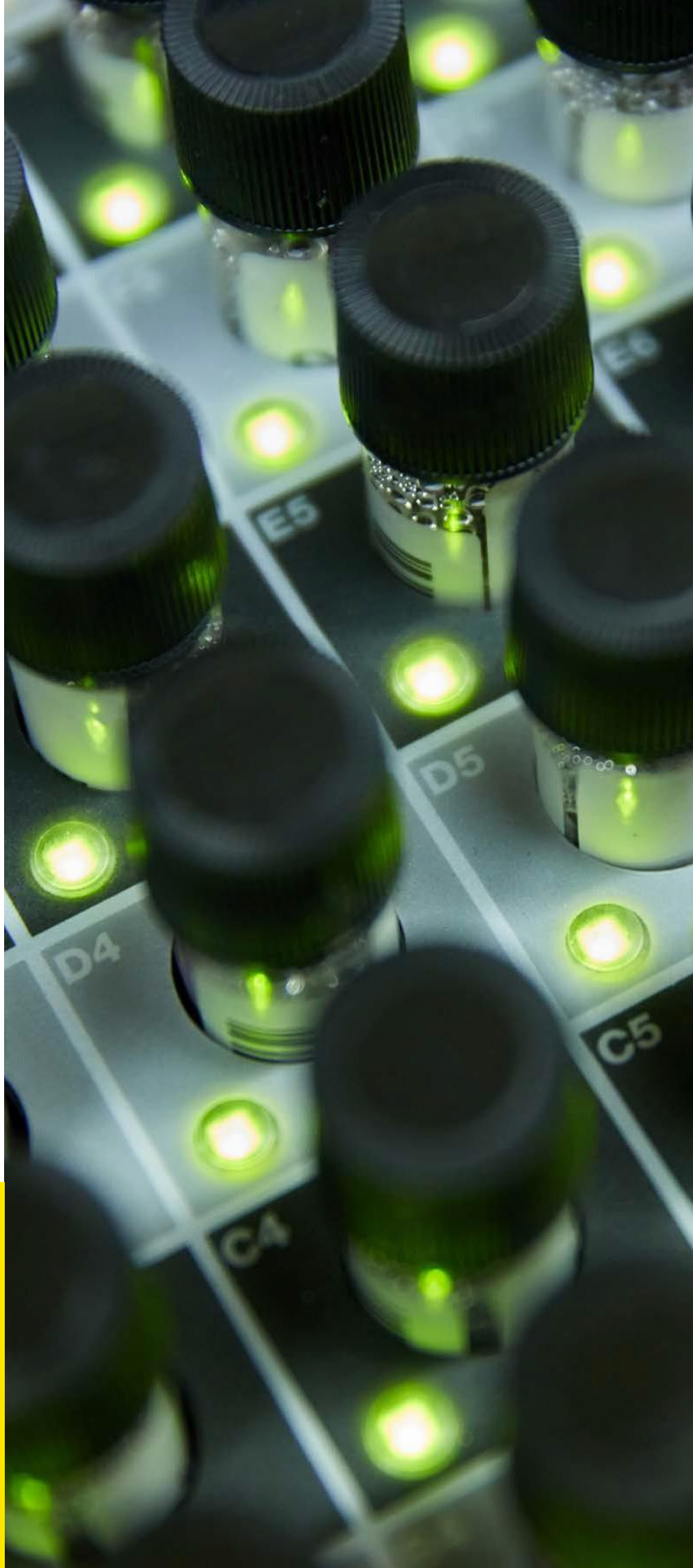


NEIKER

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

CODE OF ETHICS

neiker.eus



HISTORY OF CHANGES

Edittio n	Chapter	Reason	Date
1	All	Initial edition (approved by General Management)	2017/12/19
2	All	Review with employees and Works Committee. Approval by Neiker Board of Directors.	2018/12/19
3	All	NEIKER logo and general review including the confidentiality and information security policy and in inclusive language.	2022/01/26
4	II. LINES OF COMMUNICATION Treatment of communications received III. AVOIDING CONFLICTS OF IMPARTIALITY V. EXCELLENCE IN RESEARCH VII. ANTI-BRIBERY AND ANTICORRUPTION VIII. ACCURACY AND TRUTHFULNESS OF RECORDS X. PROTECTION AND APPROPRIATE USE OF COMPANY ASSETS	Replaced the R. compliance with the Internal Information System of the Basque Government (BIS). The Compliance Committee is included, and "company" is eliminated Eliminated Removed reference to R. compliance Reference to artificial intelligence Removed reference to R. compliance Replaced the R. compliance with the Internal Information System Reference to artificial intelligence	2024/06/30

Drawn up by: G. Management
Approvals: Board of Directors.

CONTENTS

EXPLANATORY MEMORANDUM	5
I. GENERAL PRINCIPLES FOR ACTION	7
1. Who the Code applies to	7
2. Infringements of the Code	8
3. Obligation to report	8
II. LINES OF COMMUNICATION	9
III. AVOIDING CONFLICTS OF IMPARTIALITY	10
1. What we understand by conflicts of impartiality	10
2. Incompatibilities	10
3. Gifts, presents and other courtesies	11
IV. PEOPLE AT WORK	12
V. EXCELLENCE IN RESEARCH	14
VI. APPROPRIATE RELATIONS PRACTICES	16
1. Relations with clients, suppliers, partners and employees	16
2. Relations with competitors	16
VII. ANTI-BRIBERY AND ANTI-CORRUPTION RULES	17
1. Corruption and/or bribery behaviours	17
2. Political activity	17
VIII. ACCURACY AND TRUTHFULNESS OF RECORDS	18
IX. PREVENTION OF MONEY LAUNDERING AND FINANCE FOR TERRORISM	20
X. PROTECTION AND APPROPRIATE USE OF COMPANY ASSETS	21
1. Electronic resources	22
2. Intellectual property	26
3. Confidentiality and security of information	27
XI. COMMUNICATIONS	31
1. Internal communications	31
2. External communications	31



EXPLANATORY MEMORANDUM

NEIKER personnel, due to our status as "public employees", have a series of responsibilities and obligations to the authorities on which we depend and to society, arising from the public services we provide. Moreover, as a Basque Government Public Company, our actions are subject to the principles of equality, legality, service to the general interest, efficiency, stability and transparency.

The Code of Ethics provides specific guidelines for behaviour and criteria for interpretation to **ensure that all employees, clients, suppliers and so on know how to act at all times in the course of our activities, and who to consult** about our doubts or report what might appear to be unethical, improper or illegal behaviour.

This set of commitments is in line with the Basque public sector transparency, public participation and good governance act, and is inspired by the principles set down in articles 52, 53, 54, 55 and 59 of the Basic Statute for Public Employees, in the incompatibilities of staff at the service of the public administrations act and in the NEIKER Collective Agreement, which is to apply in all disciplinary matters.

Moreover, from a business point of view it is vital for us to be able to identify risks to information security and deal with threats to information systems efficiently, not only to guarantee a fundamental right [the privacy of personal data] but also to create trust and security among our clients in the processing and protection of any organisation's greatest asset: information.



I. GENERAL PRINCIPLES FOR ACTION

We act in accordance with the following principles: objectivity, integrity, neutrality, responsibility, impartiality, confidentiality, dedication to public service, transparency, exemplarity, austerity, accessibility, efficiency, honesty, care for the cultural and natural environment and respect between women and men.

- **Integrity means rigorously obeying the law and the contents of this code, and the avoidance of any real or potential conflict of interest.**
- **We provide transparent, rigorous and reliable information to foster mutual confidence and respect between parties, avoiding any kind of deception or action aimed at distorting the facts, especially with the pertinent authorities.**
- **We extend this commitment to all areas of our activity: to employees, clients, suppliers, contractors and also society in general, always in accordance with the principles of current regulations.**

1. Who the Code applies to

To everybody at **NEIKER** and those affected by its management (suppliers, contractors, etc.).

- Ethical behaviour is an individual responsibility that affects all of us.
- *The obligations of confidentiality and secrecy laid down in this document continue to apply even after a person stops working for us.*
- Furthermore, the senior managers who make up the board of directors and general management of NEIKER are subject to the system laid down in Resolution 67/2016 approving the rewritten text of the Code of Ethics and Conduct for public employees in the Basque autonomous community and its public sector.

2. Infringements of the Code

Any infringement of our Code, and of the policies and procedures arising from it may give rise to the disciplinary measures included in the **NEIKER** Collective Agreement.

- If an infraction of the Code includes the **breaking of the law, the matter will be assessed**, and if there are rational grounds for criminal charges, the practices in question must cease and be reported to the competent authorities.
- Any infringement of the obligations of secrecy and confidentiality may lead to the opening of disciplinary proceedings or even civil and/or criminal liability if the behaviour of the employee was attributable to serious bad faith, deceit or negligence on their part, as they might constitute the offences of revelation of secrets [art. 197 to 200 of the Criminal Code], computer damage [art. 264 of the Criminal Code] or revelation of company secrets [art. 278 to 280 of the Criminal Code].

3. Obligation to report

We are all responsible for ensuring this Code is followed.

- We all have the **duty and the responsibility to report in good faith on any possible risks and any real or apparent infringements of the applicable rules as laid down in our Code, using any of the lines of communication described herein.**

II. LINES OF COMMUNICATION

- We can consult the person who best understands our functions and responsibilities, i.e. **our immediate superior**.
- We can also speak to the **head of our department**, or to **human resources management**, or to compliance committee.
- Alternatively, **we can approach the Basque Government Internal Information system (BIS)**

1. Treatment of communications received

Confidentiality

- All communications will be treated according to a **strict protocol of confidentiality** to avoid revealing the identity of the person making use of the lines of communication.
- It is advisable that the informant identify themselves in order to follow up their report and give a response when investigation allows it.
- However, it is warned that is an infringement of the Code to knowingly make a false accusation, lie to investigators or refuse to cooperate with an investigation related to the Code.

What happens when a report is received?

- The informant is contacted (if they have identified themselves) to make sure all the information is recorded.
- If it is a doubt or a suggestion, it will be considered and answered as soon as possible.
- If it is a report of an infringement, a secure investigatory procedure will be triggered, and the informant will be notified of its conclusion.
- A transparent, accurate record of all communications received and the actions taken as a result will be kept.

III. AVOIDING CONFLICTS OF IMPARTIALITY

1. What we understand by conflicts of impartiality

A conflict of impartiality occurs when a person's work, personal, professional, family or business interest **might** affect or **appear** to affect the impartial, objective performance of their work functions.

In this situation you must:

- Before taking a decision, inform Resources Management in writing of the circumstances that might stop you taking independent action. Resources Management will tell you what to do about it.

2. Incompatibilities

People who work at NEIKER are subject to the system of incompatibilities laid down in Law 53/1984 of 26th December 1984. Furthermore, the senior managers who make up the board of directors and general management of NEIKER are subject to the system laid down in Law 1/2014 of 26th June 2014 governing the code of conduct and conflicts of interest of public employees.

In general terms, providing services in NEIKER is **not compatible** with any other employment or professional activities outside it, whether in the public or the private sector, which might hinder or prejudice strict compliance with NEIKER duties, or

Am I facing a conflict of impartiality? Ask yourself:

- Could my personal interests interfere with those of the company?
- Could it appear this way to others, whether within or outside the company?

Who is my "family member" according to the Code?

- Spouse, partner, parent, sibling, grandparent, son or daughter, nephew or niece, parent in law.
- Any other family member who lives with or depends financially on you (directly or indirectly).
- Even when negotiating with family members outside this definition, care must be taken to make sure the relationship does not interfere - or appear to interfere - with the action taken within NEIKER.

which might compromise a person's impartiality or independence, with the exceptions stipulated by law.

In any case, employees wishing to combine their work at **NEIKER** with some other activity must request written authorisation by Resources Management.

3. Gifts, presents and other courtesies

- If you are offered a gift, a meal or any other kind of courtesy of a significant monetary value, i.e. not with a merely symbolic value, you must **politely decline it, explaining the company rules**. If returning it might offend the giver or the circumstances in which it was given prevent its return, it is to be handed over to Resources Management, who **will decide the best option**, for example giving the item to charity or distributing or raffling it among the workforce.
- When you are offered gifts and other courtesies whose monetary value is negligible or symbolic, a category including those of a promotional and advertising nature, Resources Management must be informed and will give the pertinent instructions.
- The offer, or promise, directly or indirectly, of any kind of improper advantage is absolutely prohibited, as is influence peddling.



IV. PEOPLE AT WORK

We offer **fair, decent working conditions** and support **professional and personal development** for all employees, displaying respect for people and **not tolerating any situations of discrimination, harassment, intimidation or violence.**

- The fundamental values that determine NEIKER's relations with its workforce are: **fair treatment, mutual respect, tolerance, cordiality** and solidarity, generating **safe working environments** in which diversity, equal opportunities and professional development flourish.
- On the basis of this commitment, **we insist that our suppliers and partner companies** respect and abide by current legality.
- NEIKER personnel must always work for gender equality and non-discrimination, and pursue equality policies that cut across all their activities.
- In the area of sexual or gender-based harassment, action must be in accordance with the stipulations of the *protocol for the prevention of and action against sexual harassment, harassment for reasons of gender and harassment related to gender identity and expression*.

Prohibited behaviour

- Degrading comments, jokes, statements or threats of an aggressive, insulting or humiliating nature, or related to people's way of dressing, sexual orientation, race, culture or religion.
- Using abusive, threatening or offensive language.
- Unjustifiably withholding information crucial to the performance of a job or manipulating it to cause error and then accuse a person of professional incompetence or ineptitude.
- Blocking the development of a person's career by hindering internal promotion or training in any way.
- Impeding the taking of a personal decision or initiative that is part of another person's responsibilities.
- Repeated, serious examples of the above behaviour in order to cause a person to leave or be absent.
- Inducing or encouraging others to engage in any of the above prohibited behaviours.

Discrimination

- This happens when a person or group of people are treated differently or negatively because of their personal features, beliefs or any other reason prohibited by law, including nationality or ethnic origin, culture, religion, political convictions and action, whether associative or trade union, age, language, physical or mental disability, gender or sexual orientation.

- Employees must not be under the effects of drugs or alcohol while doing their job. Furthermore, the consumption, sale, purchase or possession of alcoholic drinks and/or illegal drugs at work are strictly prohibited. The consumption of alcoholic drinks will only be allowed at occasional celebrations, but always in accordance with local laws in force at any given time.



V. EXCELLENCE IN RESEARCH

As a leading research centre, we pursue scientific excellence with honesty, transparency and responsibility at all times and in all places.

1. We work to **innovate for the common good and general interest**, our ultimate goal being to foster the social and economic well-being of Basque society, in line with the strategic plans in place.
2. Our **research activity is governed by principles of ethics and integrity**, which mean efficient, sustainable and rigorous use and administration of the infrastructures, costs, energy resources and financial resources assigned to each project. When artificial intelligence is used as an assistance tool for research, researchers will be responsible for verifying the accuracy and truthfulness of the results
3. Our **research is conducted to the highest standards of quality**, transparency of data and bibliography, with original, relevant work, verifiable throughout the research process to ensure the usefulness of the knowledge gained, its reproducibility and the potential development of future ideas.
4. We ensure that the **people** who take part in our research **are not exposed to unnecessary risks** and have the training necessary to avoid them.
5. In accordance with all regulations and standards of the care and **welfare of the animals** used in our projects.

Examples of actions incompatible with excellent research:

- Premeditatedly false assessment of projects [costs, purpose or results].
- Abusive interpretation of data.
- Falsification of data or evidence to fit the hypothesis.
- Fabrication of data and discoveries.
- Plagiarism of others' work.
- Misappropriation or exclusion of the identity of other scientists in research or bibliographical quotes.
- Repeated publishing of research, simulating novelty or innovation.
- Failure to abide by the procedures and good practices laid down for the research process.
- Failure to abide by auditing procedures or simulating them.
- Neglecting the training of future researchers.
- Assigning simulated or non-existent costs and/or resources to a particular project.
- Exploiting resources, information or results for personal interests.
- Failure to notify or report any of the above situations.

In case of doubt, we always consult our immediate superior.

6. We foster **respect for ethical standards in research**, based on good practices and applicable legislation, on actively avoiding any conflicts of interests, and on respect for the scientific freedom of our staff to express themselves on ethical matters and report the misuse or abuse of scientific or technological advances. **The use of artificial intelligence must comply with current privacy and data protection legislation.**
7. Ethics and responsibility extend to our **commitments in the field of information transfer**, both in the responsibility assumed for educating and training future research staff and in the publication and dissemination of reliable, proven results among the scientific community, and among the economic sectors with which we work.



VI. APPROPRIATE RELATIONS PRACTICES

We abide fully by applicable regulations in all our relations.

1. Relations with clients, suppliers, partners and employees

- We will always negotiate in good faith with clients, suppliers and partner companies, treating them honestly and respectfully and presenting our services clearly and directly.
- **NEIKER has supplier and provider selection processes in accordance with the law, with criteria of openness, competition, transparency, objectivity, impartiality, confidentiality, non-discrimination, quality and cost, prohibiting any conflict of interests or favouritism in selection.**

2. Relations with competitors

- **NEIKER competes fairly and complies with competition laws on a legal, ethical basis.**
- **In all cases we respect information not in the public domain concerning other companies, bodies or research centres, as well as third-party commitments to confidentiality.**

Guidelines for behaviour:

- We must not involve ourselves in any activity that might be reasonably perceived as impeding free competition, or which is abusive or unfair.
- We must not attempt to obtain information about the competition by means of illegal practices (industrial espionage, bribery, theft, electronic espionage, etc.).
- We must refrain from making false or misleading statements about our competitors or their services.

What are permissible sources of information?

- Publicly-available presentations by governmental bodies
- Public speeches by company executives.
- Annual reports.
- News, articles and publications in specialist periodicals.

In case of doubt, we always consult our immediate superior.

VII. ANTI-BRIBERY AND ANTI-CORRUPTION

NEIKER strictly prohibits all forms of bribery and corruption.

1. Corruption and/or bribery behaviours

- **NEIKER** rejects any form of corruption or bribery, whether in the public or the private sector, and must use all its means to investigate any indication of bribery by a third party directly or by an outside agent acting on behalf of the company.

2. Political activity

- **NEIKER** respects everybody's freedom of ideology. Staff may take part in political activities on their own behalf, providing they do not make use of company time, funds, property, resources or assets, or solicit political contributions by other employees **while working**.
- **NEIKER** acts in accordance with the principle of democratic neutrality at all times.

Anti-bribery alerts

– The following might be considered to be a bribe:

1. An unusual increase in a commission by an agent or consultant..
2. A contract to provide services or intermediation to gain a project:
 - May cover up a bribe or an improper diversion of public funds, especially if the service provided and the proportionality of its price cannot be proven.

– In such cases:

- No payments must be made until the company has investigated the concerns.

Political activity

- Do not make any comments on political positions on behalf of the company.
- Do not use your position in the company to seek to influence people to make donations of a political nature or support a specific party or politician, or use its assets and means for these purposes.

VIII. ACCURACY AND TRUTHFULNESS OF RECORDS

Accurate, complete and reliable records are essential to our company, as they form the basis of decision-making and strategic planning, and provide complete, truthful information for all our interest groups.

- All company records must be complete, accurate and reliable, drawn up in accordance with applicable laws and regulations, as well as the company's standard operating policies and procedures.
- All contracts and payments made on behalf of the company must be with the pertinent prior authorisation.
- **We do not use NEIKER funds or other assets for illicit or improper purposes of any kind, or false or misleading entries or unrecorded bank accounts, whether in connection with sales, purchasing or any other activity, or improper or unusual financial arrangements with third parties, such as for example over- and under-billing.**
- We always seek the best option when spending company money.
- We conduct all transactions with the level of responsibility required by our standard operating policies and procedures and in accordance with applicable laws, rules, standards and regulations.
- **We record and classify transactions accurately, in the appropriate accounting period and in the correct account and department.**

Mistakes made in good faith

- We must set out to be accurate when preparing information for the company, but unintentional errors may occasionally arise.
- Only intentional efforts to falsify or incorrectly record transactions or falsify company accounting records in any other way will be considered as infringements.

Basic behaviour

- Using funds received legitimately, without misuse of any kind (including in maintenance and refundable expenses).
- Following company guidelines and procedures rigorously.
- Always being honest, exact and precise in recording information (financial data, invoices, payrolls, curriculum vitae, records of hours worked, expenses, receipts and so on).

Prohibited behaviour

Record of income

- Simulating a contract to achieve the goal of the contract, cancelling it afterwards, falsifying financial records.

- **We neither delay nor advance the recording of income or expenses** to fit in with budget goals.
- We ensure that all documents, declarations and/or reports sent to the regulatory authorities are complete, reasonable, accurate, relevant and understandable.
- We ensure that, to the best of our knowledge, all documents issued and signed by us are accurate and truthful. We do not falsify documents.
- **We do not distort the real nature of a transaction, or conceal assets, liabilities or other financial information about people or companies that in fact provide goods or services.**
- **We restrict access to delicate or confidential information to ensure that it is not divulged, altered, misused or destroyed, whether accidentally or intentionally.**
- **We inform Financial Management immediately** of any unrecorded fund or asset and suspicious, false or fictitious accounting entries in our books and records, or any other irregularity, **and to the Basque Government internal information system (BIS) if the issue is not settled in a satisfactory way.**

Recording expenses

- Not recording and accounting on time for invoices received and so delaying recognition of the debt and payment deadline.
- Issuing pro-forma invoices not justified by the provision of a service.
- Refunding expenses not connected to professional activities or contravening rules and limits.

Defrauding public authorities

- Falsifying the conditions required to obtain subsidies, reductions or assistance from the authorities.
- Obtaining and having undue benefits, deductions or refunds from the tax or social security authorities.
- Obtaining social security benefits on your own behalf or that of a third party through error or twisting of facts or by deliberately concealing facts that should be reported, so harming the authorities.



IX. PREVENTION OF MONEY LAUNDERING AND FINANCE FOR TERRORISM

Money laundering is the method whereby funds obtained or generated through an illegal activity are covered up by infiltrating them into the legal circuit of business and finance to conceal their origin.

- Money laundering is a **global problem** with devastating economic and social consequences. While there are still legislative differences between different jurisdictions, we must **act diligently** to avoid **NEIKER** becoming involved or implicated in money laundering activities or other illegal activities. For these reasons:
 - We must apply the appropriate level of **due diligence before entering into a commercial relationship** with a client, service provider, subcontractor, commercial partner or other third party.
 - It is our obligation to **report immediately any suspicious activity** that might be related to money laundering or other criminal activities, using the different communication channels that exist.
- **We do not play any part in efforts by someone else to evade taxes or to launder money.**
 - For this reason, payments must in general be made only to the person or company that actually provided the goods or services.
 - Payments must be made in the supplier's country of origin, where they operate or where the goods were sold or the services rendered, unless the supplier has legitimately assigned payment or sold its accounts receivable to another organisation.
 - **NEIKER** will comply with the applicable stipulations of Law 10/2010 of 28th April 2010 on the prevention of money laundering and finance for terrorism.

Some basic protective measures

- Not accepting cash payments, unusual payments in cash or payment by cheque made out to the bearer.
- Payments being made by third parties should be avoided if they are not mentioned in their contract, likewise payments not provided for in the relevant agreements.
- Attention should be paid to payments made to bodies whose partners, owners or ultimate beneficiary cannot be identified, likewise payments to accounts held in tax havens.

Prohibited behaviour

- Accepting payments or transfers in which the origin of the funds is not specified.
- Conducting transactions in which the client or supplier is not identified.

X. PROTECTION AND APPROPRIATE USE OF COMPANY ASSETS

We all have the personal and legal responsibility to protect the company's assets and ensure that they are not damaged, wasted or used improperly.

- These **assets** include physical and intellectual property, time, information and exclusive and personal data, as well as business opportunities and resources. It is **prohibited to use NEIKER assets for illegal, unethical or improper purposes, or with the intention of gaining benefits or earnings either personally or for third parties.**
- We must always **comply with applicable laws, internal requirements, policies and standard operating procedures** with regard to NEIKER assets.
- **Theft of company assets**, whether physical theft (such as the unauthorised removal of a product, device, vehicle or information from the company) or **income deliberately gained through false information** (on hours or claimable expenses), may lead to the initiation of a disciplinary process and if appropriate to criminal proceedings.

Prohibited behaviour

- Using company computers, devices and printers, as well as work time, for activities of a personal nature.
- Asking a subordinate to deal with your personal affairs during their working hours in the company.
- Using a company vehicle for personal purposes.
- Collecting, storing and processing personal data without the consent or despite the objections of the data subject..
- Divulging, publishing, handling or transferring without consent any personal data (clients, employees, etc.) to which you may have access or which might have been revealed by any means.
- Creating user profiles based on data obtained previously.
- Infringement of confidentiality policies.

1. Electronic resources

NEIKER provides the necessary electronic resources for staff to perform its business activities. They are the sole property of the company and must be used responsibly, appropriately and ethically.

- **Electronic resources** including, among others, email, information systems and electronic devices, software, internet and network access, are the sole, exclusive property of **NEIKER**, and are tools that are only to be used by employees to perform their professional task within **NEIKER**, for purposes linked to productive work. It is therefore explicitly prohibited to use these resources for personal purposes or those unconnected with the job the employee does within the organisation.
- **NEIKER** will deal with setting up the hardware and software for work stations and telephones, and administering access to the corporate network, all password-protected to avoid improper access. Only corporate programmes authorised and licensed by **NEIKER** can be used. Should a user need a programme for their work, they may request it from Operations Management. The IT equipment placed at employees' disposal may not be altered either wholly or in part, and no others (personal organisers, printers, voice recognition devices, tablets, smartphones, etc.) may be connected without permission from Resources Management.
- **NEIKER is responsible for supervising the proper use of these resources**, so it makes the express warning that the organisation may carry out preventive and reactive checks to monitor the use of information and knowledge on its systems and premises, and it may at any time conduct specific monitoring of the resources assigned to any person in the organisation.
- In the event of loss or removal of any IT equipment or telephones, the employee must notify the company immediately, to prevent any undesired use or access by third parties.

- The user must return all telematic devices in their possession (laptop computer, mobile phone, etc.) when their employment comes to an end. In the event that they are not returned, or faults arising from improper or unauthorised use by the user are detected, **NEIKER** reserves the right to take whatever steps it considers necessary.
- All work-related **online communications** must be sent through the corporate email address.
- We are aware of the great potential that artificial intelligence offers in our activities, and we commit to ensuring that activities incorporating artificial intelligence meet the following principles: [1] Sustainability: A balanced and responsible use of AI will be ensured, taking into account environmental impact and energy consumption; [2] Transparency in the use and production of artificial intelligence; [3] Traceability, ensuring the identification of content produced with AI; [4] Confidentiality, promoting data security and privacy in the use and development of AI systems; [5] Supervision, the use of AI will be controlled by competent personnel; [6] Training in the use of artificial intelligence; [7] Ensuring compliance with Ethical Guidelines in AI developments.

a) Using NEIKER resources for the following purposes is prohibited:

- For purposes prohibited by law, such as illegal downloading of material protected by intellectual property laws. To attempt to destroy, alter, disable or damage in any other way the organisation's data, programmes or electronic or physical documents. Such actions may constitute criminal damage.
- To store files or documents of a personal nature on company machines. If this becomes necessary for justified, exceptional reasons, the pertinent authorisation must be requested from Operations Management.
- To foster or encourage harassment.
- To use it them in any way that might be perceived as racist, defamatory, discriminatory, violent, cruel, sexist or pornographic.
- The use it in any way that might harm the reputation of **NEIKER**.
- To record or capture pictures and sound on **NEIKER** premises (documentation, computer screens, research conducted, processes, other staff) **for uses other than the strictly professional, and with the pertinent authorisations.**
- To connect to the corporate network by other means than those authorised by the system administrator.

- To try to gain rights or access other than those assigned.
- To try to access restricted areas of in-house or third-party information systems, or distort or falsify the records in information systems, or attempt to decipher passwords or encrypting algorithms or systems and any other security feature involved in information technology processes.
- To possess, develop or run programmes executed within the organisation that might interfere with the work of other uses, or damage or affect any of its information technology resources.

b) Make proper use of email:

- **The use of corporate email addresses for illicit activities is strictly prohibited.**
- Avoid using email from public connections.
- **The use of non-corporate email addresses to send and receive work-related communications is strictly prohibited.**
- **Do not send mass emailings, except with authorisation, and in this case with blind copies to ensure that email address data are not passed on to people other than the addressee.**
- Information and communications of a **personal** nature sent on an exceptional, limited basis in accordance with social convention through the company's electronic means **cannot expect to be private**. Under the signature the mention of the employee's position and the name of the company must be deleted, and the email in question must include the following disclaimer: *"The contents of this message are of a personal nature and do not represent a communication by NEIKER. However, as it is sent from a corporate address, NEIKER may have access to its contents."*
- Use encrypting or secure communication tools where necessary.
- Never reply to **junk mail**.
- **Avoid opening attachments or links from unknown senders.**
- For emails sent to the email account of a user who is no longer on the system after they have left, an auto reply will be set up to answer the sender of such emails. This "auto reply" will tell the sender the following: i) that the user to whom the email was addressed no longer works for the company, and ii) the email addresses of the department or other employees the email can be addressed to.

c) Use appropriately: Internet access, used of social networks and instant messaging applications

- **Through the corporate network only.**
- For professional purposes, this is allowed on an occasional, exceptional basis for **personal** activities, but **no privacy** can be expected.
- Even if **social networks** are considered a **strategic tool**, the coexistence of private social networks and the organisation's corporate network requires that limits be set on their use:
 - **The website, corporate blogs, accounts or profiles on social networks**, etc. are for handling communication and corporate brand image, so their use and content must always be controlled, approved and verified by the organisation.
 - Obviously company control does not extend to **personal use of social networks** or instant messaging applications by its staff, **except** if the organisation is the subject of communications on the said networks, so the use of the company's name, products or services or those of other work colleagues, managers, etc. in this private context must take into account all the above, while respecting the limits of freedom of expression.
 - The following are **not allowed**: sending any reference to matters, clients, interlocutors and colleagues involved in professional activities for **NEIKER** and, in general, any kind of **information** subject to a duty of **confidentiality**. Nor may corporate logos, brands or image elements be used in personal interventions on social networks.
 - Files containing **sensitive data** or data that must be kept private are not to be sent by **instant messaging**, as the information could be accessible to many people, both known and unknown, so there may be a risk to your privacy and that of others. We recommend you do not provide **personal, private and/or intimate information** or any that you want to keep reserved, but only professional information related to the company.

2. Intellectual property

We do our job with strict respect for the intellectual property rights of both **NEIKER** and third parties, and for good scientific practice.

- **Copyright**, registered trademarks, designs, names, logos, inventions and patents, improvements, photographs, videos, discoveries and any other form of intellectual property (such as protocols, procedures, technical processes, research methods, etc.) created or modified in the course of our functions or external relations at **NEIKER** are the sole property of the company and are automatically passed on or ceded exclusively to **NEIKER** by virtue of the contractual relationship, and all reproduction, except for private use, transformation, distribution, public communication, revelation to any third party and in general any kind of **exploitation, wholly or in part, by any procedure**, are prohibited.
- If the development arises outside the relationship with **NEIKER** but using confidential information acquired in the course of your functions and activities in the company, you must notify **NEIKER** Resource Management of this, and the latter will give appropriate guidelines in this respect.
- **NEIKER** strictly prohibits all plagiarism, unauthorised use, theft or illicit appropriation of intellectual property belonging to third parties, including any information, programmes, files or applications we download from the Internet, or summaries, research projects, applications to institutional revision committees or manuscripts whether published or unpublished in any format (printed or electronic).

Bad practices

- Plagiarism is the appropriation of ideas or phrases from other papers, presenting them as original work and without citing the source, with the intention of claiming them as the writer's own. This can take different forms and involve one's own previous work or that of others.
- Fictitious authorship, attributing authorship to someone who did not take part, usually in return for some compensation or favour (generally from a superior).
- Multiple publication or duplicated, fragmented or inflated publication.

a) Regarding **NEIKER's** rights:

- **NEIKER** prioritises protection of new ideas by registering them.
- You must not reveal new ideas or plans to outside people or media until the pertinent rights have been protected, and you are sure that you have received the necessary prior authorisation.

- As an employee you recognise that in the course of your work you may acquire valuable commercial or technical experience in activities that form part of NEIKER's business or its clients' business, so you undertake not to use this know-how and confidential information with any competitor of NEIKER or of its clients, without these parties' explicit written authorisation. Any of these behaviours will be considered unfair competition and a breach of the obligations set forth in this document.

3. Confidentiality and security of information

We must protect all non-public and confidential company information to which you may have access in your work, abiding by privacy laws, to offer our clients confidence and security. Furthermore, personal data are to be processed properly and in accordance with applicable regulations.

a) Principles in handling personal data:

- Personal data, i.e. data that may be used to identify an individual either directly or indirectly, are subject to an **obligation of confidentiality**, i.e. are to be treated confidentially in personal terms, and their integrity must be assured. NEIKER will **treat such data licitly, properly and transparently**, and **protect** them from access by unauthorised persons, **illegal** processing or illicit transfer to third parties, as well as **accidental loss, alteration or destruction**, and limit the time they are kept. The **data subject must be informed** of the processing and use of their data, and where appropriate their unequivocal consent obtained in a way that can be accredited.
- All information of a personal nature collected by NEIKER may **only be processed for the purposes for which it was gathered**. Subsequent **modification** of this purpose is only possible under certain conditions and requires **prior authorisation by the data subject**.

Practical cases

- I receive, by mistake, an email with a file containing the salaries of some other employees. Can I share it with other people at work?
- No, we have no reason to have this information. We must delete the email and point out the mistake to the sender. Revealing information to other employees is an infringement of the Code.

- By default, process only the **minimum data necessary** for the purposes for which it was collected, in terms of both quantity [reserve the identity of the holder if possible] and the extent of processing and accessibility, **limiting the time for which they are kept** and establishing **deadlines for their erasure**.
- The **personal data** must be **exact and complete**, and must always be kept **up to date**, for which reason you are **asked** to duly report any **changes** in your personal data.
- The measures established by **NEIKER** to ensure data security must be respected at all times.
- The **obligations of confidentiality and secrecy** will subsist even after the relationship with the data controller or processor has come to an end.

b) Our obligations include the following:

- **Informing the Resources Dept. of the need to process personal data so that it can record and supervise this.**
- **Request authorisation by the Resources Department when it is not possible to comply with any obligation due to exceptional circumstances.**
- **Avoid** acquiring, revealing, holding or using in any way information containing the personal data of clients or the organisation itself in files - whether physical or digital - owned by **NEIKER** or in its custody for third parties for personal purposes or any other use not compatible with the purpose of the file containing the data or to provide the pertinent contractual services. This information is the sole property of the data subjects
- **Keep, protect and store** information with personal data in a safe place, both within the organisation and, in particular, if this data and information is **transferred outside it on any medium** (e.g. files, folders, etc.), taking special care not to **lose them or let any unauthorised persons access or manipulate them.**
- Return all media containing personal data to which you might have had access in your work to the company immediately after completing the tasks leading to the temporary use thereof, and in any case at the end of your employment relationship.

c) Confidential corporate information:

- **NEIKER handles a lot of information, both its own and that of clients, and confidentiality and professional secrecy are essential in the realm of research.**
- Illicitly obtaining, using or revealing non-public information is explicitly prohibited.
- All confidential information will be the sole property of NEIKER or of the organisation that owns it, and under no circumstances of employees.
- **NEIKER must protect its own and third parties' confidential information, so it must prevent its undue or unauthorised revelation.**
- **Before revealing any non-public information to anybody outside the company, a confidentiality agreement must be signed to prevent improper use of the information, or its confidential nature must be specified in the information itself.**
- The obligations of confidentiality and secrecy will subsist even after the employment relationship has come to an end.

d) How to safeguard the confidentiality of information:

- **Maintain absolute secrecy and confidentiality regarding any documentation and information on NEIKER or its clients/collaborators to which you may have access in whatever form or medium. They must not therefore be accessible, either directly or indirectly, to any third party, unless such revelation arises from a contractual agreement or is authorised explicitly by the owner of the information, bearing in mind that, in any case, any third party to whom revelation may be authorised must sign the pertinent confidentiality commitment with the company if so decided.**
- Information or documentation is not to be used either directly or indirectly for any purpose other than that for which it was handed over or obtained.
- You must return to NEIKER, once your employment relationship comes to an end, all information and documentation (originally handed over by NEIKER or arising from fulfilment of the contractual relationship) all copies thereof in your possession or that of your representatives, including all documents, files or computer, analogue, magnetic or digital media, notes, drawings and any other kind of documents, programmes and histories

incorporating or based on the said information or documentation (regardless of who prepared them), and you must confirm to the company that you have not kept any of the above.

- Destroy sensitive information securely when it is no longer needed.
- Information or documents on the company or its clients, suppliers or personnel may not be copied to any kind of digital media or external storage.
- Documents and information of all kinds of a professional nature are not to be stored in cloud storage systems such as Dropbox, Teambox, etc., without explicit authorisation by Operations Management.
- **When you leave your workstation:**
 - Always tidy your desk, leaving no sensitive documents in sight but storing them away safely.
 - Block the screen of your computer whenever you leave it unattended.
 - Turn the computer off at the end of the working day.
- **Use of printers (especially if shared)**
 - Do not leave the originals of any document in printers or photocopiers but remove them immediately, especially if they contain personal data.
- **Use of passwords:**
 - A user name and password will be provided to access electronic resources; the password will be time-limited by the system.
 - Do not share it with anybody or write it down anywhere.
 - Do not tell your computer to "remember" passwords.
- **Before opening any outside document:**
 - Avoid opening documents of unknown origin.
 - Do not click on links that might take you to insecure websites.

XI. COMMUNICATIONS

We will communicate openly, sincerely and transparently, both internally and externally, within the limits of confidentiality.

1. Internal communications

- We will pass on relevant information to our teams in a professional, prompt and clear manner. Internal communication must be professional, even when it is informal.
- In any case, we use clear, precise information and easy-to-understand language.

2. External communications

- We must make sure we abide by commitments to confidentiality of information, as mentioned above.
- We act in a professional manner when we represent NEIKER, especially when we have company identification or attend events on its behalf.
- Any participation by an employee on behalf of the company as a speaker at a talk, congress, panel or any other medium of communication (television, radio, online, social network, in print or any other) must be authorised by their head of department and its contents must be approved in advance by the head of their department and the head of communication. In the event that such participation occurs without having been planned in advance, it must be reported after the event.

General guidelines

- We ensure that our communications are professional, agile, clear and comprehensible.
- We bear in mind when we represent **NEIKER** that what we do and say in public represents the company, and we must safeguard its image and reputation.
- We do not give personal statements or opinions that might be interpreted as being on behalf of the company, or we must clarify this promptly.
- We do not make negative statements about NEIKER's reputation or brand or about our colleagues, clients, suppliers, competitors, commercial partners, collaborators or subcontractors.

Social networks

- We can identify ourselves as **NEIKER** employees in our profile, making clear our position in the company and keeping this up to date at all times so as not to cause confusion. We may also include its logo and a link to its website.
- On social networks we will act in accordance with the guidelines laid down in this Code and other internal policies.

