
Whistleblower Policy

White employees, other stakeholders and the general public will have the opportunity to anonymously report serious irregularities at White through a whistleblowing/email function on the website and intranet.

Examples of serious misconduct include corruption, bribery, misconduct, fraud, financial crime, serious security breaches, environmental crimes, leaks of sensitive information and serious misconduct.

White's guiding values are to be accountable and to act with respect and inclusiveness. These values should permeate all our activities and how we conduct and implement our missions. Serious misconduct is therefore inconsistent with our values and we encourage the reporting of any suspicions of such misconduct.

Guidelines on how the whistleblowing function works

- Notification should go to the person responsible for White's security issues, i.e. the Head of Security.
- The notification will be sent to the Security Manager's regular mailbox.
- The Head of Security should not be able to see who sent the notification.
- Employees in the Digital Office/Operations unit who normally have administrator rights to email accounts at White will not be able to see who the sender is, i.e. no one at White will be able to trace who the sender is.
- The Head of Security will report to the Board on the matters received no later than the next Board meeting or as soon as possible to the Chair of the Board if the Head of Security considers that the matter is serious.
- The Security Officer may communicate the content of the notification to those he/she considers appropriate and necessary to deal with the notification

Göteborg 2019-09-10, 2020-09-16, 2021-09-15, 2022-09-21



Alexandra Hagen
VD