Code of Business Conduct and Ethics

CONDIS®

elvexys®

Contents

1. Message 1
2. Our responsibilities 1
   2.1. Company responsibilities 1
   2.2. Management responsibilities 1
   2.3. Employees responsibilities 2
3. Key global ethics policies summary 2
   3.1. Compliance and reporting 2
   3.2. In the workplace 2
      3.2.1. Conduct in the workplace 2
      3.2.2. Health, safety and the environment 3
      3.2.3. Protecting people 3
      3.2.4. Violence 3
      3.2.5. Substance abuse 3
      3.2.6. Company assets and ressources 4
   3.3. Information asset protection 4
      3.3.1. Protecting information assets 4
   Protect information assets 4
   Protect inventions, trademarks & works of authorship 5
   Third-party information 5
      3.3.2. Privacy and data protection 5
      3.3.3. Records management 5
      3.3.4. Scientific disclosure 6
      3.3.5. Use of electronic resources 6
   3.4. Transactions 6
      3.4.1. Financial responsibility and authorization 7
      3.4.2. International boycotts 7
      3.4.3. Money laundering 7
      3.4.4. Imports and exports 7
      3.4.5. Trade or economic sanctions 7
   3.5. Interactions with external parties 7
      3.5.1. Ethical interactions and external parties 8
      3.5.2. Anti-corruption 8
      3.5.3. Antitrust and competition 9
      3.5.4. Competitor trade secret information 9
      3.5.5. Conflicts of interest 9
      3.5.6. External communications 10
      3.5.7. Securities laws and trading 10
      3.5.8. Interactions with government and public officials 10

3.5.9. Social media 11
4. Employees penalties for violations 11
What is the Company disciplinary philosophy and for what could you be disciplined? 11
What is the nature and level of disciplinary action that may be taken? 11
Why do you not hear about disciplinary action that has been taken with respect to colleagues? 12
Are there any other types of penalties that could be imposed? 12

1. Message

Condis SA, a premium contributor to the global electrical grid with Swiss made products and solutions, is a world leader in the production and development of medium- and high-voltage products and solutions for electrical infrastructure. His daughter company, Elvexys SA, an expert in the digitalization of energy infrastructures, specializes in network data management and energy transmission and distribution network engineering.

The CONDIS Group's headquarters, composed of Condis SA and Elvexys SA (hereinafter, the "**Company**"), and the production facilities are based in Rossens in the canton of Fribourg with a representative office in Shanghai. Founded in Fribourg in 1903, Condis SA supplies state-of-the-art capacitors to the international major actors of the electricity market, totaling a current installed base of more than 400'000 units. Digitization, the increase in energy, reliability of grid infrastructure and reduction of the carbon footprint are the main challenges Condis faces in ensuring a more prosperous and safe future for generations to come. Elvexys SA, acquired by Condis in 2021, a specialist in energy digitalization allows our customers to accelerate their industrial communication projects by conceiving innovative and robust solutions.

The Code of Business Conduct and Ethics of Condis SA and Elvexys SA (hereinafter, the "**Code**") describes the core values and beliefs of the parent company and provides the foundation for all business conduct. Our guidelines for conducting the Company business are consistent with the highest standards of business ethics. If you have any questions about these guidelines, please contact the Human Resources Department.

This Code applies to all our directors, officers, employees, and agents, whether they work for Condis SA and Elvexys SA on a full-time, part-time, consultative, or temporary basis. We refer to all persons covered by this Code as "employees."

It is essential that each employee views these standards not as a burden but as a core part of values and understands that violations of these standards will not be tolerated. All Condis SA and Elvexys SA employees have a duty to report any known or suspected violation of this Code, including any violation of laws, rules, regulations or policies that apply worldwide. Reporting a known or suspected violation of this Code by others will not be considered an act of disloyalty, but an action to safeguard the reputation and integrity of Condis SA, Elvexys SA and its employees.

2. Our responsibilities

2.1. Company responsibilities

The Company is responsible for ensuring, through educational and training programs, that all employees are aware of and understand the Code described in this booklet. The Company will make available continuing counsel on the Company rules and regulations to any employee who seeks it. It is the Company responsibility to provide working conditions at all locations that are supportive of employee responsibilities under the Code.

The Company and all our employees are expected to observe a basic code of conduct in the workplace. It is essential that we be:

- Dedicated and loyal to the Company;
- Law-abiding and in compliance with applicable governmental rules and regulations;
- Honest and trustworthy;
- Responsible and reliable;
- Truthful and accurate;
- Cooperative;
- Economical in utilizing the Company and customer resources.

2.2. Management responsibilities

Employees who supervise others have an important responsibility to lead by example and maintain the highest standards of behavior. Supervisors are responsible for maintaining an environment in which employees understand their responsibilities

and feel comfortable raising issues and concerns without fear of retaliation. If an issue is raised, supervisors must take prompt action to address the concerns and correct problems that arise.

Supervisors must also make sure that each employee under their supervision understands the Code and the policies, laws and regulations that affect the Company workplace. Most importantly, supervisors must ensure that employees understand that business performance is never more important than ethical business conduct.

2.3. Employees responsibilities

Recognizing ethical issues and doing the right thing in all Company business activities is every employee's responsibility.

When engaging in business activities for the Company, consider the following:

- What feels right or wrong about the planned action?
- Is the planned action consistent with the Code and other Company policies?
- How will the planned action be perceived by your manager, the Company executives, the Board of Directors, or the general public?
- Would another person's input help to evaluate the planned action?

If it appears to one of us that a fellow employee may be in violation of this policy or other Company rules and regulations, we have the obligation to bring that situation to his or her attention and, if the violation is not corrected, to the attention of the Management Team or the Board of Directors.

3. Key global ethics policies summary

3.1. Compliance and reporting

Employees must comply with the Code as well as all Company policies and procedures, all laws and regulations that apply to the Company business operations, and all applicable official directives. Employees must also, subject to limits of local law, report any known or suspected violations. Employees must not retaliate against others for making such reports.

Issues can be most effectively resolved – and harm most quickly prevented or minimized – when the Company is made aware of known or suspected compliance violations. Employees may submit reports of potential violations or raise concerns in any of the following ways:

- Contact your supervisor if you are comfortable approaching him or her about any potential violation or concern. If the person whose behavior is an issue is your supervisor or is in your line management, you may choose to raise the issue with that individual directly; however, if you feel that he or she does not resolve your concern to your satisfaction, or if you are not comfortable discussing the situation with him or her directly, you must submit a report through another of the approved reporting channels listed below:
- Contact a member of the Management Team or a Human Resources Department Representative.

3.2. In the workplace

Each and every day that we conduct the Company business, our actions must be consistent with our values and with the Company brand. We must be reliable and trustworthy. We must carry out our daily responsibilities with a commitment to integrity and excellence. We must also reflect our commitment to respect for people through the way we treat one another, Company guests, and Company assets.

3.2.1. Conduct in the workplace

Employees must behave so that the workplace is free of improper conduct, harassment or any form of discrimination.

In your daily work activities, observe normal standards of courtesy and consideration when interacting with other employees and people with whom the Company has business dealings. Be sensitive to the concerns and values of others, and do not engage in improper conduct or harass another employee or person who has business dealings with our company. Some examples of improper conduct and/or harassment include:

- Jokes, insults, threats, and other unwelcome statement or actions about a person's race, color, gender, age, religion, national origin, ancestry, sexual orientation, citizenship, disability, veteran status, social or economic status or educational background;
- Unwelcome sexual advances, requests for sexual favors, and other unwelcome verbal or physical conduct of a sexual nature, or the display of sexually suggestive objects or pictures;
- Verbal or physical conduct that interferes with another's work performance or creates a fearful or hostile work environment.

3.2.2. Health, safety and the environment

The Company health and safety rules and procedures are designed to provide a safe and healthy work environment and meet applicable health and safety laws. Maintaining a safe and healthy work environment relies heavily on the choices and behavior of individuals.

Employees must exercise good judgment regarding the environmental aspects of our use of building and property, our manufacturing processes and our products. All necessary action must be taken to minimize or eliminate generation, discharge, and disposal of hazardous materials. We must comply fully with all federal, state and local environmental protection laws and the environmental programs and policies applicable for the Company facilities and the facilities of our affiliates. Any existing or potential violation of these laws should be brought immediately to the attention of the Management Team or the Board of Directors.

In the event of an emergency situation, employees should contact the Management Team or the Board of Directors. For non-urgent situations, employees should submit a facility work order.

3.2.3. Protecting people

Employees must take appropriate safety and security precautions to protect themselves, other employees, and guests. Employees must take appropriate safety and security precautions to prevent harm to people by maintaining a secure work environment, including being compliant with health, safety, and environmental requirements.

Employees are required to provide personal contact information and are strongly encouraged to provide backup third-party contact information in the Company systems of record to facilitate prompt communication between employees and management in case of emergency situations impacting employees and/or the Company. Employees must provide business-travel itineraries to management.

Employees are also encouraged to supply contact information when traveling for personal reasons. The Company may require employees who hold certain positions to supply such contact information.

3.2.4. Violence

We are committed to the safety of our employees and property. Threats, intimidation or violence in our workplace will not be tolerated. Employees may not possess firearms, other weapons, explosive devices or dangerous materials in the workplace without express prior authorization.

3.2.5. Substance abuse

The Company strives to maintain a workplace that is free from illegal use, possession, sale, or distribution of alcohol or controlled substances. Legal or illegal substances must not be used in a manner that impairs a person's performance of assigned tasks.

3.2.6. Company assets and ressources

In addition, all employees are expected to protect the Company assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company profitability. The Company property, such as office supplies, computer equipment, buildings and products, are intended to be used only for legitimate business purposes, although incidental personal use may be permitted. Employees may not, however, use our corporate name, any brand name or trademark owned or associated with Condis SA, Elvexys SA or any letterhead stationery for any personal purpose.

3.3. Information asset protection

One of the Company most important assets is our proprietary information. The success of our business depends on our ability to protect and properly use and effectively disclose, when necessary, the Company information assets. We must fulfill our obligation to be reliable and trustworthy by protecting confidential information entrusted to us by customers, business partners, and fellow employees who depend upon us to protect their data and privacy. As an employee of the Company, you may learn of information about the Company or third parties that is confidential or proprietary. You may also learn of important information before that information is released to the general public. Employees who have received or have access to such confidential information are required to keep this information confidential.

3.3.1. Protecting information assets

Employees must take appropriate precautions to protect and properly use and handle information assets of the Company and those entrusted to the Company by others. This includes following all copyright, trademark, privacy, data protection, and other legal and Company requirements.

Protect information assets

Identify and evaluate the risks to the Company as you make decisions that affect the Company information assets and information entrusted to the Company by others.

Take appropriate action to protect information assets. Safeguard the confidentiality, integrity, and availability of information assets by marking them appropriately, keeping them secure, and limiting access to those who have a business need to know and use them to do their jobs. When creating or modifying information, verify the accuracy of any resulting Company records.

Disclose information and records only with appropriate approvals, and to those who have a business need for it. If your job requires you to disclose the Company information to third parties, a confidentiality agreement may also be required, approved by the Management Team and signed by the outside party to whom you intend to disclose the information. In addition, special review and approval processes apply to disclosures that are made publicly or in a forum accessible by the public.

Confidential information includes any information developed by or for the Company relating to the Company business that is generally not known to the public and any confidential information that suppliers, customers, or business partners have entrusted to us. Examples of confidential information include: business, marketing and services plans, financial information, product architecture, source codes, engineering and manufacturing ideas, designs, databases, customer lists, pricing strategies, personnel data, personally identifiable information pertaining to our employees, customers or other individuals, and similar types of information provided to us by our customers, supplier and partners.

Be careful not to discuss confidential information in areas where you may be overheard and do not display it in areas that may allow inappropriate access to the information. For example, do not discuss or display confidential information in areas generally accessible to the public, including public areas in your place of work, as well as airports, airplanes, restaurants, lobbies, elevators, and restrooms.

Protect inventions, trademarks & works of authorship

All employees must protect the Company trademarks, copyrights and patents. Materials that can be protected by copyright include publications, documentation, training materials, computer codes and other works of authorship developed for the Company. You may also create, discover or develop software, methods, systems or other patentable inventions when performing your responsibilities or utilizing information or resources available to you in connection with your employment.

Employees must submit complete details about their Company-related inventions or works of authorship to the Management Team for study and review. You must cooperate fully in the protection of these inventions, ideas, and works, either by maintaining them as trade secrets or by obtaining patents on them, as decided at the Company discretion.

Third-party information

The Company and its employees must respect the intellectual property rights of others and refrain from these or other improper activities:

- Do not obtain confidential information of other parties by improper means or disclose it without authorization;
- Do not practice the patented technology of other parties without first obtaining a license from the outside party;
- Do not use any material copyrighted by other parties without first obtaining or confirming copyright permission;
- Do not seek trade secret information from individuals under obligations not to disclose such information or otherwise employ improper means or methods to obtain non-public competitor information.

In the case of property rights with an expiration date, such as patents, employees must be certain that the expiration date has passed if licensing or outright purchase is not feasible. All employees must refrain from infringing the intellectual property rights of others.

3.3.2. Privacy and data protection

Employees must protect personal information that could identify an individual. Employees must comply with all legal requirements and policies that apply to the collection, use, and retention of personal information.

Personal information is information about an employee, customer, contractor, or vendor.

Employees must collect, use, store, handle, and disclose individuals' personal information in accordance with the Company global and affiliate-based privacy and data protection laws and policies.

If you have any question regarding the collection, use, handling or disclosure of personal information, please contact the Human Resources Department for guidance.

3.3.3. Records management

Employees must comply with all Company records management and retention requirements, including the storage and disposition of Company records. You are responsible for proper management, including retention, protection, and disposition, of the Company records under your control, regardless of the media. You must store records in such a manner that the information is preserved for the period required by the Records Retention Schedule. It is equally important to appropriately dispose of material that no longer needs to be retained.

The Company does not knowingly destroy or discard evidence. Records relevant to a legal action cannot be destroyed or discarded without the approval of the Management Team. If the Company receives a subpoena, a request for records or other legal papers, or if we have reason to believe that such a request or demand is likely, the Company policy is to retain all records relevant to the matter. If you receive such a request or other legal papers, notify the Management Team immediately.

All Company records are the exclusive property of the Company and its affiliates.

3.3.4. Scientific disclosure

The Company approval is required prior to public disclosure of scientific information generated by or on behalf of the Company that communicates any aspect of the Company scientific research and development activities or describes how the Company conducts and manages its scientific processes and information.

Any proposed scientific disclosure must be consistent with an applicable data disclosure plan approved by the Management Team.

These policies apply when you author, present, or support the development or delivery of scientific disclosures such as:

- Journal articles and supplements (both print and electronic);
- Abstracts, posters, oral presentations;
- Slides, slide kits;
- Book chapters, lecture transcripts;
- Scientific symposia, symposia highlights/reviews;
- Editorials, perspectives;
- Book reviews, scientific reviews, invited reviews;
- Any type of brief, rapid, or expedited scientific communication.

3.3.5. Use of electronic resources

Use of the Company networks is both a necessity and a privilege. If you have access to our information systems and computer networks, you are responsible for adhering to the highest standards of behavior in all your usage and communications. When you access our networks from remote locations (for example, at home or from other non-company locations), you are subject to the same standards of use as are employees who access our networks while on company premises. Our networks and information systems are for legitimate company-related business purposes. Limited personal use may be acceptable if it is authorized by your work location and does not interfere with your job responsibilities. Employees must comply with the Company requirements for and restrictions on the use of electronic resources to protect information assets of the Company and those entrusted to us by others.

Use electronic resources (such as computers, e-mail, portable electronic devices, including cell phones, and the Internet) responsibly and in line with the law and Company values and policies. In particular:

- Use electronic resources for the business purposes of the Company;
- Use electronic resources securely (for example, do not share passwords, open suspicious e-mail attachments, or store Company related information on personal devices or media);
- Do not make changes to an electronic resource (such as disabling virus protection, installing prohibited software, or installing non-Company provided hardware);
- Do not use electronic resources to transmit, retrieve, view, store, or reproduce communications or material of a discriminatory, harassing, offensive or obscene nature.

Users are responsible for knowing and understanding the security requirements for the electronic resources they use. Security issues include access control, resource reliability, data security and disaster recovery.

3.4. Transactions

Various stakeholders, including shareholders, vendors, and those who purchase the Company products and devices, rely on the Company to be reliable and trustworthy in the way it carries out and documents its transactions. The Company is also required by law, including, specifically, securities laws, to maintain accurate books and records and a related system of internal controls. The policies described in this section govern Company transactions and the Company employees' actions relating to those transactions to ensure that they will be carried out in a compliant manner and with reliability and integrity. Please also see other related the Company and local policies and procedures.

3.4.1. Financial responsibility and authorization

Each Company employee must ensure that no false or intentionally misleading entries are made in the Company accounting records. Intentional misclassification of transactions regarding accounts, departments, or accounting periods violate the law and the Code. All transactions must be supported by accurate documentation in reasonable detail, recorded in the proper account and in the proper accounting period.

If any employee has concerns or complaints regarding questionable accounting, auditing or other financial records, he or she must report those concerns to the Management Team.

Employees must act with absolute financial and record-keeping integrity in processing travel and expense reports and other financial transactions. Employees must follow requirements regarding responsibility and approval for committing Company financial or other resources. Cash or other assets must not be maintained in any unrecorded or "off-the-books" fund for any purpose. Compliance with Generally Accepted Accounting Principles (GAAP) and the Company's system of internal controls is required at all times. Proper justification is required when alternative accounting treatment is possible under GAAP.

3.4.2. International boycotts

Employees must not engage in or agree to engage in any Company transactions or make commitments that would support a boycott of any country that is friendly to Switzerland or would otherwise violate applicable laws.

3.4.3. Money laundering

Money laundering is a process by which individuals or entities conceal unlawful or unreported funds, or otherwise make such funds appear legitimate. The Company does not condone, facilitate or support money laundering. Two areas that require special attention are unusual ways in which payments may be requested, and customers who appear to lack integrity in their operations. Be particularly alert for:

- Requests for cash payment, travelers checks or checks from an unknown third party;
- Complex payment patterns;
- Unusual transfers to or from countries not related to the transaction;
- Suppliers or customers who suggest any action to avoid recordkeeping requirements;
- Transactions involving locations previously associated with money laundering or tax evasion.

3.4.4. Imports and exports

According to Swiss law, the import, the export or the transit of certain goods or products are prohibited. For instance, this applies to narcotics and protected animal and plant species. Certain goods may be taken across the border only on a restricted basis or with a special permit, such as arms. The measures serve to protect the population, the environment, and the economy.

Before dealing with any person or entity that you have reason to believe may be associated in any way with any terrorist organization, you must consult with the Management Team.

3.4.5. Trade or economic sanctions

Employees must not engage in or agree to engage in Company transactions with individuals, entities, or countries against which the Swiss Government or any other government maintains trade or economic sanctions without first verifying with the Management Team that the transaction is permissible.

3.5. Interactions with external parties

The conduct of our business depends on effective interactions with external parties. We must earn, on a continuing basis, the trust and respect of all Company stakeholders, including those who regulate our business, use our products, invest in Company stock, supply the Company with goods and services, and those with whom we collaborate, by conducting our business ethically and legally. We must demonstrate the utmost integrity, transparency, and reliability whenever we conduct the Company business.

3.5.1. Ethical interactions and external parties

All employees must act ethically, and comply with all applicable laws, regulations, and industry codes of practice that govern the Company interactions with all external parties, including customers, suppliers, government and public officials, and private individuals.

The following is a list of examples when issues may arise:

- Conduct the Company business with government or public officials or private external parties;
- Attend, organize, or assist with Company meetings and events for government or public officials or private external parties;
- Engage in promotional or educational activities or the preparation or review of related materials;
- Engage in public relations activities on behalf of the Company;
- Make payments, or provide Company gifts, hospitality, or entertainment to external parties;
- Receive, review, or approve requests from external parties for grants or donations;
- Negotiate or contract for commercial transactions and discounts for Company products;
- Interact on behalf of the Company with professional associations, special interest, or other organizations;
- Organize Company international events or activities involving external parties;
- Have responsibilities regarding local policies that relate to interactions with external parties.

3.5.2. Anti-corruption

It is against the Company policy to make unlawful, improper or other kinds of questionable payments to customers, government employees or officials, or other parties. We do business and sell our products only on the merits of price, quality and service.

- Employees must act ethically in both the public and private sectors. Employees must not bribe government or public officials or private individuals;
- Employees must not give, offer, promise, or authorize any payment, benefit, or gift of money or anything else of value to a government or public official, directly or through a third party, to obtain or retain any business or secure any improper advantage;
- These same prohibitions apply to employee interactions with private individuals and employees of companies with which the Company has an existing or prospective business relationship.

Employees must never:

- Pay expenses that are excessive, lack adequate description or supporting documentation or appear to be improper;
- Make, disguise, or arrange to have made or disguised, or fail to correct or report, any false or artificial entries in any Company books or records, or in any books or records of other persons or companies with whom the Company does business;
- Omit, delete, or alter any entries in any Company books or records without following appropriate Company procedures applicable to that type of action.

Under the Company policy and the laws of various countries in which the Company operates, Company employees and third-parties acting on behalf of the Company must not:

- Offer, promise, or give or authorize the payment or gift of money or anything else of value to a government or public official, or to a family member of, or any other entity or individual on behalf of, or for the benefit of, a government or public official directly or indirectly through a third party for the purpose of:
    - Influencing an official act or decision of the government or public official;
    - Inducing the government or public official to do or omit to do any act contrary to his or her duty;

- Inducing the government or public official to use his or her influence to affect or influence any act or decision;
- Securing any improper advantage in order to obtain, retain, or direct business to any person or entity.

For further information on the definition of government or public official please consult the Management Team.

In addition, the Company is required to maintain a system of internal accounting controls, and make and keep books, records, and accounts which, in reasonable detail, accurately and fairly reflect Company transactions and the disposition of its assets.

With respect to such internal accounting controls, employees are responsible for:

- Making accurate and reasonably detailed entries in official records of the Company;
- Complying with the Company global and local accounting policies and procedures and other internal control requirements;
- Recording the Company transactions properly and correctly, regardless of magnitude.

3.5.3. Antitrust and competition

Antitrust and competition laws are intended to promote vigorous competition in a free market. It is in the Company best interest to promote free and open competition. The Company must make its own business decisions, free from understandings or agreements with competitors that restrict competition. While it is beyond the scope of this Code to explain the antitrust laws in detail, the Company considers compliance with these laws of vital importance. Employees must not engage in anti-competitive activities and must seek advice from the Management Team about any communications or situations that could potentially have an anti-competitive appearance.

This guidance applies when you:

- Deal with suppliers on behalf of the Company;
- deal with customers who sell Company products;
- Interact with representatives of Company competitors, especially at trade association events and meetings.

Antitrust and competition considerations are also relevant to certain joint activities with business partners; consult the Management Team needed.

3.5.4. Competitor trade secret information

Employees must not seek trade secret information from individuals under obligations not to disclose such information or otherwise employ improper means or methods to obtain non-public competitor information. For example, this could include situations in which an employee is seeking non-public information about competitors, working with consultants or vendors who also provide goods or services to competitors, or interacting with current or former employees of competitors.

3.5.5. Conflicts of interest

Employees are challenged to be alert to any situation that could compromise the position of trust they hold as a Company employee. Employees must avoid situations in which personal interests, outside activities or relationships conflict or appear to conflict with the Company interests. Employees must either decline involvement in situations that present potential conflicts of interest or request that the Company evaluates them by requesting a review of such potential conflict by the Management Team.

Examples of potential conflicts include:

- Outside employment – Participating in a business involved in any field related to the business of the Company or that may conflict with you performing your job at the Company, or working for an actual or potential competitor, supplier, or customer of the Company;
- Boards, panels, consulting arrangements – Acting as or accepting a position as an officer, advisor, consultant, or director of any business or organization involved in the electronics industry or doing business with the Company (such as a supplier or customer);

- Payment for services – Accepting from external parties any payment, significant goods, or services for activities such as authoring or editing publications, serving on advisory panels or boards, speaking, making or creating presentations, or participating in symposia or other professional or technical forums that are work-related;
- Relatives and close personal relationships – Conducting Company business with any relative or with a business with which you or a relative or domestic partner are associated;
- Gifts – Accepting gifts, entertainment, payment, or services from parties conducting business with or seeking to do business with the Company, including, for example, suppliers or potential suppliers of the Company;
- Investments and Ownership Interests – Investments or ownerships in companies that do or seek to do business with the Company or are competitors, or in property (such as real estate, patent rights, or securities) that the Company may have an interest in purchasing.

3.5.6. External communications

The Company approval must be obtained before communicating externally, in a public forum or any forum accessible by the public, any information related to the Company, its products, policies, or activities, or those of its competitors.

In some cases, employees must refer inquiries to others within the Company for appropriate handling. The type of approval or referral required varies according to the type of information and the intended audience. To determine which approval is required, please contact the Management Team.

3.5.7. Securities laws and trading

The Company shares information openly with its employees. At times, we may receive confidential company information before it is made publicly available to ordinary investors. Some of that information may be considered significant, or "material", and could be important to an investor deciding to buy, sell or hold securities.

Examples of information that could be material are:

- Information about possible business deals, such as a merger, purchase, sale or joint venture;
- Financial results or changes in dividends;
- Important management changes;
- Major raw material shortages or discoveries;
- Significant product or manufacturing process developments;
- Gain or loss of a significant customer or supplier;
- Major lawsuit or regulatory investigation;
- Any other information that may positively or negatively affect the stock price of the Company or any other company.

Do not use confidential information for personal benefit. Do not trade securities based on material inside information. Do not provide inside information to others. Employees may not purchase or sell Company stock or transfer stock into or out of the Company stock funds in any company savings plan or other benefit plan during announced Trading Black-Out Periods. Even if you are not covered by formal blackout restrictions, you are encouraged to wait until at least 24 hours after material inside information has been publicly disclosed before trading to ensure the market has had an opportunity to absorb and evaluate the information.

3.5.8. Interactions with government and public officials

Employees must be truthful and accurate and conduct themselves in a lawful and respectful manner when communicating and interacting with representatives of government agencies, ministries, and public entities. Employees must observe the highest ethical standards and comply with all applicable laws and regulations when conducting business with government and public officials. You must submit accurate, complete information to government agencies or representatives.

Generally, you should not contact such officials on behalf of the Company unless specifically authorized by the Company. If employees are contacted by such representatives, or have a need to initiate communications with them, the communications should be channeled through appropriate Company personnel.

3.5.9. Social media

The Company recognizes that Social Networking (such as personal web sites, blogs, Facebook, LinkedIn, Twitter, Google+, online group discussions, text messaging, message boards, chat rooms, etc.) can be used by employees for personal as well as business purposes. The Company also understands how the use of internet social network sites and blogs can shape the way the public views our products, employees, vendors, partners and customers. The Company respects the right of any employee to maintain a blog or post a comment on social networking sites. However, we are also committed to ensuring that the use of such communications serves the needs of our business by maintaining the Company identity, integrity, and reputation in a manner consistent with our values and policies. Therefore, we have established the following guidelines for communicating the Company-related information via Social Media forums whether used in or outside the workplace. The simple rules of thumb are to keep on-topic and be respectful of others. When representing the Company toward external parties or when using the Company assets, employees must not provide content which contains any of the following material:

- Material that infringes the copyright of another person (plagiarism or passing off other people's material as your own) or copyright material not referenced or acknowledged;
- Unauthorized posting of personal information (names, address, phone number, email, etc.) of other users;
- Material that contains vulgar, obscene or indecent language or images;
- Material which defames, abuses or threatens others;
- Statements that are bigoted, hateful or racially offensive;
- Material that advocates illegal activity or discusses illegal activities with the intent to commit them;
- No Flaming; there is a difference between voicing a legitimate concern or grievance and simply badmouthing or some other form of written abuse of someone or some service. These will be deleted upon discovery;

If you believe that a company employee has provided content which falls into one of the categories above in a manner which ties the Company to the content provided, then please contact the Management Team.

4. Employees penalties for violations

What is the Company disciplinary philosophy and for what could you be disciplined?

The Company provides performance management, coaching, and feedback tools to help employees link their work efforts to the priorities and business goals of the Company and to demonstrate successful performance. Discipline is an additional tool the Company uses to correct behavioral or performance issues.

Examples of employee behaviors or activities that could result in disciplinary action include, among others:

- Authorizing or participating in an activity that results in a violation of the law, the Code, the Company policies or procedures, or an official order or consent decree;
- Failing to report a violation or suspected violation (except where reporting is prohibited by local law);
- Refusing to cooperate with the investigation of a suspected violation;
- Retaliating against an individual who reported a suspected violation;
- Failing to complete required training;
- Performing in a manner that doesn't meet job expectations;
- In the case of a supervisor, failing to detect a violation if this resulted from inadequate supervision.

What is the nature and level of disciplinary action that may be taken?

Circumstances vary in each case involving the potential for disciplinary action by the Company; therefore, each situation is handled individually. The nature and level of any action taken will depend on the:

- Nature and severity of the problem;
- Expectations of the position;
- Circumstances involved.

If disciplinary action is warranted, subject to local law, it may range anywhere from a warning to termination of employment. Please discuss any questions with your supervisor and/or your human resources representative.

Why do you not hear about disciplinary action that has been taken with respect to colleagues?

The Company believes that its values of integrity, respect for people, and excellence should be evident in the way disciplinary investigations and decisions are implemented. Where possible, the Company strives to keep any disciplinary process a confidential matter between the involved employee, the supervisor, and human resources. The goal is to increase the chance that an employee subject to disciplinary action has the opportunity to return to successful performance. The Management Team may from time to time publish actual examples of situations involving compliance failures in order to promote shared learning. These examples may include information about disciplinary actions but will be anonymous to protect the identity of the employees involved.

Are there any other types of penalties that could be imposed?

In extreme situations involving noncompliance, a government may choose to take action against individual employees as well as the Company. The potential consequences vary according to local law and the type of alleged violation. The penalties may be severe, and could include criminal fines, imprisonment, and an official prohibition from working in the electronics industry or engaging in international transactions for the sale of goods.

Rossens, March 2nd, 2021

CONDIS SA

Per H. Dybwad
Executive Chairman

Didier Wuilloud
Administration and Finance Director