6. Security incident management (formerly “TreuInfo”)

Security incidents are caused by activities intended to damage Siemens and can be categorized as follows:

* criminal acts (for example, theft, property damage, threats)
* missing persons / extortion / kidnapping
* civil unrest / armed attacks / terrorism
* economic espionage
* violations of travel security regulations.

All employees are required to immediately report security incidents to the relevant security officers and/or in the tool [IncidentReporting@Siemens](https://incidentreporting.siemens.com) (IR@S). GM SEC will support the relevant managers as needed.

Effective January 1, 2020, all reporting to the CFO and CEO will be conducted by GM SEC. The suppliers contributing to the dataset will also receive access to the reports.

The roles and responsibilities for incident processing and the related procedures are set out on the [Incident Management homepage.](https://intranet.for.siemens.com/cms/056/en/processes/security/Pages/security.aspx)

## 6.1. [IncidentReporting@Siemens](https://incidentreporting.siemens.com) (IR@S)

Effective January 1, 2020, the TreuInfo compliance process will be superseded by [IncidentReporting@Siemens](https://incidentreporting.siemens.com) (IR@S). Damages will be recorded in the Criminal Act template, which is accessible in the tool.

In contrast to the previous definition of TreuInfo damages, there is a reporting obligation for 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). This constitutes a fiduciary case.

|  |
| --- |
| For IR@S Cases the following criteria must be fulfilled:   * + an intentional act involving Siemens employees and/or third parties, and   + an economic loss or material damage to the company´s property (no lost assets) or projects and/or   + an economic loss or material damage that occurred on the company’s properties or project sites. |

There is, in general, no threshold level for reports.[[1]](#footnote-1)[1] As a rule, the value of a damage is equal to the replacement value in euros (where applicable, at the current exchange rate).

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 by GM SEC. The incidents and damage amounts recorded in this template will be included in the overall report. For this reason, the department responsible for a particular case must have entered all relevant incidents in the template, at the very latest, by the time case processing is completed. Any changes in the individuals with authorized access must be reported to GM SEC.

The change with respect to TreuInfo does not affect the registering procedure for Compliance cases as defined in the [Compliance Handbook L. 2.1.](https://webbooks.siemens.com/public/LC/chen/index.htm?n=Part-3-Compliance-Internal-Tasks,L.-Case-Handling,-Discipline-and-Remediation,2.-Case-Handling,2.1.-Compliance-Cases) These will still be registered in TRACI. Cases that are reported directly to GM SEC but also constitute Compliance cases will be forwarded by GM SEC to the Compliance organization for further handling.

**Which damages must I report as an employee?**

Any incident with damage which is

1. **intentional**  
   The damage must have been caused deliberately. If an item is simply only lost (i.e. on a train, etc.) and there is no indication that a theft has occurred, no report is necessary, but other processes might apply (i.e. wipe device, report loss at lost and found, report lost information on device, etc.).

and is

1. **damage to Siemens assets**

Siemens property was affected by the incident. This can be the result of theft, but other damages are possible (i.e. through sabotage, vandalism, etc.)

and/or

1. **happens on a Siemens site or project**

Not only damage to Siemens is important to us. We want to know when an incident happens on a Siemens site or project even when private property is affected. The circumstance that there is crime on the site or project is relevant to us.

There is no damage-threshold for reporting except for office material (e.g. printer-paper, toner, pens, etc.) which lies at 200.-EUR. Any damage must be converted into EUR according to the current exchange rate in order to maintain comparability. The damage value should reflect the replacement value or costs to restore the desired state of the damaged item. For items which cannot be replaced with an identical item (maybe due to only newer versions being available), the value of a comparable replacement or - if still available - the original purchasing price can be reported.

**Which damage must I report as Compliance, HR, SFS CO?**

Any damages which are not already reported as a Security Incident (e.g. resulting from a TRACI case, a HR investigation or Fraud investigation by SFS CO) must be reported using the template which was created for this use case. The template is only for damages resulting from cases which are handled by the above-mentioned entities and can be found in IR@S under “Report Incident” -> “other templates” -> “Compliance, SFS CO and HR-Compliance Damage Report”. Any damages reported here will be part of the global reporting to the CFOs. Damages must be entered after conclusion of the case at the latest. Contributors to the reports will have access to their own reported cases and to a dashboard with numbers relevant to their area of responsibility. Any changes to access rights can be requested at [GM SEC](mailto:samuel.roberts@siemens.com?subject=Change%20to%20access%20rights%20in%20IR@S).

## 6.2. Training and supporting material

Training and supporting material can be found on the [Security](https://intranet.for.siemens.com/cms/056/en/processes/security/Pages/security.aspx) [Incident Management Homepage.](https://intranet.for.siemens.com/cms/056/en/processes/security/Pages/security.aspx)

## 6.3. History of changes

|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Major changes of binding content** |
| January 1, 2019 | Uwe Breitenstein | First release through the Compliance Handbook based on Siemens Circular SC No. 226 “Global Compliance”, Appendix 6. |
| January 1, 2020 | Julia Wirth | Update regarding responsibilities of recording of fiduciary cases (former TreuInfo cases). |

## 6.4. 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 IR@S is:

[Samuel Roberts (GM SEC ICM CPI)](https://soc.siemens.cloud/profile/Z000RFFP)

1. [1] Except for office supplies (for example, printer paper, writing implements and toner). A reporting threshold of €200 applies in this case. [↑](#footnote-ref-1)