Whistleblowing Policy

0.1 Background

At Web Manuals, we are committed to fostering an open and transparent workplace, free from misconduct. To uphold this standard, we provide clear and secure channels for confidential whistleblowing. If there are suspicions of ongoing or past malpractices, it is imperative that resources are readily available for reporting such concerns. By facilitating the reporting of malpractices as set out in this Whistleblowing Policy, we aim to enhance the trust of our employees, customers, partners and the general public.

This Whistleblowing Policy applies to all entities in the Web Manuals Group, currently consisting of the following companies:

- Web Manuals International AB
- Web Manuals Sweden AB
- Web Manuals Americas AB
- Web Manuals Technologies AB
- Web Manuals Innovation 1 AB
- Web Manuals Group, Inc
- Web Manuals, Inc
- Web Manuals Asia Pte Ltd
- Web Manuals Australia Pty Ltd

0.2 Definitions

- **GDPR**: General Data Protection Regulation, which is a European regulation governing the processing of personal data and the free movement of such data within the European Union.
- **The Whistleblower Directive**: EU Directive 2019/1936 on the protection of persons reporting irregularities in Union law.
- **Whistleblower Act**: National implementation of the Whistleblower Directive in EU Member States.
- **California Labor Code Section 1102.5**: Also known as the Whistleblower Protection Act applicable in the State of California.
- **New York Labor Law §740**: Whistleblower protection and non-retaliation provisions applicable in the State of New York.
- **Visslan**: The Whistle Compliance Solutions AB's service Visslan, which enables digital reporting of misconduct: **https://visslan.com/**
- **Misconduct**: Acting or omissions that have emerged in a work-related context that there is a public interest in it occurring.
- **Reporting**: Written or verbal submission of information about misconduct using Visslan.
- **Internal reporting**: Written or verbal provision of information about misconduct within a company in the private sector.
- **External reporting**: Written or verbal provision of information about misconduct to the competent authorities.
- **Publication or to make public**: To make information about misconduct available to the public.
- **Reporting person**: A person who reports or publishes information about misconduct acquired in connection with his work-related activities.
- **Retaliation**: Any direct or indirect act or omission which occurs in a work-related context and which is caused by internal or external reporting or by a publication, and which gives rise to or may give rise to unjustified injury to the reporting person.
- **Follow-up**: Any action taken by the Case Manager(s) of a report to assess the accuracy of the allegations made in the report and, where appropriate, to deal with the reported infringement, including through measures such as internal investigations, investigations, prosecutions, actions to recover funds and to close the procedure.
- **Feedback**: providing reporters ("whistleblowers") with information on the actions planned or taken as a followup and on the grounds for such follow-up.

1.1 Who can report?

You can report and receive protection from the Whistleblower Act if you are an employee, volunteer, trainee, active shareholder, person who is otherwise available for work under our control and management or is part of our administrative, management or supervisory body. Contractors, subcontractors and suppliers to us who have found out about malpractices within the company can also submit reports according to this policy.

The fact that you have ended your work-related relationship with us, or that it has not yet begun, does not prevent you from reporting malpractice or receiving protection for reporting malpractices.

In addition to this, we also enable people outside the above categories to use our internal reporting channel. We will treat all reports equally, even if you are not covered by the Whistleblower Act's protection against retaliation.

1.2 What can I report?

In case of suspicion of possible misconduct, law and/or regulation violation, we encourage you to submit a whistleblowing report. When reporting, it is important that you at the time of reporting had reasonable grounds to believe that the information about the misconduct that was reported was true. Assessing whether there were reasonable grounds, circumstances and information that were available to you at the time of reporting should be the basis for whether you may have assumed that the misconduct was true. In addition, it is also important that it can actually be considered a violation that can be reported, and thus give you protection against retaliation.

Before you blow the whistle, read **5 questions to determine if you are protected by the Whistleblower Act**.

1.2.1 Malpractice in the public interest

You can report information about misconduct that has emerged in a work-related context where there is a public interest in their disclosure. In the event of other types of personal complaints that do not have a public interest in their disclosure, such as disputes or complaints regarding the workplace or the work environment, we encourage you to contact your immediate manager, Employee Experience or your local Health and Safety Officer. This is to ensure that these matters are handled in the best possible way. Consult with our Case Manager(s) set out in **6 - Contact information for case manager(s)** if you have any further questions in this regard.

Examples of malpractices of a serious nature that should be reported include:

- Deliberately incorrect accounting, internal accounting control or other financial crime.
- Theft, corruption, vandalism, fraud, embezzlement or hacking.
- Serious environmental crimes or major deficiencies in workplace safety.
- If someone is exposed to very serious forms of discrimination or harassment.
- Other serious misconduct affecting the life or health of individuals.

At Web Manuals, we consider all unethical or illegal behavior as irregularities worth reporting. We therefore treat all reports received equally, based on the intention of applicable law and provide protection against retaliation for all reporters.

If the reporting does not meet the criteria of the Whistleblower Act, we will still provide the same confidentiality and retaliation protection as a report made according to the Whistleblower Act, provided that the reporting is true and/or made in good faith.

The following are examples of unethical or illegal behavior that could be reported:

- Actions and omissions that go against our culture, vision and values.
- Actions that are not in line with good practice and standards in the labor market.
- Drug and alcohol abuse during working hours.
- Dangerous acts that could cause physical damage to a person or property.
- Discrimination of any kind.
- Exploitation of position and/or abuse of power.

1.2.2 Misconduct contrary to EU Law

In addition, there is the possibility to report information about misconduct that emerged in a work-related context that is contrary to EU laws or regulations. If you suspect that this occurs, then please read the scope of the **Whistleblower Directive** in Article 2 and Annex Part 1 for applicable laws.

Furthermore, if we receive a report regarding misconduct that has taken place in the US, we will handle your case in accordance with California or New York State Laws.

1.3 How do I report?

1.3.1 Written reporting

For written reports, we use **Visslan**, which is our digital Whistleblowing Channel, available at **https://webmanuals.visslan-report.se**. On the website, you choose to "report" in order to then be able to describe your suspected misconduct. Please describe what happened as thoroughly as possible, so that we can ensure that adequate measures can be applied. It is also possible to attach additional evidence in various format, for example written documents, pictures or audio files, even though this is not a requirement for the sake of reporting a whistleblowing case. A flowchart describing the Whistleblowing Case Management is attached in **7 – Whistleblowing Case Management Flowchart**.

1.3.2 Sensitive personal data

Please do not include sensitive personal information about people mentioned in your report unless it is necessary to be able to describe your case. Sensitive personal data is information about; ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, a person's sexual life or sexual orientation, genetic data, biometric data used to uniquely identify a person.

1.3.3 Anonymity

You can be anonymous throughout the process without affecting your legal protection, but you also have the opportunity to disclose your identity under strict confidentiality. Anonymity can in some cases complicate the ability for follow-up measures, in which cases it could be appropriate to disclose your identity in strict confidentiality to the applicable Case Manager(s).

1.3.4 Follow-up and login

After you have submitted your report, you will receive a sixteen-digit code, which will allow you to access your report via **https://webmanuals.visslan-report.se**. It is very important that you save the code, else you will not be able to regain access to your report.

If you lose the code, you can submit a new report referring to your previous report.

Within **seven days**, you will receive a confirmation that the Case Manager(s) has received your report. The Case Manager(s) contact details are attached in “6.1 Contact information for Case Manager(s)”. In case of questions or concerns, you and the Case Manager(s) can communicate through the platform's built-in and anonymous chat function. You will receive feedback within **three months** on any measures planned or implemented due to your report.

It is important that you, by using your 16-digit code, log in to the reporting channel regularly to answer any follow-up questions Case Manager(s) may have. In some cases, the report cannot be properly handled without answers to such follow-up questions from you as the reporting person.

1.4 Verbal Reporting

In addition, and subject to applicable law, it is also possible to submit a verbal report by uploading an audio file as an attachment when creating a report at **https://webmanuals.visslan-report.se**. You do this by selecting that you have evidence for the report, and select an audio file that is uploaded with the report. In the audio file, you shall describe the same facts and details as you would have done in a written report.

In addition, you may request a physical meeting with the Case Manager(s) via Visslan. This is done by either requesting it in an existing report, or creating a new report requesting a physical meeting.

1.4.1 External reporting

We urge you to always report malpractice internally first, but in the event of difficulties or considered inappropriate, it is possible to conduct external reporting instead (or after internal reporting without results). In those cases, we can refer you to contact the competent authorities or, where applicable, to EU institutions, bodies or agencies.

1.5 What are my rights?

1.5.1 Right to confidentiality

When we receive and manage your report, we will ensure that your identity is treated confidentially and that no unauthorized personnel will access your case except for the Case Manager(s). We will not disclose your identity without your consent unless required by mandatory law, and we will ensure that you are not subjected to retaliation based on your report.

1.5.2 Protection against reprisals or retaliation

In the event that you submit a whistleblowing report, you enjoy protection against negative consequences from having reported misconduct in the form of a ban on reprisals and retaliation. The protection also applies in relevant cases to persons in the workplace who have assisted you in your report, for example, colleagues, friends or relatives, and legal entities that you own, work for or are otherwise related to.

The protection means that threats of retaliation and attempts at retaliation are not permitted by Web Manuals. Examples include if you were to be fired, forced to change work tasks, imposed disciplinary measures, threatened, discriminated against, blacklisted in your industry, or similar, due to your report.

Even if you were to be identified and subjected to reprisals, you would still be covered by the protection as long as you had reasonable grounds to believe that the misconduct reported was true and within the scope of the Whistleblower Act. Note, however, that protection is not obtained if it is a crime in itself to acquire or have access to the information reported.

The protection against retaliation also applies in legal proceedings, including defamation, copyright infringement, breach of confidentiality, breach of data protection rules, disclosure of trade secrets or claims for damages based on private law, public law or collective labour law, and you shall not be held liable in any way as a consequence of reports or disclosures provided that you had reasonable grounds to believe that it was necessary to report or publish such information in order to expose a misconduct.

1.5.3 Publication of information

The protection also applies to the publication of information. It is then assumed that you have reported internally within the company and externally to a government authority, or directly externally, and no appropriate action has been taken within three months (in justified cases, six months). Protection is also obtained when you have had reasonable grounds to believe that there may be an obvious danger to the public interest if it is not made public, for example in an emergency. The same applies when there is a risk of retaliation in the case of external reporting or that it is unlikely that the misconduct will be remedied in an effective manner, for example in the event that there is a risk that evidence may be concealed or destroyed.

1.5.4 The right to review documentation at meetings with case manager(s)

If you have requested a meeting with the Case Manager(s), they will, with your consent, ensure that complete and correct documentation of the meeting is preserved in a lasting and accessible form. This can be done, for example, by recording the conversation or by keeping minutes. Afterwards, you will have the opportunity to check, correct and approve the protocol by signing it.

We recommend that this documentation is kept in Visslan's platform by the whistleblower creating a case where the information can be collected in a secure way, with the option to communicate securely.

1.6 GDPR and handling of personal data

We always do our utmost to protect you and your personal information. We therefore ensure that our handling of these is always in accordance with the General Data Protection Regulation ("GDPR") or similar applicable data protection regulations.

In addition to this, all personal data without relevance to the case will be deleted and the case will only be saved for as long as it is necessary and proportionate to do so. The longest a case will be processed is two years after its conclusion. For more information about our handling of personal data, see our Privacy Policy.

1.7 Additional contact

If you have further questions regarding how we handle whistleblower reports, you are always welcome to contact Case Manager(s).

For technical questions about Visslan's platform, feel free to create a case at **https://webmanuals.visslan-report.se**. Should this not be possible, contact Visslan. Contact information for both can be found below.

1.7.1 Contact information for case manager(s)

Name	Fredrik Karlsson	Ylva Lindgren
Function	General Counsel	Chief People Officer
Email	legal@webmanuals.com	legal@webmanuals.com
Phone number	+46 40 694 10 40	+46 40 694 10 40

1.7.2 Contact information for Visslan (The Whistle Compliance Solutions AB)

Email	clientsupport@visslan.com
Phone number	+46 10 750 08 10
Direct phone number (Daniel Vakine)	+46 73 540 10 19

1.8 Whistleblowing Case Management Flowchart