance unit.

- Terrorist Financing – Company is committed to preventing the use of its financial services for terrorist financing purposes. We will not knowingly deal, directly or indirectly, with any person, entity or group subject to anti-terrorism measures or whom we believe or have reason to believe is involved in the financing of terrorist activities. We must report transactions or activities that we know or suspect relate to terrorist financing to Compliance unit and follow applicable procedures, if any, to allow for any appropriate action to be taken.

- Theft and Fraud – Defalcation, embezzlement, fraud, theft or misappropriation of funds or property belonging or entrusted to Company or others, is strictly prohibited and will not be tolerated.

2.2.6. Protecting Company Assets

We must make every effort to protect all Company property and information assets from theft, fraud, harm, loss or misuse, especially those that are in our custody or control and are our responsibility.

The Company requires us to act in a proactive and coordinated manner to prevent and detect potential financial crimes and fraud. If we become aware of or suspect any actual, potential or attempted theft, fraud, harm, loss or misuse of Company property or assets we must immediately notify our manager or other appropriate units (such as Information Security unit for security matter or data protection officer for personal data matter) in order to allow for any corrective action that is appropriate under the circumstances. Company property that is entrusted to us may be used only for the purpose of executing our accountabilities with the Company, except to the extent that non-business use is expressly permitted.

2.2.7. Company Brand

Care should be taken in the use of Company stationery (including forms, letterhead and envelopes), where the name, address or phone number of any Company, business segment or organisational unit appears on the fax, or emails (paper or electronic copies) where the @website is a Company website.

Incidental personal use of such material may be allowed where we make it clear in the communication that it is from us personally.

2.2.8. Copyrighted Material

We must only reproduce and use software, videos, music and other copyrighted material licensed for use by Company and in accordance with applicable copyright laws.

2.2.9. Company's card and business expense policy

We are required to follow the requirements set out in the Company's business expense policy, car usage policy and travel policy, which outlines the preventative and detective control measures along with expectations of our roles and responsibilities in implementing them.

We are also required to comply with the policies and procedures, including claiming only reasonable expenses actually incurred for Company business within Company guidelines and we are accountable to follow our authorization limits when we authorize expense commitments, transactions or employee claims for reimbursement.

In addition, we must not use a Company corporate credit card for any purpose other than for proper Company business expenses, and we must manage the card in accordance with applicable policies and procedures. In particular, use of a Company corporate credit card for personal charges (including cash advances) is strictly prohibited.

2.2.10. Criminal Record

We must inform our manager and/or Human Resources unit when charged with any criminal offence, and keep them informed on the related outcomes of such processes.

There may be employment consequences if an employee is charged with or found guilty of an offence, or pleads guilty or no contest to an offence relating to the employees' job description.

Minor motor vehicle-related offences of a less serious type of misdemeanour (e.g. speeding) do not have to be reported to Company. If you are not sure whether a charge, guilty finding or plea should be reported, employees should discuss the situation with your manager or Human Resources unit. Heads of first line units should discuss the situation with Head of Compliance unit.

2.2.11. Cooperating with Audits and Investigations

We are required to fully cooperate with any investigation whether including actions from Internal Audit, Compliance, Information Security, Legal Affairs, and Human Resources units and any other areas of Company which may, from time to time, audit or investigate issues within Company. Further, we must not in any way obstruct, hinder or delay any internal investigation. The obligation to cooperate may extend to providing truthful information pursuant to, or in the defence or prosecution of, legal proceedings and investigations involving the Company, its customers or employees.

We must respond to all sensible requests (via email or other) from our colleagues and employees in reasonable timely and with respectful, responsible and professional in tone.

2.2.12. Managing Conflicts of Interest

2.2.12.1. Introduction to Conflicts of Interest

In keeping with expectations regarding ethical corporate conduct, customers and the public have a right to openness and honesty in all their dealings with the Company.

In keeping with culture of openness, trust and integrity with any of the Company's partners, and as representatives of Company, we must avoid activities or circumstances that create conflicts between our personal interests and our responsibilities as employees or managers. This means that we have to comply with the following policies and procedures that manage potential conflicts between Company's interests and those of other stakeholders, such as customers and counterparties:

- conflicts of interest arise when individuals or organizations have personal interests that may interfere with, or appear to interfere with, the independent exercise of judgment in business dealings;
- we must avoid having our decisions on behalf of Company influenced (or to even be seen to be influenced by) conflicting interests. For these reasons, actual, potential and perceived conflicts of interest (each a "Conflict" and collectively described as "Conflicts" in this section) must be carefully managed.

The following Conflict of interest sub-sections describe many of the more commonly encountered Conflicts, but we must always be alert to other situations that may give rise to Conflicts. In any situation where there is a Conflict, we must bring the situation to the attention of our manager, Human Resources unit or other contact listed in this Code.

For purposes of this section, "relatives and people with whom we share a financial or close personal relationship" include for example, a spouse, domestic partner, party to a civil union, others with whom we share a romantic relationship, parent, child, grandchild, grandparent, sibling, guardian, roommate, business partner, co-investor, guarantor, etc., but do not include nominal financial relationships.

2.2.12.2. Conflicts Arising from Personal Benefit

A Conflict may arise where we may be motivated to act in a manner that is not in the best interests of Company, our customers and/or our shareholders. Often this is because we, or our relatives or people with whom we share a financial or close personal relationship, stand to benefit from the action in some way.

We must avoid acting in a manner that places our personal interests ahead of the best interests of Company, Company's customers and/or Company's shareholders. As noted above, we must also avoid situations that might create the appearance of a conflict of interest whether or not it actually exists and whether or not we believe we would be improperly influenced. Where we face a potential conflict, we must disclose the situation to our manager or Head of Human Resources.

2.2.12.3. Corporate Opportunities

We must not use Company property or information, or information concerning Company's employees, customers, prospective customers, suppliers or agents, including, for example, their accounts, transactions, or other financial, business or credit information, our position at Company, or our access to, or knowledge of Company systems, policies or assets:

- for personal gain, or the gain of our relatives and people with whom we share a financial or close personal relationship;
- to compete with Company; or
- to take advantage of opportunities that are discovered in the course of conducting Company business.

We are expected to advance the legitimate interests of the Company whenever the opportunity arises. Great care must be taken to avoid any Conflict when purchasing or selling assets or services from or to the Company, its customers or its suppliers.

In specific cases, however, a personal opportunity may be approved if it is disclosed in advance and in writing to Head of Human Resources (or, in the case of the Chief Executive Officer or a director, to the Head of Compliance) and is determined not to be material. In case of Head of Compliance, such personal opportunity may be approved provided by the Management Board.

2.2.12.4. Relationships in the Workplace

We must not give or receive any special consideration relating to employment or conditions of employment to or from relatives and people with whom we share a financial or close personal relationship. Our business and human resources decisions must be based on sound ethical business and management practices, and not influenced by personal concerns.

Relatives and people with whom we share a financial or close personal relationship may not work in positions where there is an actual or potential conflict of interest. For example:

- Where the job positions serve as controls for each other;
- where there is a direct reporting relationship between them;
- or where either one has the authority to influence, directly or indirectly, any term or condition of employment of the other,

will be avoided, unless the situation has been disclosed to the organisational unit manager and to the Head of Human Resources and their approval has been obtained.

In case of heads of first line units, they should disclose such a situation to the Chief Executive Officer or to Head of Compliance (and if it is the Chief Executive Officer, he/she should disclose the situation to Head of Compliance). In case of Head of Compliance, such disclosure should be provided to the Management Board.

If such a Conflict exists, one of the parties may be relocated to another organisational unit, which does not give raise to conflict of interest.

2.2.12.5. Disclosing Interest and Abstaining from Participation

To avoid any actual, potential or perceived conflict of interest, we must disclose any interest we have in an existing or proposed material contract or transaction involving the Company in which we may have some influence or perceived interest. If we are an officer or director of an entity that is party to any such contract, that relationship must also be disclosed. These disclosures must be made to our manager at the earliest opportunity (or, in the case

of the Chief Executive Officer or a director, to the Head of Compliance Director). In case of Head of Compliance, such disclosure is provided to the Management Board.

In addition, we must not have or be reasonably perceived to have influenced a decision with respect to a material or proposed material contract in which we have an interest described above.

2.2.12.6. Directorships, Outside Business Activities and Investments

We may not enter into any employment, directorship, office, trade, volunteer activity or business outside of Company or invest in a company (other than an interest of less than 10% of a publicly traded corporation) that competes with the company without obtaining a prior consent from the Company.

As a general principle, outside business activities should not interfere with the performance of our duties at the Company or our ability to exercise judgment in Company's best interests.

The Chief Executive Officer, head of first- line organisational unit and any other members of the senior executive team must also obtain the consent of the Company.

2.2.12.7. Political and Charitable Activity

As employees and managers, we may make personal political contributions and charitable donations at our discretion, subject to ensuring that there is no regulatory prohibition or reporting restriction on such contributions. However, we must not commit the Company to charitable contribution without prior approval from Marketing unit. We must not commit or make political contributions on behalf of Company.

We should not engage in any political activity in the workplace. If we are soliciting financial or other donations on behalf of charities we should exercise discretion in soliciting donations from co-workers, customers and suppliers (i.e. they should never be made to feel any obligation to make a donation) and must comply with any applicable Company policies. We must not use email group lists for purposes of requesting donations without approval from the responsible head of organisational unit.

2.2.12.8. Conflicting Company Interests

Company is committed to avoiding material Conflicts between its interests and those of its customers and counterparties. A material Conflict would exist if the Company were to engage in any transaction or activity that could involve or result in Company's interests being materially opposing to the interests of a customer or counterparty.

If required, Company will establish, maintain and enforce information barriers to physically separate employees or functions, or limitations on types of activity, to help prevent Conflicts from involving or resulting in a materially adverse effect on a customer or counterparty.

If, regardless to the information barriers established, we know or should reasonably know that a specific transaction or activity may involve a Conflict that could result in a materially adverse effect on a customer or counterparty, we must discuss the situation with our manager and/or our Head of Compliance representative and assess whether disclosure of the Conflict to the customer or counterparty is necessary or appropriate. If so, we must ensure that (i) we make clear, timely, and effective disclosure of the Conflict and (ii) the customer or counterparty has the opportunity to negate, or substantially mitigate, any materially adverse effect created by the Conflict.

2.2.13. Protecting Classified Information

We may have access to confidential (non-public) information concerning the Company, its customers, suppliers, regulators or our fellow employees. We have an obligation to comply with applicable laws and our internal policies

and procedures of our business segment and region pertaining to classified information as prescribed in Company's Information Security Classification Model Rulebook.

We are all responsible to safeguard such information in our possession from unprotected access or disclosure. If or when it is necessary for us to take, send or work on classified information outside of Company premises or systems, including when we are working from a non-Company location, we must ensure it is appropriately protected and classified, regardless of whether the information is in physical or electronic form.

We may have had access to the confidential and proprietary information of past employers during employment prior to joining the Company. We must never use or disclose any of these information to anyone, including employees, customers or vendors, as part of, or during, our employment with Company. If we become aware of or suspect any violation of this obligation, we should immediately report it to our manager.

2.2.13.1. Protecting Client Information and Personal Data

Customer information and personal data must be kept private and confidential according to internal policies which in more detail prescribe such procedures.

We must not leave customer information and personal data unattended and we must not discuss or disclose any customer information (including that an individual or institution is a customer of Company) to anyone outside of the Company unless we are required to disclose by law, are authorized to disclose by the customer, or are directed to disclose in circumstances described in policies and procedures applicable to our business segment.

We must not access customer information and personal data except in the normal course of our duties, for a legitimate purpose and with proper authorization or consent. In addition, we must not disclose or share customer information with other Company employees who do not have a legitimate need to know the information and who do not have the appropriate clearance. When dealing with customer information and personal data, we must comply with all laws as well according to internal policies which in more detail prescribe such procedures.

2.2.13.2. Protecting Employee Information

Company is permitted to collect, use and disclose employee personal data for employment administration purposes in accordance with Collective Agreement and based on legitimate interest pursued by the Company as based on applicable laws.

We must exercise care and discretion with the personal data and information of other employees in our possession and never leave it unprotected and as prescribed in relevant privacy and personal data protection policies. We must never discuss or disclose it to anyone outside of Company unless for a legitimate purpose and we are permitted or required to disclose by law, are authorized to disclose by the employee, or are permitted to disclose in circumstances described in the policies and procedures applicable to our business segment. We must not disclose or share another employee's personal data or information with other Company employees who do not have a legitimate need to know the information unless we are authorized to do so based on applicable laws.

2.2.13.3. Protecting Company Information

We must carefully protect the classified and proprietary Company information to which we have access, and not disclose it to anyone outside of Company or use it without proper authorization, and then only for the proper performance of our duties. We must also avoid discussing or disclosing it to other Company employees who do not have a legitimate need to know the information.

2.2.13.4. Computer Systems Security

When using Company computer systems and accessing Company information, we must be properly authenticated at all times according to internal policies which in more detail prescribed Company's internal acts. It is our responsibility to take the necessary steps to protect our logon ID, passwords, digital signature or other means we use to identify ourselves to the Company computer network and to otherwise protect Company computer systems from unauthorized access (including ensuring that our computers are always locked when we leave them unattended).

This also applies to access given to third parties or agents through any shared system or direct access to Company systems. We must also exercise vigilance in protecting Company systems against computer viruses. As employees, we must comply with internal policies which in more detail prescribe such procedures including the obligation to be alert to, and to take reasonable steps to prevent potential security threats to ourselves, other employees, Company assets and property, and to report any, even potential, security and personal data incidents.

All computer hardware, software, email, voicemail and internet accounts provided to employees are the property of Company and may be monitored, recorded and accessed by authorized Company representatives in accordance with mentioned security policies and rulebooks and applicable law.

In addition, all information stored, processed or transmitted on any Company system, network, equipment or device or external system used by Company to conduct business, is considered the property of the Company.

2.2.14. Disclosure of Company Information

The Company is committed to providing timely, accurate and balanced disclosure of all material information about the Company, and is also committed to transparency in its reporting obligations to shareholders, authorized supervisory authorities and the public. All of us, as employees, officers, managers and directors of the Company are required to comply with legitimate and lawful requests or disclosure from such stakeholders.

2.3. Work Environment

2.3.1. Appearance and Courtesy

To customers and prospective customers, our individual employees with whom they come in direct contact represent the Company. Therefore, our choice of work attire should be guided by what is appropriate when meeting our customers and based to the degree of direct contact with customers.

Our work environment for employees encourages us to dress comfortably for work. Nevertheless, we must not wear anything that other employees might find offensive or that might make co-workers uncomfortable. This includes clothing with profane language statements or clothing that promotes causes that include, but are not limited to, politics, religion, sexuality, race, age, gender, and ethnicity. Inappropriate work attire includes also shorts, flip-flops or training clothes as well as any revealing clothes.

Work attire must be neat and clean, having due regard to personal hygiene and grooming. We must also be courteous and respectful in all dealings with the public and other employees and in all other business relationships. The Company expects that our business attire, although casual, will exhibit common sense and professionalism. We are expected to demonstrate good judgment and professional taste.

2.3.2. Health and Safety

Under Company's health and safety program, we share the responsibility of maintaining a healthy, safe and respectful work environment. We are all expected to observe the established health and safety policies, regulations and practices applicable to our business segments and regions and report accidents, injuries and unsafe equipment, substances, practices or conditions.

Employees who have specific accountabilities under health and safety legislation (e.g. health and safety representatives, etc.) are required, and the Company will endorse them, to acquire the necessary training, understand their additional responsibilities and act on them to protect the health and safety of individuals within the workplace as requested and organized by the Company.

In addition, we are all responsible to ensure our own safety while travelling for business purposes. When we are planning business travel we are required to use Company's corporate travel policies so that the Company can monitor and advise us of potential security issues, and also support us (e.g., getting us home safely) should an emergency arise.

2.3.3. Physical Security

The Company has developed a set of rules and conducts (such as the Visitor Code of Conduct) to help fulfil its commitment to protect employees and assets, while mitigating the risk resulting from various security threats. We are all expected to be alert to, and to take reasonable steps to prevent potential physical security threats to ourselves, other employees, Company premises and property, and to report security incidents according to prescribe in more detail prescribe such procedures.

2.3.4. Reporting Violations

Where we are aware of or suspect any conduct that violates the Code (or related policies or internal acts, supplemental, compliance manuals, other duties owed toward the Company, etc.) we have an obligation to report such conduct using any available channels:

- In any case, reports of cases of non-compliance with this Code can be sent by email to compliance.CEE(at)nexigroup.com.
- We may also report violations to our manager or Head of Human Resources
- The Company guarantees that whoever reports a case of non-compliance in good faith will be protected from any form of retaliation, discrimination or penalisation, and ensures maximum confidentiality, based on the Whistle-blower principle, except in cases otherwise indicated by law.
- If we are not comfortable with these channels, we may choose to report the violation to any executive officer of the Company.
- We may also choose to instead report the violation through other means available to us, including but not limited to the employee complaint, anonymous drop boxes, or other escalation process in our business or location.

It must be noted that nothing in this Section, the Code or any Company policy prohibits, or is intended to prohibit, us from exercising our lawful rights to communicate with or report violations of law or regulations to an appropriate government authority.

If circumstances exist where reporting a matter internally would impede our ability to report the matter to or communicate with an appropriate government authority, then we are not obligated to report the matter internally.

The Company prohibits retaliation against employees because they exercise their obligation to report internally or their legal right to report to or communicate with an appropriate government authority.

2.3.5. Protection Company Reputation

All of us, either as employees, officers, managers or directors of the Company, in every location, every job, at every level, and at all times, is responsible to safeguard the reputation of Company, including by complying with this Code.

2.3.6. Failure to Comply

It is our responsibility to be familiar with and understand the provisions of this Code as well as other applicable and valid Company policies (i.e. internal acts), including those specifically identified in this Code and that have been published on the Intranet under “Registry of Internal Acts”.

Failure of an employee or a manager/director to comply with the Code or any other applicable policy may result in disciplinary action in accordance with respective rules.

2.3.7. Waivers

In certain limited situations, Company may waive the application of sections of the Code.

For employees (other than heads of first line organisational units), any such waiver requires the express approval of the Head of Compliance and the Head of Human Resources. For executive officers and directors (heads of first line organisational units), any such waiver requires the express approval of the Management Board of the Company.

3. FINAL PROVISIONS

3.1. Implementation of the Code in connection with other internal acts and applicable laws

We must also comply with local laws and regulations, as well as our responsibilities to professional associations, self-regulatory organizations or regulators where these may impose greater or more rigorous standards than provided for in the Code or Company’s internal acts.

In the event of an apparent conflict between the provisions of this Code and local laws and regulations or with other internal acts, we must seek guidance from our manager and/or head of Compliance. Within this framework, employees and managers are expected to exercise good judgment and be accountable for their actions.

3.2. Review and Update of this Code

The Code will be reviewed and updated periodically in order to keep it current and reflective of emerging laws, regulations, policies and best practices.