Group Whistleblowing Policy

First publication	: February 2016
Current publication	: January 2023
Version	: 5
Document type	: Policy
Scope	: Global

Life Is On | Schneider Electric

Policy name: Group Whistleblowing Policy

Purpose:

- Explain how employees, interns and contractors, and external stakeholders of Schneider Electric can report concerns about suspected misconduct in confidence and without fear of retaliation;

- Describe what employees, interns and contractors, and external stakeholders of Schneider Electric can expect if they report such a concern.

Legal framework: As Schneider Electric is a French group, this policy complies with the principles of the European Directive on Whistleblower's protection[1] and requirements set out by French law[2]. All entities and subsidiaries controlled by Schneider Electric must comply with this policy regardless of where they are established or operate from, except to ensure compliance with local law and regulations. In such circumstances, adaptations of the policy will be made by the relevant Regional Compliance Officer with legal support; in cases when local adaptations are necessary, the final local policies will be validated by the Chief Compliance Officer.

Related documents:

- Trust Charter;
- Case Management & Investigation Policy;
- Internal Investigation Guide;
- Data Privacy notice available on our Trust Line page.

Audience: All employees, interns and contractors, and external stakeholders of Schneider Electric and its subsidiaries

Content:

Confidentiality Status: Public

Local adaptation authorization: Possible to ensure compliance with local law and regulations. Local adaptations, when needed.

Document Owner: Audrey Morin, Group Compliance Director

Document Reviewers:

Pascale Gelly, Group Data Protection Officer

Sandrine Reinneis, Group HR Compliance Officer

Pierre Lormeau, Fraud Examination Director

Peter Wexler, SVP Group Chief Legal Officer

Pierre Levêque, SVP Group Internal Audit & Control

Nicolas Vlieghe, SVP Group Chief Compliance Officer

Karine Armand-Fedida, SVP Total Rewards & Performance

Document Approver: Hervé Coureil, EVP Chief Governance Officer and General Secretary

[1] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019

[2] Law No. 2016-1691 of 9 December 2016, modified by Law No. 2022-401 of 22 March 2022, and Law no. 2017-399 of 27 March 2017

1. Definitions

Concern – Allegation made by a Reporter about a conduct.

Alert – Concern assessed as a potential Misconduct resulting from the activities of Schneider Electric and its subsidiaries, as well as the activities of subcontractors and third parties with whom Schneider Electric maintains a business relationship.

Non-Alert – Concern not assessed as a potential Misconduct resulting from the activities of Schneider Electric and its subsidiaries, as well as the activities of subcontractors and third parties with whom Schneider Electric maintains a business relationship.

Misconduct – Violation of laws and regulations, and/or our Trust Charter and group policies.

Reporter (or "Whistleblower") – Anyone who wishes to report a Concern in good faith about a potential Misconduct.

Reported Person – Person identified by a Reporter as having committed a potential Misconduct.

2. What is Whistleblowing?

Whistleblowing corresponds to **all methods of reporting** available to employees, interns or contractors, and external stakeholders **to report on a voluntary basis a potential Misconduct**.

As a worldwide company, Schneider Electric (the Company) is committed to conduct business with integrity, by upholding strong ethical values. That is why this Policy aims to encourage employees and others stakeholders who have ethical concerns to come forward and voice those concerns. Indeed, employees, interns or contractors, and external stakeholders are often the first to realize when there might be something seriously wrong. Whistleblowing is viewed by Schneider Electric as a positive act that can make a valuable contribution to the Company's efficiency and long-term success.

3. Who can report a Concern?

The Reporter may be **any individual** who wishes to report a Concern in **good faith**. He/she can thus be:

- Internal: employees, interns and contractors working for the Company or one of its subsidiaries;
- External: anyone in relations with the Company such as third parties (e.g. supplier, customer, client/distributor representative, consultant, former or prospective employees, shareholders) or who are impacted by the Company's activities such as representatives of local communities and non-governmental organizations.

Good faith - Malicious allegations

It is expected good faith from Reporter's end when reporting Concerns, i.e. he/she must have the reasonable belief that the facts are true to the best of his/her knowledge at the time he/she reports them.

Any Concern will be handled with particular care to identify or avoid any malicious or bad faith reporting. Appropriate disciplinary action could be taken in accordance with the local disciplinary procedure against any person who is found to have raised a Concern in bad faith or by intentionally providing false information.

No sanction will be taken against any person who has reported a Concern in good faith, regardless the investigation outcome, and to the best of their knowledge at the time of reporting.

4. What Concerns can be reported?

The Reporter can report a Concern about potential Misconduct, i.e. **a suspected violation of**:

- **Laws and regulations**; or
- Our **Trust Charter** and **group policies**.

Such suspected violation may result from the activities of the Company and its subsidiaries, as well as the activities of subcontractors and third parties with whom the Company maintains a business relationship. A Concern assessed as a suspected Misconduct **will be qualified as an Alert**.

An Alert is categorized as follows:

- Fraud & Business Misconduct: Antitrust and non-competitive behavior, Asset misappropriation, Bribery & Corruption, Conflicts of Interests, Fraudulent statement, Insider trading and violation of securities law, Money laundering, Sanctions & Export Controls;
- HR & Workplace Violation: Discrimination, Disrespectful behavior, Harassment, Health & Safety, Sexual harassment, Unfair treatment, Violation of human rights, Violation of labor laws, Violent behavior;
- Other Misconduct: Grey Market, Environmental issues, Quality issue, Other.

The definition of each type of issue can be found in Appendix 3.

IMPORTANT: The Reporter cannot mention information in his/her report covered by (i) national defense secrecy, (ii) medical confidentiality, (iii) legal privilege (iv) confidentiality linked to prosecutions, (v) secrecy of legal proceedings and (vi) judicial deliberations secrecy.

5. How and when to report?

5.1. What are the reporting channels?

Reporters may report Concerns about potential Misconduct through a variety of channels, either by contacting an appropriate person in the Company and/or using the Trust Line, Schneider Electric's whistleblowing system:

- **Appropriate persons**:

  The Reporter may contact in writing or orally:

- A trusted manager;
- A HR Business Partner;
- A Legal Counsel;
- A Regional Compliance Officer.

If the recipient of the Concern assesses it as an Alert as defined in section 4, he/she must ensure the case is reported in the Trust Line, either by advising the Reporter to report directly or by doing it him/herself or by escalating to the Regional Compliance Officer. In case the recipient intentionally does not report the Concern, this may be considered a severe omission and/or, potentially, as a form of retaliation, which may lead to disciplinary action against the recipient. For more information, refer to the Case Management & Investigation Policy.

IMPORTANT: The Reporter has a choice to request a meeting with an appropriate person to report orally through face-to-face meeting, telephone or any other voicemail system (e.g. Teams). The appropriate person will have to meet the reporter within 20 working days after receipt of the request.

WARNING! When there is an emergency (such as an immediate threat to life or property), the Reporter should directly contact the relevant Regional Security Officer, Compliance Officer, Safety Officer, or local authorities.

- **Trust Line**:

The Reporter may use Trust Line, Schneider Electric's whistleblowing system, which is available:

- online: https://www.se.com/ww/en/about-us/sustainability/responsibility-ethics/trustline/
- or by phone: phone numbers available on https://www.se.com/ww/en/about-us/sustainability/responsibility-ethics/trustline/ and on posters displayed on the Company's sites.

It is a digital platform, available 24 hour a day, 7 days a week, managed by an independent third-party company. Reports can be done in the local and/or official language where Schneider Electric has business. This is a confidential and encrypted reporting channel. When accepted by local legislation, the Reporter can choose to report in a totally anonymous manner. Anonymity is fully respected by the set-up of Trust Line, which prevents knowing the identity of the Reporter.

Reports received outside of Trust Line and appropriate persons

No other internal reporting channel exists in Schneider Electric, except the ones recognized in local laws (e.g. employees' representatives). All Concerns about potential Misconduct received by any employee outside of the Trust Line and appropriate persons must be immediately forwarded to the Regional Compliance Officer for assessment and potential investigation.

Ethics Delegates

The Company has appointed Ethics Delegates as a further point of contact for employees, interns and contractors to help them with any questions about Trust Charter, Compliance Policies and about on how to report a Concern, including how to use of the Trust Line.

5.2. What kind of information needs to be provided?

When a Reporter reports a Concern about a potential Misconduct, he/she should provide at least a **description of the situation at stake** (date, time, location, general nature of the Concern, names of person(s) involved, etc.) and, if possible, **any additional relevant information** (names of possible witnesses, documents, etc.) to facilitate the assessment of his/her Concern. A reported Concern can be managed more efficiently if it contains sufficient factual information and clear access to further data for assessment and/or investigation purpose.

Is it possible to report a Concern when all the facts are not known?

If someone is aware of a potential Misconduct and acts in good faith (see section 3), he/she should report it with the facts that he/she is aware of. It is not expected from the Reporter to know all the information at stake, and he/she does not have to prove that the Concern is a founded Alert, as it is up to the Company to do so.

People should not investigate the matter themselves and seek evidence. The Company guarantees that no disciplinary measures or other steps will be taken against a Reporter if his/her reporting Concern later turns out to be mistaken or misguided.

6. What happens after a Concern is reported?

Any reported Concern will be managed according to the Case Management & Investigation Policy. The Case Manager and investigator(s) are bound by the following principles from assessment of the case to closing of it: neutrality, impartiality, independency.

6.1. Step 1: Reception

All reported Concerns are logged into the Trust Line, our whistleblowing system. Access to the cases reported into the Trust Line is restricted to a limited Compliance audience: the relevant Regional Compliance Officer, the members of the Group Operational Compliance Committee and the Compliance administrators of the Trust Line tool.

Group Operational Compliance Committee

The Group Operational Compliance Committee is Schneider Electric's internal authority in charge of detecting and supervising cases of non-compliance with the Ethics & Compliance program, and of reviewing monthly the effectiveness of the whistleblowing system.
It is composed of the following members: Chief Compliance Officer (Committee Secretary), Chief Legal Officer, Group Internal Audit & Control Officer, Group Compliance Director, Group HR Compliance Officer, and Head of Fraud Examination Team.

The Company takes every reported Concern of potential Misconduct seriously. Whether the Concern is reported orally or in writing, the Reporter will receive a written acknowledgement of receipt within 24 hours.

When the Reporter chooses to report a Concern anonymously, he/she will be given access to an anonymous messaging platform through the Trust Line tool. All interactions and information sharing will take place on this platform; without the Reporter's credentials ever being asked or disclosed.

6.2. Step 2: Initial Assessment

The Concern will be assessed by the relevant Regional Compliance Officer, who will confirm the qualification of the Concern as an Alert or not and notify the Reporter accordingly with justifications. If the Concern is qualified as a valid Alert, it will be appropriately investigated. If the Concern is not qualified as a valid Alert, the Concern will be closed, the Reporter will be informed in writing and, if necessary, referred to the relevant organization likely to help him/her.

6.3. Step 3: Investigation of a valid Alert

The Alert is managed by a Case Manager who can be, depending on the nature, urgency and potential impact of the Concern: the relevant Regional Compliance Officer who works under the supervision of the Group Operational Compliance Committee, or directly by the Group Operational Compliance Committee in case of high severity (severity criteria defined by the Case Management & Investigation policy).

The Case Manager can lead the investigation or assign an investigation team, at discretion and after critical evaluation, composed of people trained in conducting internal investigations. If needed, any external or internal experts (e.g. lawyers or accountants) can be mandated to support the investigation. All investigators and supports work under strict confidentiality. To secure safe, respectful and inclusive collaboration, the Case Manager may also propose intervention of an internal or external mediator to help rebuild respectful collaboration.

WARNING! No one beside the nominated investigation team is entitled to conduct investigation, interfere with an investigation, nor to gather any evidence or supporting documents related to the Concern if not entitled to do so.

6.4. Step 4: Post-Investigation

Once its investigation is complete, the investigation team will submit an investigation report, possibly including recommendations, to the Case Manager. If an Alert is founded (i.e. Misconduct is confirmed), the Case Manager may take steps to ensure that appropriate measures may apply depending on local disciplinary policies and law. They can take the form of:

- disciplinary measures decided by the relevant managers together with Human Resources, or by the Group Disciplinary Committee for the most sensitive alerts;
- remediation measures (such as launch a specific audit, review a process, perform training, etc.).

In addition, external actions can be taken, such as entering civil litigation or similar legal proceedings.

At discretion and after critical evaluation, the Case Manager can appoint people for next steps following the closing of the case, such as the monitoring of the proper execution of the measures decided.

Group Disciplinary Committee

The Group Disciplinary Committee is in charge of levying sanctions and remediation actions on serious non-compliance cases confirmed by the Group Operational Compliance Committee.

It is composed of the following members: Chief Governance Officer & Secretary General, Chief Human Resources Officer, Chief Compliance Officer (Committee Secretary), Chief Legal Officer, and one rotating member.

7. Rights and responsibilities of people involved

7.1. Rights & Responsibilities of the Reporter

Anonymity

When reporting a Concern into the Trust Line, the Reporter may choose to do so anonymously, except in countries where it is not possible because of local regulations. The Reporter will then be able to communicate with the Case Manager and/or appointed investigator(s) through an anonymous messaging platform available in the Trust Line tool. It is a secure channel protecting anonymity when parties exchange on a Concern.

Confidentiality

The identity of the Reporter is kept confidential and may only be accessible to the restricted list of persons involved in the case management (subject to obligations arising from the law or the applicable legal proceedings): the relevant Regional Compliance Officer, the members of the Group Operational Compliance Committee, the Compliance administrators of the Trust Line tool, the appointed investigator(s), and any external or internal person mandated to support the investigation or next steps following the closing of the case. No one else must be informed.

The identity of the Reporter must be kept confidential at any circumstances (regardless of the job position or seniority in the Company) and, if necessary for the investigation to inform another person, the Case Manager should be consulted and approve. An unauthorized disclosure may lead to disciplinary actions.

In all cases, the identity of the Reporter will not be provided to the Reported Person, unless expressly agreed by the Reporter or required by law or in the framework of legal proceedings.

Good faith

It is expected good faith from Reporter's end when reporting Concerns, i.e. he/she must have the reasonable belief that the facts are true to the best of his/her knowledge at the time he/she reports them. For more information, refer to section 3.

Non-retaliation

Schneider Electric has a zero-tolerance policy against retaliation, therefore prohibits retaliation or other discrimination against anyone who reports in good faith. Protection applies even if the alleged violation is unfounded after investigation is closed.

The Non-Retaliation Procedure is detailed in Appendix 2.

Right to information

The Reporter will be regularly informed – no later than 3 months after the acknowledgment of receipt of the Concern – about the outcome of the assessment and, if any, the progress of the Alert management. The Reporter is informed in writing when the Alert is closed. However, for reasons of confidentiality, privacy and the legal rights of persons involved, full details of the investigation and outcome may not be shared with the Reporter.

Protection & Care

In the course of the investigation, specific measures can be offered to the Reporter, in case he/she needs and as per local legislation, such as:

- Security measures (distancing)
- Accommodations
- Flexible Time management
- Change of function/service
- Mediation
- Psychological support

Privacy

The Company is committed to protecting the privacy of the Reporter. It implements organizational and technical measures in order to protect personal information from unauthorized access and processing. Any personal information obtained in the framework of this Whistleblowing Policy will only be used for the purposes explained in this Policy or to comply with the law. Please find more details on the protection of personal information in Annex 1.

7.2. Rights & Responsibilities of the Reported Person, witnesses and all third parties mentioned in the report

Confidentiality

All persons involved are entitled to confidentiality in order to avoid unnecessary damage to their reputation. Therefore, the identity of the Reported Person, the facts reported, and the subsequent investigation and findings are kept confidential and limited to the strict necessity of the management of the Concern (subject to obligations arising from the law or the applicable legal proceedings).

Information shared must be kept confidential at any circumstances (regardless of the job position or seniority in the Company) and, if necessary for the investigation to inform another person, the Case Manager should be consulted and approve. An unauthorized disclosure may lead to disciplinary actions.

Cooperation

If a Schneider Electric employee becomes involved in an investigation, he/she must cooperate in good faith and answer all questions completely and honestly. Lying to the people performing the investigation as well as delaying, interfering with or refusing to cooperate with an investigation may lead to disciplinary measures. In addition, it is strictly forbidden to willfully destroy documents, tamper with information, interfere with or threaten witnesses, intentionally mislead investigators, or block an investigation in any way.

WARNING! People external to Schneider Electric involved in the investigation (including, but not limited to former Schneider employees) are not obliged to cooperate with an internal investigation. It is voluntary and entirely at their discretion.

Non-retaliation

The non-retaliation protection mentioned in section 7.1. about the rights of the Reporter is also extended to the following persons:

- "Facilitators", i.e. anyone who helped the Reporter in the reporting process (e.g. obtaining the information, evidence, etc.);
- Investigation cooperators (e.g. witnesses);
- People connected with the Reporter and who could suffer retaliation in a work-related context (in particular co-workers);
- Legal entities that the Reporter owns, works for or is otherwise connected in a work-related context.

Protection applies even if the alleged violation is unfounded after investigation is closed.

Right to information

All persons involved in an investigation have the right to know the reasons for their involvement in the investigation and the investigation process. Depending on the needs of the investigation, they are kept regularly informed of its progress.

Presumption of Innocence

The presumption of innocence is guaranteed. Any individual involved and/or suspected of a potential Misconduct cannot be considered to have committed such a Misconduct until it has been established otherwise by investigation. Nevertheless, in case of founded Misconduct with regards to Trust Charter and group policies, an employee can be subject to disciplinary measures (up to termination) as per his/her employment contract and related duties, in respect with local labor laws and regulations.

Protection & Care

In the course of the investigation, specific measures can be offered to the Reported Person and witnesses, in case they need and as per local legislation, such as:

- Security measures (distancing)
- Accommodations
- Flexible Time management
- Change of function/service
- Mediation
- Psychological support

Privacy

The Company is committed to protecting the privacy of everyone involved. It implements organizational and technical measures in order to protect personal information from unauthorized access and processing. Any personal information obtained in the framework of this Whistleblowing Policy will only be used for the purposes explained in this Policy or to comply with the law. Please find more details on the protection of personal information in Annex 1.

8. In case of doubt

If in doubt about any aspect of this Policy, employees should seek advice from their line manager, HR Business Partner or Ethics Delegate or contact their Regional Compliance Officer. Their contact information is available on Schneider's Ethics & Compliance intranet page.

Annex 1: Protection of Personal Information

The handling of Concerns and Alerts involves the processing of personal information as described in this Group Whistleblowing Policy. To enable the raising of Concerns in confidence, an online platform is provided by a third party on behalf of Schneider Electric, using such degree of care as is appropriate to prevent risks of unauthorized access, use or disclosure. It is implemented by Schneider Electric Industries SAS and its affiliates to comply with a legal obligation and to pursue the legitimate interest of the group in order to ensure a trust environment within the group, maintain the reputation of the group and ensure a consistent approach in dealing with reports across the group. Information may also be processed for statistical purposes in order to further improve the platform and the management of concerns reported, in the legitimate interest group.

Categories of processed personal information

The following data are collected to manage and investigate Alerts:
- Identity, job position and contact details of the person issuing a Concern;
- Identity, job position and contact details of the person(s) against whom the Concern is issued;
- Identity, job position and contact details of the persons involved in collecting or processing the Concern;
- Reported facts;
- Information collected as a result of investigation;
- Investigation reports;
- Action(s) taken in response to the Alert.

Sharing of personal information

Concerns and Alerts are managed as described in this Policy. Schneider Electric being a global company, teams involved in the processing may have global or multi-country roles. These teams and our suppliers can be located anywhere where Schneider Electric operates. In such cases, we take measures to ensure that your personal information receives an adequate level of protection, which include Standard Contractual Clauses and our Binding Corporate Rules.

Personal information may be disclosed to the police and/or other enforcement or regulatory authorities. For example, if the alleged facts are related to a criminal prosecution, or in the context of a control carried out by public authorities.

Privacy Rights

The Reporter, the Reported Person and any person involved in the Alert have a right of access to their personal information and rights of rectification, deletion, restriction to the processing of personal information which can be exercised by contacting group.compliance.team@schneider-electric.com.

Questions or comments about Schneider Electric data processing activities under the Group Whistleblowing Policy can be addressed to our Group Data Protection Officer (Group DPO) at DPO@schneider-electric.com. A person believing that personal information has been processed in violation of applicable law may file a complaint with the Group DPO or with a supervisory authority.

Data retention

In case of Concerns not validated as Alerts, the Group Operational Compliance Committee or Regional Compliance Officers must without undue delay delete them or anonymize them by deleting any personal information if they need to keep Concerns for statistic purpose.

If after investigation, alleged Misconduct is unfounded, the Alert must be anonymized within two months following the closure of the investigation.

If after investigation, alleged Misconduct is founded but there is no disciplinary action neither legal proceeding initiated, the Alert must be anonymized within two months after the closing of any remediation actions decided.

If after investigation, alleged Misconduct is founded and there is disciplinary action and/or legal proceeding initiated, the Alert must be anonymized after all rights of appeal have been exhausted or following the final court decision.

The Group Operational Compliance Committee and Regional Compliance Officers are responsible to ensure compliance with the rules above. They may decide to archive an alert instead of anonymize it for the following reasons: (i) to comply with applicable legal requirements, (ii) to protect the Reporter from retaliation until the risk is properly handled, or (iii) to ensure that findings of the investigation are available for request by public authorities. Access to the archived Alert will be subject to prior validation by the Group Operational Compliance Committee. It will have to be justified by (i) one of the grounds for archiving the personal information, (ii) a request by an individual on the basis of personal data protection rights, or (iii) an existing or potential legal action initiated by or against Schneider Electric.

Annex 2: Non-Retaliation Procedure

1. Risk identification

When receiving a Concern, the relevant Regional Compliance Officer shall analyze if there is any retaliation risk. If this is the case, he/she may decide specific risk management and/or care measures.

During the investigation and after the case is closed, a Reporter, a victim or any other person protected against retaliation (as explained in section 7.2) who feels or is afraid to be retaliated against can report the situation through the Trust Line or directly by informing the Regional Compliance Officer.

2. Risk management

When the retaliation risk is confirmed, specific protection measures may be proposed by the Regional Compliance Officer with the relevant management and Human Resources, subject to the person's consent, such as:

- temporary or permanent reassignment (e.g. work from home);
- change in reporting line;
- placement on special leave with full pay;
- engagement with the manager or Human Resources Business Partner to ensure monitoring of the workplace situation;
- rescission of the retaliatory decision, including reinstatement;
- transfer of the person who allegedly is engaged in retaliation (subject to local regulations and internal rules).

In addition, a follow-up by the Regional Compliance Officer or the Group Operational Compliance Committee will be performed after 6 months of the closing of the investigation in order to make sure that recommended actions have been applied and there has been no retaliation (see Case Management & Investigation Policy).

Employees who carried out retaliation may be subject to disciplinary actions, including employment termination.

Annex 3: Definitions of Alert Types

FRAUD & BUSINESS MISCONDUCT	
Antitrust and non-competitive behavior	Practice that prevents or reduces competition in a market.
Asset misappropriation	Asset misappropriation schemes include both the theft of company assets, such as cash or inventory, and the misuse of company assets, as follows: - Theft of assets: it is any stealing or misuse of Schneider Electric's tangible or intangible (proprietary data, patents, etc.) assets without permission. - Fraudulent disbursements: When an employee uses his position of employment to cause a payment for some inappropriate purpose. The perpetrator has taken money from his employer in such a way that it appears to be a normal disbursement of cash, as follows, but not limited to: • Billing schemes: For example, when an employee divert cash through overbilling the company in collusion with a vendor or through payment of products or services not delivered or not rendered by the vendor, • Payroll schemes: For example, when disbursements are made as payments of wages to ghost employees, or through falsified working hours or timecards for workers, • Expense reimbursement schemes: An employee submits falsified expense claims as to generate fraudulent disbursements. - Embezzlement is the fraudulent misappropriation of goods of another by a person to whom it has been lawfully entrusted or to whom lawful possession was given. If a plant manager diverts cash through a billing scheme it will be considered as an embezzlement. If a worker steals product from the stock it will be considered as a theft.
Bribery & Corruption	Abuse of entrusted power for private gain and it can take many forms, including bribery. Bribery can be defined as the offering, promising, giving, accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust. Inducements can take the form of gifts, loans, fees, rewards or other advantages (taxes, services, donations, favors, etc.).
Conflicts of Interests	It is when an employee's personal interests' conflict with those of Schneider Electric. In other words, it is the situation in which the personal interests of an employee are likely to affect his decision in the performance of his professional duties. It includes favoritism, which is a practice of giving unfair preferential treatment to one person or group at the expense of another.
Fraudulent statement	Fraudulent statement schemes are intentional false statement or misrepresentation of the facts made with the intent to deceive another party, as follows: - Financial statement fraud: It is the deliberate misrepresentation of financial conditions and operating results of an enterprise or entity including concealment of liabilities and omission of disclosures. It can be a way to deceive financial statement users, particularly investors and creditors as to increase stock value or obtain, for example, more favorable financing conditions. The outcome of financial processes are the financial statements which include the balance sheet, the statement of income (P&L statement), statement of cash flow, etc. plus the accompanying explanation notes and disclosures. In addition, it may be deliberate misstatement or omission of amounts or disclosure of financial statements to deceive financial statement users, particularly investors and creditors. - Accounting fraud/manipulation: Intentional misrepresentation or alteration of journal entries and accounting records regarding sales, revenues, expenses, assets or liabilities for example. When the amounts manipulated are small there may be no impact on the financial statements. • It may be a way for local management to reach the objectives and get better incentives, • It is also a way to conceal a fraud scheme such as a fraudulent disbursement or a theft of products from the inventory. - Falsification of document: Act of intentionally changing or modifying information on a document with the intention of misleading company's stakeholders, authorities or regulatory bodies.
Insider trading and violation of securities law	Practice in which securities or trading laws have been violated, including insider trading. Insider trading can be defined as practice of purchasing or selling a publicly traded company's securities while in possession of material information that is not yet public information. Material information refers to any and all information that may result in a substantial impact on the decision of an investor regarding whether to buy or sell the security.

Money laundering	Process by which criminal proceeds are "cleaned" so that their illegal origins are hidden. It is usually associated with the types of organized crime that generate huge profits in cash, such as fraud.
Sanctions & Export Controls	Laws and regulations published by various regimes that are intended to protect and enforce national security, foreign policy and local country economic interests. Behaviors, transactions, and business dealings are subject to Sanctions and Export Control Regulations. Failure to abide by local country regulations may result in restriction or suspension of economic or commercial relations (or other areas) with a particular country or groups of individuals and entities imposed by law, or regulations relating to the shipment or transfer, by whatever means, of items, software, technology, or services out of a territory.

HR & WORKPLACE VIOLATION	
Discrimination	Any behavior or decision that involves treating someone unfavorably because of a personal characteristic which can include (but not limited to): • a disability or temporary disability • a disease or injury • parental status • skin color, descent, national origin, or ethnic background • generation • sex, including pregnancy, childbirth, or related medical conditions • gender or gender identity • membership to an industrial organization, like a trade union • religion • nationality, immigration status, citizenship, or ancestry • sexual orientation • marital status • political opinion • socio-economic background • medical record
Disrespectful behavior	Any attitude/act that shows a lack of respect. This includes verbal or non-verbal, abusive or insulting words, or rude behaviors. It includes also bullying which is a repeated and intentional behavior intended to cause fear, distress, hurt or harm to another person's body, emotions, self-esteem or reputation.
Harassment	Any offensive, inappropriate, unwelcomed, or even inadvertent behaviors at the workplace, that has the effect of violating a person's dignity or creating a degrading, humiliating or offensive/hostile work environment.
Health & Safety	Any practice that does not ensure that a safe and free environment at work is maintained at all times. It relates to both your physical health and your mental health.
Sexual harassment	Any unwelcomed sexual conduct (physical, visual, verbal or written) which affects an individual's dignity and creates an intimidating, hostile or uncomfortable working environment.
Unfair treatment	Any unfair or non-equal treatment with no fair procedure.
Violation of human rights	Behavior that endangers the basic rights and freedoms that belong to every person in the world, from birth until death. The Universal Declaration of Human Rights, adopted by the United Nations on 10 December 1948, sets out the basic rights and freedoms that apply to all people. For discrimination or any type of harassment, use specific issue.
Violation of labor laws	Actions by employers that violate labor laws.
Violent behavior	Any aggressive or violent behavior, in the intent of causing harm. It can be physical, verbal (like threats) or non verbal (like violent threatening gestures, etc.).

OTHER MISCONDUCT	
Grey Market	Genuine, branded products sold through unauthorized distribution channels or imported into another country for sale without the consent and knowledge of the brand owner.
Environmental issues	Issue or behavior that can generate possible harmful effects to natural systems (on small or large geographical areas), including water bodies, soils, air quality, biodiversity, climate, or generate an increased risk of natural disaster (flood, land slide, etc.). Environmental issues can lead to human health risks, reputational risks, fraud risks, financial loss and/or litigation. In addition to occasional events, environment issues should be reported if there is possibility of widespread occurrence across many Schneider Electric locations.
Quality issue	Intentional breach of quality policies, directives and procedures in order to obtain a personal gain or a benefit for the Company, at the expense of lower product quality, additional risks of malfunction and customer impact
Other	Any other misconduct not listed and defined above.