2. Case Handling - Investigations

Siemens expects its employees to comply with the law and Siemens’ internal regulations, to behave in a law-abiding and exemplary manner in order to prevent compliance cases from arising and to immediately report all information they may have regarding impending or existing compliance cases.

Siemens also expects its employees when affected to cooperate in internal compliance investigations in a transparent and open manner in order to enable Siemens to detect and to stop any potential misconduct.

Siemens will react adequately to determined Compliance violations by asserting claims for damages and the implementation of disciplinary measures. However, considering all circumstances of the individual case, it may be in the best interests of the company to refrain from these actions against an employee who has committed a Compliance offense or who is suspected of such (“Granting of Leniency”).

This is particularly the case if,

* the company is dependent on the active participation of suspicious employees for the clarification of Compliance-relevant facts with serious material or immaterial effects, and if such participation can only be obtained in this way, and
* the employee shows understanding and convincingly communicates that he will abstain from future misconduct and act as a role model for integrity.

Details can be provided by LC CO IR RD

## 2.1. Compliance Cases

The matters listed below are “compliance cases” if they involve actions that are performed by Siemens employees in the course of their business activities or by third parties acting on Siemens’ behalf and/or that may damage the overall reputation of Siemens:

* all plausible allegations
* of a violation of criminal or administrative law or
* of a violation of a Siemens-internal regulation relating to criminal or administrative law (for example, the [Business Conduct Guidelines](https://intranet.legal-compliance.siemens.com/docs/2019_SAG_BCG_English_FINAL.pdf));
* all impending or current criminal or administrative proceedings against Siemens AG, one of its Affiliated Companies or one of its employees as well as any related requests for information;
* all impending or current proceedings by a multilateral development bank (for example, the World Bank) or a credit insurer (for example, Euler Hermes, KfW) as well as any related requests for information;
* all information[[1]](#footnote-1) regarding intentional violations of accounting regulations – that is, regulations regarding accounting and financial reporting, independent audits of financial statements, bookkeeping and bookkeeping controls;
* all intentional damages (no lost assets) that occur to the detriment of Siemens AG or its Affiliated Companies and/or occur on the company’s properties or projects (in this case also private property) (“security incidents”, formerly “TreuInfo cases”) as described in chapter 6 “Security incident management, formerly “TreuInfo””;
* all information regarding intentionally false reports of compliance cases;
* all information regarding possible breaches of data privacy law;
* all information regarding possible money laundering or terrorist financing activities;
* all information regarding possible human rights violations
* all information regarding a violation of export control or embargo regulations
* all plausible HR cases, if LC CO IR, at its discretion and in alignment with HR, considers the handling by itself necessary.

In contrast to the above items, for matters mentioned under 6) to 9) this is irrespective of whether such activities are performed by Siemens employees or by related or unrelated third parties when Siemens can be held liable for the misconduct.

## 2.2. Responsibilities

There is no differentiation between local and central compliance cases – there is only one “Compliance Case”. However, a Compliance Case is to be classified following a risk based approach as “high”, “medium”, or “low” risk The risk level is determined by the risk the case may have: cases which expose Siemens globally are classified as “high” risk cases; cases with exposure to the relevant business unit and / or to the specific regional company only are classified as “medium” risk cases; and cases which do not have any immediate risk exposure at the time they have been reported, are classified as “low” risk cases.

All Compliance Cases will be handled by Compliance Investigation and Regulatory – the bundling of the responsibility in one department ensures that all cases are being handled by experts and in the same way; hereby, the high-quality level is guaranteed throughout the handling of all Compliance Cases.

Impending or current criminal or administrative proceedings against Siemens AG, one of its Affiliated Companies or one of its employees as well as any related requests for information or any searches must be reported immediately to the local Legal or Compliance department. These units must immediately notify Compliance Investigation and Regulatory (LC CO IR).

### 2.2.1. ”High” risk cases

The following matters are generally classified handled as “high” risk compliance cases due to their potential risk exposure to Siemens globally:

* all impending or current criminal or administrative proceedings by law enforcement agencies or other public authorities in Germany against Siemens AG, one of its Affiliated Companies or one of its employees;
* requests for information by law enforcement agencies or other public authorities in Germany;
* all information regarding active corruption or the providing of unfair advantage by employees or third parties acting on Siemens’ behalf;
* all information regarding possible antitrust violations;
* all information regarding intentional violations of accounting regulations – in particular, regulations regarding accounting and financial reporting, independent audits of financial statements, bookkeeping and bookkeeping controls;
* all impending or current proceedings by a multilateral development bank (for example, the World Bank) or a credit insurer (for example, Euler Hermes, KfW) as well as any related requests for information;
* all information regarding intentional wrongdoing that has led or can lead to damages of over € 50,000 to tangible or intangible assets;
* all information regarding intentional wrongdoing on the part of an employee who is an ICFR and Supporting Certifier or belongs to the Top Management;
* all information regarding a violation of export control or embargo regulations;
* compliance cases that cannot be handled locally due to potential conflicts of interest as far as the conflict of interest cannot be resolved locally;
* all information regarding intentional false reporting of compliance cases;
* all information regarding possible money laundering or terrorist financing activities and
* all information regarding possible human rights violations if not under the responsibility of another department.[[2]](#footnote-2)

### 2.2.2. ”Medium and Low Risk” cases

All compliance cases that do not meet the criteria set out in point 2.2.1. of this chapter will be classified with “medium” or “low” risk. In general, the cases will be handled by LC CO IR in the same way as the “high” risk” cases. However, the Mandating and Reporting process differs: “Medium” risk cases will be mandated by the Compliance Legal together with the Compliance Officer responsible for the region / the business; these are also the ones responsible for issuing the final report.

“Low” risk cases do not require a mandate but will be monitored by Compliance Investigation and Regulatory together with the Compliance Officer responsible.

### 2.2.3. Other cases

There are also other cases that – although involving violations of Siemens’ internal regulations – will not be handled by the Compliance Organization. These cases include, for example, matters in which specialist expertise is required or matters in which no intentional violation of Siemens’ internal regulations is alleged. Unless these cases are central compliance cases, they will be forwarded to the relevant specialist department for action.

This applies in particular to the following HR-specific matters for which the HR organization is responsible:

1. HR standard processes such as hiring, dismissal, issuance of work permits etc.
2. workplace environment, pay, incentives, calculation of bonuses, workloads, overtime, and all other organizational or procedural HR topics
3. improper favoritism, workplace intimidation, all forms of discrimination, harassment or other inappropriate behavior on the part of coworkers, managers or other company employees
4. irregularities related to travel or organizational expenses
5. improper use or damage of company property
6. matters related to workers councils and unions
7. matters related to pensions

The following cases may be taken over by LC CO IR at its discretion and I alignment with HR. Allegations in connection with:

* ongoing/imminent governmental or criminal investigations
* material damage to the company (more than 50.000 €)
* asserted retaliation against a whistleblower
* intentional false reporting of compliance cases
* allegations against top executives, Country Heads, Heads of Corporate Units, ICFR Certifiers, and senior managers
* harassment or discrimination (including, but not limited to, based on race, gender, national origin, sexual orientation) that could result in material financial risk or impact the company’s reputation in public opinion or the press.
* improper use of social media that could result in material financial risk or impact the company’s reputation in public opinion or the press.
* allegations of substantial systemic misconduct with significant financial or reputational impact

In addition, the GM SEC organization is responsible for the following GM SEC-specific and similar cases with no apparent relation to compliance matters:

1. Sabotage (i.e. to products, machines, production lines, vehicles, etc.)
2. Politically motivated crime (i.e. arson to cars, etc.)
3. Organized crime, gang crime
4. IT and cyber-related crime
5. Theft
6. Terrorism (i.e. supporting authorities)
7. Espionage
8. Extortion

GM SEC will immediately inform LC CO if they become aware of a matter that is relevant to the compliance organization.

LC CO will immediately inform GM SEC if they become aware of a matter that is relevant to GM SEC.

In appropriate cases, and within the limits of availability, GM SEC resources are accessible to the compliance organization for investigation assistance and can be mandated accordingly.

In matters that are the responsibility of GM SEC and require law enforcement interaction, GM SEC shall consult with LG CO IR if the matter is material, has the potential for civil, administrative or criminal legal risk to the company, or has potential public relations implications.

Furthermore, specifics apply for the recording of DP and EX Cases in TRACI. The handling of pure work errors at LC CO DP and LC CO EX should be recorded according to the following criteria in a case-by-case analysis in TRACI:

• Indications of systematically determined misconduct by the same person or group of people.

• Indications of intentional or grossly negligent misconduct by the same person or group of people.

• repeat cases.

• recurrent process weaknesses and organizational deficits.

• If, in relation to the relevant work error and a hypothetical overall view, it can be assumed that an authority / an examiner would initiate an official measure / procedure against Siemens.

If LC CO DP or LC CO EX intends to disclose internally identified misconduct by employees and misconduct / process weaknesses through voluntary disclosure and / or other approaches to authorities, this must be reported to the clearing committee via LC CO IR CF. On this basis, LC CO IR CF decides whether a TRACI registration should be carried out (regardless of whether a case has already been initiated by the authorities or not). For further details please see [here](https://findit.compliance.siemens.com/content/10000101/Compliance/LC_CO/LC_CO_RG_CH/findIT_LC_CO_RG_CH_9193.pptx).

## 2.3. Case tracking tool – TRACI

In order to provide a uniform system for recording compliance cases (as defined in point 1 of this chapter) within the Compliance Organization, the compliance case tracking tool (TRACI: Tracking Compliance Cases Internationally) was implemented from October 1, 2009[[3]](#footnote-3).

Governance responsibility for TRACI lies with Compliance Risk Management and Mitigation department (LC CO RFC RC) in conjunction with the head of Compliance Investigation and Regulatory (LC CO IR).

### 2.3.1. Registration of compliance cases in TRACI

The employees of the Compliance Organization worldwide must ensure that all compliance cases known to them are registered immediately in TRACI.

### 2.3.2. Reporting and certification

The uniform TRACI procedure standardizes and simplifies compliance review reporting. It ensures that all compliance cases that are to be reported to management are known at Compliance Investigation and Regulatory and that Siemens meets its internal and external reporting obligations and can take appropriate measures to investigate potential wrongdoing.

Compliance Officers must confirm on a quarterly basis that – to the best of their knowledge and belief – the new cases within their respective areas of responsibility have been accurately and completely entered in TRACI (“certification”). The tool also enables other Compliance Officers assigned to the previously mentioned Compliance Officers to implement certification. Certification at the end of a quarter is possible up to the tenth business day of the subsequent quarter (U+10).

At the end of every quarter, Compliance Investigation and Regulatory analyzes the compliance cases registered in the TRACI system and reports key data to the Chief Compliance Officer, who – jointly with the Chief Counsel Compliance – informs the Managing Board of Siemens AG, the Audit Committee of the Supervisory Board and the independent auditors.

### 2.3.3. Handling of compliance cases

The responsibilities for handling compliance cases are set out in section 1 of this chapter.

TRACI supports the work processes in the Compliance Organization and reflects the responsibilities for handling a Compliance case.

Compliance Investigation and Regulatory will keep the respective Compliance Officers updated on ongoing cases.

### 2.3.4. Registration of security incident cases

Effective January 1, 2020, the TreuInfo compliance process will be superseded by [IncidentReporting@Siemens](https://incidentreporting.siemens.com) (IR@S) in the responsibility of GM SEC.

For damages that arise outside GM SEC’s area of responsibility (for example, in areas for which LC, SFS CO or HR are responsible), a template for recording key data will be provided. Such cases that also constitute Compliance cases and are reported directly to GM SEC will be forwarded by GM SEC to the Compliance organization for further handling.

Further information can be found in chapter 6 “Security incident management (formerly “TreuInfo”)”.

### 2.3.5. Technical details

The TRACI application can be accessed from the intranet via https://traci.Compliance.siemens.com/traci. Questions regarding the tool and related topics may be directed to [traci-treuinfo.Compliance@siemens.com](mailto:traci-treuinfo.Compliance@siemens.com).

Details on the tool are provided by the intranet-based training programs and by information in the tool itself.

### 2.3.6. Access authorization

Due to the sensitivity of the data in the TRACI system and to avoid conflicts of interest and apply a strict need-to-know principle, only those employees of the Compliance Organization who are fully authorized to perform the tasks of the Compliance and Legal organization will have access to TRACI cases. Applications for exceptions must be submitted to Compliance Investigation and Regulatory and accompanied in every case by a written justification. Rights of use and access authorizations for TRACI will be handled via the Finance Portal. Therefore, all entries in the Finance Portal for access authorization must be accurate and complete, and must be updated to take account of any changes. The relevant Compliance Organization will review the accuracy of the entries of all authorized users in the Finance Portal at least once a quarter and correct those entries immediately, if necessary.

## 2.4. Investigation process for allegations

All compliance cases reported to the Compliance Organization will either be handled by Compliance Investigation and Regulatory or forwarded to the relevant specialist department or Siemens unit for further action.

### 2.4.1. Main principles

The following main principles of a compliance investigation must be complied with:

* The responsible investigative unit must conduct an objective and impartial investigation into all reported compliance allegations. Any internal investigation requires a formal mandate[[4]](#footnote-4) .
* All Siemens personnel and units engaged in internal investigations and fact-finding activities must perform their duties in a manner that is consistent with applicable laws and Siemens’ values.
* Inquiries must be conducted on the basis of a presumption of innocence.
* The identities of the complainant, witnesses or the subject of the investigation will not be disclosed to third parties unless this is required by law. Internal inquiries regarding ongoing investigations must be handled according to the "need-to-know principle”. These principles ensure that all investigations are conducted in accordance with the confidentiality requirements and the law within each jurisdiction.
* Investigative measures must be suitable, necessary and appropriate for fulfilling the aims of the investigation.
* The code of conduct for internal compliance investigations as laid down in chapter 3 “Code of conduct for compliance investigations and fact-finding” outlines the requirements that must be observed during such activities.

### 2.4.2. Steps in the evaluation of a cases

The process for evaluating compliance cases comprises the following steps:

* The first step is to determine whether a reported case is a compliance case (as defined above). If it is not a compliance case, the matter will be forwarded to the relevant specialist department (HR, GM SEC, EHS etc.) for further action.
* If a reported case is a compliance case, the plausibility of the related allegations will be reviewed. If these allegations are not plausible, the case will be closed in the compliance case tracking tool TRACI and will not be pursued further
* If the allegations are sufficiently plausible, their substance will be reviewed in a second step to determine if sufficient information is available to permit an internal investigation (a so-called initial suspicion).
* If the allegations are sufficiently substantial and the case is a “medium” risk compliance case, the Compliance Officer together with Compliance Investigation and Regulatory – Compliance Legal will issue an investigation mandate.
* If the case is a ”high” risk compliance case, the relevant counsel (case lawyer) at Compliance Investigation and Regulatory will issue an investigation mandate, which will be reviewed by the Head of Compliance Investigation and Regulatory and approved by the Chief Compliance Officer.
* Compliance Investigation and Regulatory (LC CO IR), Legal Competition (LC M&A CMP) – particularly in the case of antitrust violations – and third parties may be mandated to conduct investigations of central compliance cases. Compliance Investigation and Regulatory will provide legal support for all investigations of central compliance cases. The local Compliance Office or another local specialist department (for example, HR, Taxes, Export Control or EHS) may be mandated to clarify ”medium” risk compliance cases or individual aspects of compliance cases.
* Outside counsel will be mandated by Compliance Investigation and Regulatory if necessary. In order to avoid labour law related deadlines, the responsible local HR and/or legal department should be informed at the earliest possible stage.

### 2.4.3. Mandate contents

All mandates will contain

* an identifying TRACI number
* the name of the unit mandated to conduct the investigation/clarification, and
* a statement of the allegations and the Siemens unit involved.

In “high” risk compliance cases, investigations mandates will contain the signatures of the Chief Compliance Officer and the Chief Counsel Compliance.

In “medium” risk compliance cases, investigation mandates will contain the signatures of the relevant lawyer at LC CO IR CF and the relevant Compliance Officer.

Mandates may be shown to interviewees for the purpose of authorizing investigative activities. Therefore, in order to protect reporters and ensure the integrity and effectiveness of investigations, they will not contain any information or personal data in addition to the information listed.

### 2.4.4 Need-to-know principle / procedure of an investigation

The Chief Compliance Officer (in “high” risk compliance cases) or the relevant Lead Country Compliance Officer (in “medium” risk compliance cases) will inform – on a need-to-know basis – the CEO, CFO, General Counsel and Compliance Officer of the relevant Siemens unit (OPCP, or Business Unit) and of the relevant local unit and/or Lead Country and OPCO that the mandate has been issued. The Chief Compliance Officer will inform other individuals of the mandate as required.

In connection with their investigations, investigating units must be provided – to the extent permitted by law – with access to all relevant information available to Siemens AG and its Affiliated Companies. This applies in particular to

* interviews conducted with relevant employees and witnesses,
* the collection and securing of documents and other written information, and
* the collection and evaluation of electronic data.

In connection with their investigation, investigation units must be provided – to the extent permitted by law – with access to all relevant information available to the units for which they are responsible.

In its investigation, the investigating unit must comply with the Code of Conduct for Compliance Investigations and Fact-Finding (chapter 3) and all applicable local laws. Its activities must be suitable, necessary and appropriate for fulfilling the aims of its investigation. In the course of its investigation, the investigating unit must accordingly inform the Compliance Officer or Compliance Investigation and Regulatory (in central compliance cases) of all findings on a regular basis so that they may review the appropriateness of the investigative measures to be implemented. In ”high” risk compliance cases, the Chief Counsel Compliance must be directly informed of all findings on a regular basis so that he or she may review the appropriateness of the investigative measures to be implemented.

Violations by fact-finding units of the Code of Conduct for Compliance Investigations and Fact-Finding may be deemed compliance cases and sanctioned accordingly.

Employees must be notified of any investigations – and in particular of any collection of data – relating to them to the extent that such notification does not endanger the purpose of the investigation.

### 2.4.5. Data collection

Data may be collected only to the extent permitted under applicable local law.

An agreement regarding the aspects of compliance investigations governed by labor law and data privacy law has been concluded with the Central Works Council of Siemens AG[[5]](#footnote-5).

The investigating units will submit and sign an application for data mirroring and collection (Data Collection Request – DCR). The DCR will be forwarded to Compliance Investigation and Regulatory for review. Compliance Investigation and Regulatory will consult the Data Privacy Organization to ensure that the DCR complies with data privacy laws. DCRs will be approved and signed by the relevant counsel at Compliance Investigation and Regulatory and the Chief Counsel Compliance.

### 2.4.6. Conclusion / results

After concluding their investigations, investigating units will issue investigation reports. These reports, which must be approved by Compliance Investigation and Regulatory will include a description of the investigation/clarification framework, the findings of the investigation, the legal assessment of those findings and any related recommendations for action.

In cases where the investigating/clarifying units did not substantiate a wrongdoing by an employee, the employee concerned should receive a Clearance Letter, if legally permissible under local law.

In ”high” risk compliance cases, the Chief Compliance Officer will provide the reports to all relevant individuals on a need-to-know basis and to Compliance Investigation and Regulatory Discipline and Remediation (LC CO IR RD). If disciplinary measures are required, the reports will also be forwarded to the relevant HR department.

In ”medium” risk compliance cases, the responsible Compliance Officer will provide the reports to the relevant individuals on a need-to-know basis. Investigation reports must always be treated confidentially and may not be distributed further without the prior consent of the Chief Compliance Officer (in ”high” risk compliance cases) or the responsible lawyer from Compliance Investigation and Regulatory (in “medium” risk compliance cases),

## 2.5. Prohibition of retaliation

Retaliation of any kind against individuals who have reported complaints or compliance cases in good faith will not be tolerated. This prohibition applies to any action that may directly or indirectly harm the employment relationship, earning potential, bonus payments, career development or other work-related interests of the reporter.

Disciplinary sanctions imposed in a due process in response to a reporter’s involvement in any reported wrongdoing are not regarded as retaliation under this policy.

Reporting of retaliatory actions

Employees who notice or learn of a current or impending retaliatory action should immediately inform Compliance Case Handling (LC CO IR) either directly or via a member of the Siemens Compliance Organization. Compliance Case Handling will immediately take all steps necessary to protect the interests of the relevant employees. There may also be an internal investigation into the allegations. If such an investigation finds that this policy has been violated, appropriate measures will be taken. These measures may include disciplinary measures against the individuals who are responsible for and/or have taken part in the impermissible retaliatory actions.

Documentation of disciplinary measures

If disciplinary measures or other measures under labor law are taken against an employee who has reported a compliance case, Compliance Case Handling must be informed immediately.

If such measures are not connected with the reporting of a compliance case, the facts, the chronology and the basis for the measures must be documented by the relevant manager prior to their implementation.

## 2.7. Training and supporting material

[Compliance Academy](https://intranet.legal-compliance.siemens.com/internal/ComplianceAcademy/) (see Learning Landscape for Investigations Training and Case Library)

[Siemens Compliance Brochure](https://www.siemens.com/content/dam/internet/siemens-com/global/company/sustainability/downloads/responsible-business-behavior-compliance-at-siemens.pdf)

[Business Conduct Guidelines](https://findit.compliance.siemens.com/content/10000101/Compliance/CL_CO/CL_CO_AT/findIT_CL_CO_AT_128.pdf)

## 2.8. History of changes

|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Major changes of binding content** |
| January 1, 2019 | Bernd Plagemann | First release through the Compliance Handbook based on Siemens Circular SC No. 226 “Global Compliance”, Appendix 5. |
| April 1, 2019 | Bernd Plagemann | Discontinuation of the differentiation between central and local cases. |
| January 1, 2020 | Julia Wirth | Update regarding responsibilities of recording of fiduciary cases (former TreuInfo cases). |
| July 1, 2020 | Julia Wirth | Update on handling of DP and EX cases and HR cases in TRACI. |
| October 1, 2020 | Julia Wirth | Update on HR cases and the definition of CO cases. |

## 2.9. Contacts

Compliance Officer

The Compliance Officer responsible for your unit can be found through the following [link](https://intranet.for.siemens.com/cms/059/de/about/org/Pages/compliance_organization.aspx).

Corporate Governance Owner

The contact person for case handling is:

[Annette Kraus (LC CO IR)](https://soc.siemens.cloud/profile/Z002K99S)

The contact person for "medium" and "low" risk cases is:

[Michael Rackow (LC CO IR EG E)](https://scd.siemens.com/luz/IdentitySearch?cn=RACKOW+MICHAEL+Z0028PWK&tcgid=Z0028PWK&c=DE&o=SIEMENS&ou=LC&l=MCH+P&department=LC+CO+RG+CH+EA+EU&&utI=I&utX=X&utT=T&rtH=H&rtS=S&rtZ=Z&rtO=O&rtAktiv=A)

The contact persons for the Case tracking tool – TRACI are

[Marco Liese (LC CO PT CO)](https://soc.siemens.cloud/profile/Z000E4MF)

[Manja Ehnert (LC CO IR CF](https://soc.siemens.cloud/profile/Z002HX8A))

1. “Information” in this context includes reports provided by employees or third parties, findings by Compliance Officers, requests for information by public authorities, criminal or administrative proceedings by law enforcement agencies or other public authorities, and searches. [↑](#footnote-ref-1)
2. E.g. regarding employment practices or health and safety [↑](#footnote-ref-2)
3. For Germany only: The agreement announced in [CHR Circular No. 65/09](https://wse04.siemens.com/content/P0006195/Shared%20Documents/dir2010_2019/2009/CHRRS6509_8.pdf) (including the relevant supplements) applies to the TRACI application. The data privacy regulations included in that agreement must be complied with. [↑](#footnote-ref-3)
4. For details, please refer to section 2.4.3. of this chapter “Mandate contents”. [↑](#footnote-ref-4)
5. For Germany only: The contents of this agreement were announced in [CHR Circular No. 44/15](https://wse04.siemens.com/content/P0006195/Shared%20Documents/dir2010_2019/2015/HRRS4415_1.pdf) and its supplements. [↑](#footnote-ref-5)