COCUS Code of Conduct

COCUS AG
Prinzenallee 11
40549 Düsseldorf, Germany

Table of contents

Introductory words from the CEO

1. We act out of conviction

2. Compliance with Laws
   - 2.1. Adherence to Applicable Laws
   - 2.2. Insider Trading
   - 2.3. Fair Competition and Antitrust
   - 2.4. Prevention of Money Laundering
   - 2.5. Gifts and Invitations
   - 2.6. Anti-Bribery and Corruption
   - 2.7. Trade Controls
   - 2.8. Economic Sanctions

3. Individual Conduct
   - 3.1. Information Security and Data Protection Compliance
   - 3.2. Information Security
   - 3.3. Handling of Information
   - 3.4. Use of Company Resources
   - 3.5. Visitors
   - 3.6. Document Management
   - 3.7. Data Protection
   - 3.8. Avoiding Conflicts of Interest
   - 3.9. Respect for Local Laws and Cultures
   - 3.10. Expense Policies and Environmental Factors

4. Employees
   - 4.1. Respect
   - 4.2. Harassment, Bullying, and Discrimination
   - 4.3. Preventing and Reporting Misconduct

5. Communication
   - 5.1. Speaking on behalf of COCUS
   - 5.2. Social Media

6. Health and occupational safety

7. Financial Integrity
   - 7.1. What financial integrity means
   - 7.2. Contracts and expenditures
   - 7.3. Procurement responsibility
   - 7.4. Protection of COCUS
   - 7.5. Public conduct
   - 7.6. Financial responsibility

8. Society and environment
   - 8.1. Social responsibility
   - 8.2. Environment

9. Scope of application of the Code of Conduct

Introductory words from the CEO

As the CEO of COCUS, the **Co**mpany for **Cus**tomers, I would like to emphasize that our foundation of trust, transparency, and integrity, is what defines us both internally and externally. Over the past decades, we have earned the trust of our customers, colleagues, and partners. This trust is based on our commitment to making the right decisions and acting responsibly in all circumstances.

This Code of Conduct outlines the principles, values, and standards of COCUS, and is intended to serve as a practical guide for all employees, contractors, subsidiaries, and suppliers. It is designed to help everyone act with integrity, make responsible choices, and uphold our corporate values, especially in challenging situations.

I urge everyone working with or for COCUS to read, understand, and adhere to this Code of Conduct - at COCUS and beyond.

Oliver Hüttig
CEO, COCUS AG

Contacts

HR

Alexandra Monteiro

peopleoperations@cocus.com

Compliance Officer

Stephan Hock

shock@cocus.com

Security

Catarina Pereira

infosec@cocus.com

Data Protection Officer

Matthias Edelmann

datenschutz@cocus.com

Corporate Social Responsibility Officer

Viola Rösener

vroesener@cocus.com

1. We act out of conviction

Our principles are built on trust, openness, and integrity.

Our Code of Conduct reflects the values and expectations that we, as COCUS and as employees, uphold in our collaboration with one another, as well as with our customers and suppliers, as COCUS and as employees.

The Code of Conduct helps us to make not only convincing but also the right decisions. It serves as a guide to maintaining and further developing the COCUS standard while always remaining true to our principles and values.

Who does the Code of Conduct apply to?

Our Code of Conduct applies to everyone who works for or with COCUS.

We expect all employees, managers, contractors, subsidiaries, suppliers, and business partners to understand and adhere to the principles set out in the Code. COCUS ensures that the Code of Conduct' requirements align with applicable local laws and regulations, and that every individual understands and adheres to them.

Failure to comply with the Code of Conduct, legal provisions, or applicable policies may, lead to serious consequences in certain cases,. For employees, depending on the severity of the violation, these consequences may range from verbal warnings and disciplinary measures to termination of employment.

For suppliers, depending on the severity of the violation, consequences may range from corrective actions and proof of future compliance with the Code to termination of the business relationship. Any party in breach of the Code is liable for any damages caused to third parties as a result of non-compliance.

What exactly does this mean?

Everyone associated with COCUS is expected to familiarize themselves with the rules of conduct outlined in this Code and act in an ethically responsible manner. The Code serves as a guide to support everyone fulfil their legal, contractual, and regulatory obligations by applying its principles to their daily actions.

How can I be sure that I am acting in accordance with the Code?

In most cases, putting our values and principles into practice is straightforward. However, there may be situations where making a decision feels uncomfortable. If you find yourself in such a situation and are unsure whether your actions, or those of others, align with our values, ask yourself the following questions:

- Is the action lawful?
- What does my conscience tell me?
- Do I have all the information I need to make a decision?
- Am I deciding freely, or am I being pressured?
- Does the action feel right, fair, and honest?
- How would I feel if I were affected by this decision?
- How might others perceive it?
- Would I feel comfortable telling others about it?
- Can I justify the action to myself and to others?

If you cannot answer any of these questions with a clear conscience or, if you are uncertain, it is likely that the action conflicts with our principles.

As an employee, in case of doubts, please contact your team, your manager, the People team, or our Compliance Officer directly.

As a COCUS business partner, please reach out to your contact person within COCUS or directly to our Compliance Officer.

2. Compliance with Laws

2.1 Adherence to applicable laws

COCUS operates in many countries and across various jurisdictions, not least because of our international workforce. While our Code of Conduct cannot cover every national regulation, each employee and supplier must know and comply with the laws and regulations applicable to their work location, as well as any relevant international provisions governing their area of responsibility.

If you are uncertain, please contact your supervisor, your HR representative, or the Compliance Officer.

As a COCUS leader, you are expected to familiarize yourself with our Code of Conduct and to internalize our principles and expectations in line with our core value: “Making the right decisions.”

Managers at COCUS are expected to:

- Serve as role models who embody our principles and expectations;
- Ensure that their teams understand and follow this Code;
- Encourage accountability and help resolve questions of interpretation; and
- Respond appropriately to any violation of applicable rules.

We expect our business partners and suppliers to comply fully with all applicable laws and with every provision of this Code - both at their own sites and in the countries where they perform services for or on behalf of COCUS.

2.2 Insider Trading

The disclosure of confidential information, including insider trading, is strictly prohibited. Any information that is not publicly available and that you obtain through your work at COCUS must remain confidential during and after your employment or business relationship with us.

This protects both COCUS and you personally. Insider trading may result in severe fines or even imprisonment. If you have any questions or concerns, please consult the Compliance Officer.

Please remember:

- Do not buy, sell, or trade in shares or securities of any company - especially customers or suppliers - if you possess inside information about that company.
- Do not share insider information about customers, suppliers, or other companies obtained through your work at COCUS with anyone, including partners, relatives, or friends.

The use or disclosure of inside information violates confidentiality obligations and constitutes a criminal offense.

2.3 Fair competition and antitrust

COCUS maintains a reputation for integrity, which is of utmost importance to us. We compete based the quality of our products and services and we are committed to free and fair competition.

Antitrust and competition laws safeguard open markets and prohibit collusion or behavior that restricts trade. We comply with all such laws in every country in which we operate, avoiding practices that could be considered anti-competitive, including:

- Exchanging or discussing confidential information such as costs, prices, revenues, or profit margins, with competitors;
- Agreeing with competitors to divide customers, territories, or market segments;
- Coordinating prices, discounts, or commissions with competitors or partners;
- Setting resale prices jointly with distributors or partners; and
- Entering into informal arrangements or information exchanges with competitors.

If it is unclear whether another company qualifies as a competitor, exercise caution and, in case of doubt, consult the Compliance Officer so that the relevant experts can be involved.

2.4 Prevention of money laundering

COCUS is committed to preventing, detecting, and reporting money laundering and the financing of illegal activities. We conduct business with due diligence and apply internal controls to identify suspicious transactions. If you have reason to suspect money laundering or notice irregular transactions, contact the Compliance Officer immediately.

2.5 Gifts and invitations

Gifts and invitations can be a legitimate part of business relationships, yet they must never influence, or appear to influence, a decision. This applies equally to benefits given or received.

You must decline any gift or invitation that, because of its value, motive, or timing, could compromise your objectivity or expose you or COCUS to criticism. Be especially

cautious with benefits that are not socially appropriate or clearly exceed customary business courtesies.

Remember that COCUS can be held liable for the conduct of third parties acting on its behalf. If you are uncertain whether to accept or offer a gift or invitation, discuss the situation with the Compliance Officer beforehand.

2.6 Anti-bribery and corruption

COCUS rejects all forms of bribery, corruption, and extortion. No corrupt behavior is tolerated, whether by employees or through third parties. Bribery and corruption may involve not only direct cash payments (“kickbacks”), but also concealed commissions, excessive donations or sponsorships, or other material advantages granted to influence a decision, whether provided to the recipient personally or to a third party. Offering or

accepting money or similar payments is strictly prohibited. Special care must be taken when dealing with public officials. All applicable local and international anti-corruption laws must be observed.

COCUS also refrains from making political contributions. Even charitable donations can be considered improper if they are used to obtain an unfair advantage.

If you, your family members or others are threatened in an attempt to coerce you into taking specific actions or omitting them, contact the Compliance Officer immediately.

2.7 Trade Controls

International trade controls are in place to protect global peace and security by regulating the movement of goods, technologies, knowledge, and services across borders.
As a global company, COCUS complies with applicable national and international export control laws.

Employees and suppliers acting on behalf of COCUS must verify, prior to any export or re-export, whether the product, technology, or service - or the recipient country or entity - is subject to trade restrictions. When required, obtain the appropriate export licences and permits.

If you are uncertain, consult the specialists responsible for the product or technology or contact the Compliance Officer.

2.9 Economic Sanctions

In addition to trade controls, international sanctions laws restrict financial transactions with certain countries, entities, and individuals. COCUS complies with applicable national and international sanctions regimes.

Employees and suppliers must ensure that all parties involved in any relationship, agreement, or transaction on behalf of COCUS, have been screened against relevant sanctions lists.

If you are asked to conduct business with a sanctioned country, entity or person, you must immediately inform the Compliance Officer so that the case can be reviewed.

3. Individual Conduct

3.1 Information Security and Data Protection Compliance

COCUS is proud to be ISO/IEC 27001 certified and TISAX labeled, reflecting our strong commitment to safeguarding information assets, maintaining confidentiality, integrity, and availability of data, and ensuring compliance with international security standards.

As part of this commitment, every employee, contractor, and business partner plays a crucial role in maintaining and continuously improving our Information Security Management System (ISMS). Information security and data protection is a shared responsibility across the entire organization.

All employees are required to:

1. Follow all compay policies, standards and guidelines related to Information Security and Data Protection
2. Report any suspected or actual security incidents or data breaches immediately through the dedicated channels
3. Participate in regular security and data protection trainings to remain aware of current threats, responsibilities and company requirements

3.2 Information Security

As a solutions and service provider, COCUS handles vast amounts of information every day. All information, whether written, verbal, physical, or digital, must always be protected.
We expect all employees and third parties to handle information responsibly by following the CIA principle:

- **Confidentiality:** Information must remain confidential and protected from un authorized access.
- **Integrity:** Information must be safeguarded against un authorized alteration.
- **Availability:** Information must be accessible when legitimately required.

Protect access to your work tools and all entrusted data. Follow the COCUS guidelines for IT system use and data protection. All policies can be found in the *Information Security and Data Portal's on SharePoint*.

3.3 Handling of information

Classify the information you handle according to its sensitivity. Guidelines for this can be found in the *Information Security Classification Policy* on SharePoint.

Information must be assigned to one of the following categories:

Secret:

Disclosure would cause extreme financial or legal damage to COCUS, and the information is of existential importance to COCUS. This information is restricted to certain groups and may only be shared in special circumstances.

Examples:

- Financial insider information prior to its publication
- Company acquisitions
- Salary information
- Intellectual property rights related to developments
- Personalised passwords
- Special categories of personal data (in accordance with the GDPR, the Federal Data Protection Act, the Telecommunications Act, and the Telemedia Act):
    - Content and circumstances of private correspondence and telecommunications (e.g., unopened personally addressed letters, private emails, private telephone calls, and itemised call records
    - Personal usage data (e.g., VPN service)
- Non-COCUS information subject to non-disclosure agreements with third parties or other contractual obligations to ensure confidentiality.

Confidential:

The unauthorized disclosure of "Confidential" information would clearly harm COCUS and/or violate the privacy of customers, partners, or employees. Relationships with service providers, business partners, external auditors, or regulatory authorities may, in some cases, require that information classified as "Confidential" or higher be shared with third parties. In such cases, the following requirements must be observed:

- The information owner must provide written consent (e.g., via email)
- The recipient must sign a legally binding non-disclosure agreement (NDA)
- Both authorisation for access and the NDA must be archived in accordance with legal requirements

If third parties provide their own confidential information to COCUS for use, the contractual terms governing such information must be strictly adhered to. COCUS employees are not authorized to sign confidentiality or non-disclosure agreements personally; such agreements must be handled in accordance with the company's signing policy.

Appropriate security measures must be implemented for this type of information, such as encrypted transmission and storage.

Examples:

- Personnel files or employee data
- Customer data
- Supplier data
- Business or marketing plans
- Financial data
- Offers and cost calculations
- Contract content or details
- Technical details of security measures
- Passwords for technical, non-personal user accounts (if the technical account provides access to information classified as "Secret" and/or to business-critical IT systems, the password must be classified as "Secret")

Internal:

Basic protection and careful handling are necessary to safeguard COCUS's interests. The unauthorized disclosure of information classified as "Internal" would contradict COCUS's interests and is therefore intended for internal use only.

In special circumstances and for a valid business reason, it may be necessary to share such internal documents accessible with third parties, such as service providers or business partners. In these cases, the information should be shared in a controlled manner whenever possible, for example:

- Providing only the table of contents
- Allowing access to the document only within COCUS premises
- Not distributing copies or digital versions
- Requiring the signing of a legally binding non-disclosure agreement by the recipient to maintain confidentiality if further information is shared

Examples:

- Operational business information or reports
- Corporate policies, standards, and guidelines

- Internal communications
- Detailed technical documentation
- Company directory and telephone list

Public:

Any information that is publicly available and that cannot cause harm to COCUS may be communicated. However, a basic level of protection is still required, particularly with regard to integrity and availability. Information is classified as “Public” when it has been authorized for public release. Information at the “Public” level is not considered sensitive in content and does not require special protection.

Examples: Information created for public dissemination, such as:

- Press releases
- Marketing materials
- Advertising
- Job postings

3.4 Use of company resources

Follow these rules:

- Never share your password or any other data that could allow third parties to access your information. Use the approved password management system. Your password should be sufficiently secure to protect against potential attacks. Memorize it well—do not write it down or store it in easily accessible tools or files.
- If you leave your workspace or computer unattended, make sure you follow the clean desk and clear screen policy and lock your screen. Likewise, do not leave confidential physical documents exposed on your desk. This is especially important at the end of the workday: your workspace should be tidy, and all sensitive materials should be securely stored away.
- Be careful not to leave original documents in printers or photocopiers.
- Watch out for phishing! Think twice before opening an unknown email attachment or clicking on a link in an email. These may lead to unsafe websites and, in the worst case, compromise our security systems. “Better safe than sorry”.

- The internet and email can be used for many types of attacks on information security. Follow the safe internet and email use guidelines available in Information Security and Data Protection Portal.
- Use only the official, secure COCUS business email address for professional communication.
- Never send company or customer information to a private email account or download it to personal computers or other private devices.

Despite all caution, mistakes can happen. If something does occur such as an accidental click, lost documents, or an email sent to the wrong recipient, you should act quickly:

- If you suspect malware, disconnect your computer from the network immediately, e.g., by turning off the Wi-Fi adapter.
- If you have shared your user credentials in a phishing attack, change your password immediately to a new, strong password that differs significantly from the old ones.
- Then promptly report the security incident to IT Support and the Information Security Officer.

The same rules apply when working off-site, at home, or on customer premises. Please refer to Remote Work Policy available in our SharePoint portal for details.

3.5 Visitors

To ensure our workplaces remain as secure as possible, please announce any visitors in advance and register them upon arrival or enter their details in the visitor logbook / visitor management form. Visitors should be met at reception and accompanied to the meeting room or workspace.

While on our office premises, visitors must wear a visitor badge to clearly identify themselves as external persons.

3.6 Document Management

Store documents carefully and securely. Avoid unnecessary printing - use digital formats wherever possible. After the retention period defined in local policy, destroy paper documents in an environmentally safe manner and delete digital records in

compliance with audit requirements and documents. For additional detail please refer to the Classification of Information Policy available in SharePoint portal.

3.7 Data Protection

Data protection and privacy are at the heart of our business. COCUS is committed to safeguarding the personal data of employees, contractors, customers, and suppliers.

All employees and suppliers must adhere to the company's *Data Protection Policies* which are accessible on SharePoint portal. Suppliers are bound by the respective contractual clauses or data-processing agreements.

As part of our work, we collect personal data from employees, former employees, customers, suppliers, and other affected parties. This data is intended solely for the purpose for which it was provided and is collected, processed, used, and stored in accordance with legal requirements.

If you are entrusted with information processing, it is essential to ensure the confidentiality, integrity, availability, traceability, and resilience of the protected information. Unauthorized internal or external use of personal data provided to you is strictly prohibited and must be prevented at all times.

Please ensure that the collection, storage, processing, transfer and any other use of personal data is carried out only with the consent of the data subject, under a contractual agreement, in accordance with a legal provision.

If you, as an employee or supplier acting on behalf of COCUS, have any questions regarding the data protection of specific information, please contact our Data Protection Officer.

3.8 Avoiding conflicts of interest

Situations may arise where your personal interests conflict with COCUS's business interests. If you find yourself in such a situation, or if you are unsure whether a situation constitutes a conflict of interest, please inform us and disclose the situation openly. The best way to do this to contact the People team.

Sometimes it is not entirely clear whether a particular situation represents a conflict of interest. Here are a few examples, though this list is not exhaustive:

- Close personal relationships with the management of a competitor, customer, or supplier
- Engaging suppliers or customers based on personal rather than professional interests, especially if a personal financial interest is involved
- Hiring employees with whom you have a family or very close personal relationship
- Maintaining personal relationships with suppliers or customers during tender processes
- Secondary employment that conflicts with your employment contract, legal regulations (e.g., maximum daily working hours), or the legitimate interests of COCUS
- Use of COCUS resources for personal and/or political purposes

If you are uncertain about actions and a potential conflict of interest may exist, please speak with your manager, or the People team. It is possible that you may need your supervisor's approval for certain actions.

Do not participate, either directly or indirectly, in contract negotiations with business partners where a conflict of interest exists.

When hiring, ensure that you do not favour any candidate in order to gain personal or professional advantages from the hiring decision.

Do not make donations on behalf of COCUS.

Report any secondary employment or other professional activities before signing your contract with COCUS, and await written approval. These regulations also apply to suppliers acting on behalf of customers in relation to COCUS or COCUS clients. If you have any questions or are felling uncertain, please contact your designated Partner Manager at COCUS.

3.9 Respect for local laws and cultures

COCUS operates beyond Germany's borders. As one of our offices is located in another European country and our customer base is international, negotiations and projects may occasionally take you abroad. At COCUS, we believe that it is important to respect applicable German and Portuguese laws and culture, but also to uphold this attitude when traveling internationally. Before travelling, consult colleagues or supervisors to learn about potential cultural differences and how to handle them appropriately.

3.10 Expense Policies and environmental factors

To ensure that we can reimburse all your travel and other COCUS-related expenses, you must adhere to the applicable travel expense policy. This policy is available in our COCUS intranet. It covers everything from car rentals and hotel stays to meal allowances and train travel.

When planning your expenses, please consider cost efficiency and environmental awareness, and adhere to the policy when submitting your expense reports. Maintaining a healthy balance between business needs, financial costs, your well-being, and environmental impact is essential.

If you have any questions about the reimbursement process, please consult your supervisor for feedback and if, necessary, approval.

Please keep all receipts carefully, as they must be submitted for reimbursement.

4. Employees

4.1 Respect

Equal opportunity and fair treatment are fundamental principles of our open and inclusive work environment at COCUS. We are proud that our employees interact with one another with respect, cooperation, tolerance and appreciation of diversity.

We explicitly reject all forms of discrimination and racism. This expectation applies to all employees, and any violation of these standards will be addressed through disciplinary measures.

At COCUS, fairness and respect are non-negotiable. All personnel decisions are based solely on performance, ability, and professional qualifications.

If you believe that you, or anyone else at COCUS have been discriminated against or targeted because of age, gender, sexual orientation, cultural background, religion, or any other personal attribute, please report it immediately. Your point of contact People team, and every concern will be handled individually and confidentially. The Whistleblower platform is available to all German employees.

4.2 Harassment, Bullying, and Discrimination

Harassment, bullying, or discrimination of any kind have no place at COCUS. Any conduct intended to harm, humiliate, intimidate, or coerce another person - whether physically or psychologically—is strictly prohibited. This includes derogatory or offensive comments, even if they are not made directly to the affected person.

Always treat colleagues and business partners with the same respect you would wish for yourself. If you are subject to harassment or bullying, report it immediately to People team. If you witness such behavior, encourage the affected colleague to report it - or do so yourself.

4.3 Preventing and Reporting Misconduct

We ask every employee to report any behavior that violates this Code of Conduct. Treat others with respect —just as you would expect respect in return.

All reports will be handled confidentially, and your identity will be protected. No whistleblower who raises a legitimate concern in good faith will face retaliation from COCUS management or colleagues. Once a report has been received, it will be documented and reviewed in coordination with the Compliance Officer. Depending on the nature of the issue, the investigation may involve People team, the Compliance Team, or Data Protection Officer. Your identity will only be shared with these departments if you agree. If you choose not to remain anonymous, you may be contacted for further details and kept informed of the progress where appropriate. All investigations will be recorded and archived in accordance with internal compliance procedures.

5. Communication

At COCUS, we value open and transparent communication. We are proud to communicate honestly and responsibly with all stakeholders while safeguarding

confidential business information. Please contribute to this by ensuring that information not intended for the public remains internal.

Within our teams, communication should be informal yet always professional and respectful.

5.1 Speaking on behalf of COCUS

In today's information-driven world, statements can have significant impact. It is therefore essential that any communication made *for or on behalf of COCUS* adheres to our external communication guidelines.

No employee may speak publicly on behalf of COCUS without proper authorisation. If you are approached by journalists, external organizations, or individuals seeking a statement on business-related matters, notify your supervisor before responding.

Remember that everything we communicate externally reflects COCUS as a company. If you wish to publish a statement, announcement, or article referencing COCUS and require assistance, please contact the Marketing Team.

5.2 Social Media

Social media plays an important role in COCUS's external presence. We use professional channels to share information about our company, solutions, and career opportunities, and we encourage employees to engage professionally online as brand ambassadors.

At the same time, we ask everyone to remain mindful that thoughtless posts can have unintended consequences.

We welcome your interaction with our official profiles and encourage you to share your experiences with COCUS, provided you adhere to the following principles:

- Communicate professionally, respectfully, and factually.
- Do not post criticism that is not justified or comments that could harm COCUS' reputation.
  If you have concerns or feedback, please share them internally with People team or your supervisor.

- Never disclose client information or express negative opinions about customers, even internally on social platforms.
- Anonymous reviews on employer-rating sites are acceptable but they must always be truthful and respectful.
- Do not share confidential information, including financial data, pricing, or project details.

By acting thoughtfully, each of us helps to protect the reputation and credibility of COCUS across all communication channels.

6. Health and occupational safety

COCUS takes its responsibility for the health and safety of all employees seriously. Our goal is to provide working conditions that protect well-being, maintain performance, and foster job satisfaction.

All employees are expected to adhere to occupational health and safety regulations at all times.

This means you must never knowingly endanger your own or other's safety. To help ensure this, please observe the following principles:

- Be aware of how your decisions and actions affect the safety and health of yourself and others.
- Do not work under the influence of alcohol, drugs, or any medication that impairs concentration or judgment.
- Intervene if you see someone putting themselves in danger, but never endanger yourself in the process
  In case of doubt, call for assistance or emergency services.
- When traveling to or from work locations, comply with all traffic regulations and exercise caution.
- Follow all applicable rules and safety instructions when on customer premises.

If you have any questions, suggestions, or concerns, please contact People team.

COCUS places particular emphasis on **prevention**. We want to avoid situations that could compromise physical or, increasingly, mental health.

To support this, in Germany employees have available the **Employee Assistance Programme (EAP)**.

Through the contact information provided on the intranet and posted on site, you or your family members can reach the EAP service provider anonymously. They can connect you with qualified experts, who can help with medical, psychological, or other personal issues.

Your health, safety, and well-being are essential to our shared success.

7. Financial integrity

7.1 What financial integrity means

At COCUS, we base all investment decisions, acquisitions, and business relationships on sound economic criteria. We are committed to acting in a cost-consciously, sustainable, and responsible manner. Any manipulation of financial reporting that violates company policy or the law is strictly prohibited.

Company funds may only be used for legitimate business purposes. All employees are responsible for ensuring that expenditure are appropriate, properly authorized and in COCUS's best interests. Adhered to internal **Finance, Travel, and Approval Policies** to maintain transparency and control.

Managers are accountable for the proper management of budgets. They must carefully review spending and authorize it only when it meets COCUS's quality, service and ethical-procurement standards, and aligns with our general terms and conditions.

7.2 Contracts and expenditure

Employees must comply with all COCUS policies governing contracts and travel expenses. Do not enter into any agreement or create any financial obligation on behalf of COCUS without the necessary authorization.

All contracts are subject to legal and commercial review before signing. Ensure that conditions are examined and approved in line with our internal approval hierarchy.

If you are uncertain about any contractual term or expense, discuss it with your supervisor before committing to it.

Managers are responsible for carefully managing their budgets and ensuring that funds are spent only on approved business purposes.

7.3 Procurement responsibility

COCUS works with a network of suppliers and service providers who have been selected based on objective and transparent criteria and who meet our procurement, information security and data protection standards.

If you are involved in purchasing decisions, you should always obtain and evaluate alternative offers. Consider ethical standards, sustainability, and environmental impact when selecting vendors.

7.4 Protection of COCUS Brand

Our shared objective is to protect the reputation and integrity of the COCUS brand.

Contribute to this by following our **Branding and Communication Guidelines**. Contact the Digital Experience & Marketing team if you suspect the misuse of the COCUS logo or intellectual property.

Our brand assets must never be used by third parties without prior approval.

COCUS competes with many national and international companies. Our ideas, projects, and product concepts are key to safeguarding our collective jobs and ensuring our continued success.

Do not publish new ideas, projects, or product concepts externally without prior authorization from the Digital Experience & Marketing team and, if applicable, confirmation that intellectual property protections are in place.

When communicating with customers or suppliers, only share approved information and verify that valid confidentiality agreements exist. If you have any questions, please contact your Sales team or the Compliance Officer.

7.5 Public Conduct

No employee may publicly represent COCUS without authorization. If you are asked by the media, public authorities, or external organizations to comment on business matters, consult your supervisor first.

COCUS does not participate in political activities and strictly prohibits donations or contributions to political parties or campaigns.

When representing COCUS in public, follow the Media and Public Relations Guidelines. Never use your role/position at COCUS to influence others politically or to support political initiatives on behalf of the company.

7.6 Financial responsibility

COCUS is committed to the accurate and complete recording, storage, and retention of all business documentation, including financial statements, invoices, regulatory filings, and accounting records. All disclosures must be transparent and truthful, and made in accordance with applicable laws and generally accepted accounting principles.

Integrity in financial reporting ensures trust - with our employees, partners, regulators, and the public.

8. Society and environment

COCUS aims to make a positive and lasting contribution through its actions and business activities, improving people's lives in a sustainable way. To fulfil this responsibility, we comply not only with all applicable national and international laws,

as well as global conventions and principles designed to protect people and the environment.

8.1 Social responsibility

COCUS places great importance on promoting and developing its employees. We want to create workplaces where people can contribute, grow, act responsibly and collaborate respectfully and successfully. Equal opportunity and fair, locally appropriate compensation are essential principles for us.

We do not work with companies - whether customers or suppliers - that violate these standards or fail to share them.

As a medium-sized enterprise, we have strong ties to our roots and local communities. We therefore support the regions in which we operate, and we welcome proactive employees who wish to engage in local initiatives that strengthen this commitment.

COCUS recognizes all international human rights, including those set out in the **United Nations Universal Declaration of Human Rights** and the **International Labour Organization's Declaration on Fundamental Principles and Rights at Work**.

Furthermore, we are committed to implementing the UN Guiding Principles on Business and Human Rights. We reject all forms of child labor, forced or compulsory labor, and any form of modern slavery or human trafficking. We will immediately terminate cooperation with any business partner who does not adhere to these same principles.

We ensure fair compensation and guarantee at least the legally mandated national minimum wage. We also meet fulfil all obligations relating to social security contributions and taxes. We comply with national labor regulations regarding working hours and expect the same compliance from all suppliers and subcontractors. Any violations may result in the re-evaluation or termination of our cooperation.

COCUS recognizes the fundamental right of all employees to organize, to form unions or worker representations, and to engage in open, cooperative dialogue with such organizations.

8.2 Environment

As an international company, COCUS acknowledges its responsibility towards both people and the environment in all the countries in which it operates. We conduct our business in an ecologically sustainable manner, aiming to minimize any negative environmental impact. Our operations adhere to socially responsible, economically sound practices that comply with all applicable environmental, health, and safety laws and regulations.

When developing products, services, and processes, we assess and limit their environmental impact to the lowest feasible level. We expect the same environmental awareness from our customers, suppliers, and contractors.

In recent years, COCUS has implemented several sustainability measures – such as:

- Replacing paper-based workflows with digital processes
- Installing central water dispensers to reduce bottled water deliveries
- Electrifying more than 50 % of our company car fleet.

Each of us can contribute environment protection by:

- Knowing and complying with all relevant environmental regulations and guidelines
- Avoiding and reducing waste while using recycling systems
- Opting for digital meetings instead of unnecessary travel
- Considering environmental impact in purchasing decisions
- Using COCUS's sustainable commuting options such as public transport passes and bike-leasing programs
- Forming carpools with colleagues whenever possible.

Together, we ensure that sustainability remains an integral part of how COCUS operates and grows.

9. Application of the Code of Conduct

The rules set out in this document apply to all **COCUS employes** and those of its subsidiaries, as well as to all COCUS suppliers and business partners acting on behalf of COCUS. Where additional or more specific guidelines exist for particular business units or subsidiaries, those policies apply **in addition** to this Code of Conduct.

Violations of the Code of Conduct may result in disciplinary action for employees, including managerial staff, up to and including termination of employment.

All **managers with disciplinary responsibility** are required to:

- Communicate the principles of this Code to their teams,
- Ensure that every employee understands and follows the rules, and
- Monitor compliance within their areas of responsibility.

No employee will be disadvantaged for adhering to the Code of Conduct or for refusing to act in violation of it - even if this results in the loss of a business opportunity or other short-term disadvantage.

We encourage all employees and partners to **report any suspected violations** of this Code or of other COCUS policies. Reports will be treated confidentially and reviewed in accordance with established internal procedures.

By following this Code of Conduct, each of us helps to uphold the integrity, trust, and reputation that define COCUS.

For ease of reading, the masculine form is used throughout this document. All references to persons apply equally to all genders.