Whistleblowing Policy

Avast is in the business of protection. This doesn’t just mean protecting the digital lives of our customers, but also each other and our business. We believe honest communication is critical to the success of our teams. Everyone at Avast should feel comfortable speaking up if they believe something is wrong. Anyone associated with Avast may report valid misconduct without fear of retaliation.

Avast’s Whistleblowing Policy outlines the steps for reporting misconduct and serious breaches of Avast policy or ethical guidelines without fear in cases which cannot be resolved through normal channels for reporting grievances.

If you are uncomfortable raising your concerns through normal channels, or if you fear retaliation, then you may raise an issue as a whistleblowing report. We are committed to ensuring that all concerns are immediately addressed to ensure the trust of all our employees and partners.

Making a whistleblowing report

All Avast employees, or any other person associated with Avast, are encouraged to keep Avast informed of any illegal or unethical behaviour which may violate Avast’s applicable policies. This applies whether the information is confidential, is happening now, or has already happened. Avast will oversee the handling of concerns in this area.

When to use the whistleblowing channels

If you have a concern you should first try to address this with your manager or your HR business partner or through the Legal Department, through normal reporting channels. As an alternative, you may raise the issue as a whistleblowing report.

Use of whistleblower@avast.com

You may submit a whistleblowing report by email to whistleblower@avast.com. When doing so you are encouraged to provide your name, position and contact details. These details will make it easier for us to investigate the matter. However, you are free to report anonymously.

Whistleblowing hotline

In addition to the email address listed above, you may report concerns on our Avast Ethics & Reporting Line (dial-in numbers below), or by submitting a report online at: http://avast.ethicspoint.com.

<table>
<thead>
<tr>
<th>Country</th>
<th>Line Type</th>
<th>Dial-in Number(s)</th>
<th>Access code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>ITFS</td>
<td>1 800 79 2095</td>
<td>NA</td>
</tr>
<tr>
<td>Canada</td>
<td>DD</td>
<td>1 855 862 1160</td>
<td>NA</td>
</tr>
<tr>
<td>China (incl. Hong Kong)</td>
<td>DA</td>
<td>10 811 (Southern) 108 888 (Northern)</td>
<td>855 862 1160</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>ITFS</td>
<td>800 143 875</td>
<td>NA</td>
</tr>
<tr>
<td>Germany</td>
<td>DA</td>
<td>0800 225 5288</td>
<td>855 862 1160</td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td>0034 811 001 (NTT) 00 539 111 (KDDI) 00 663 5111 (Softbank Telecom)</td>
<td>855 862 1160</td>
</tr>
<tr>
<td>Netherlands</td>
<td>GIS</td>
<td>0800 292 9255</td>
<td>NA</td>
</tr>
<tr>
<td>Norway</td>
<td>ITFS</td>
<td>800 13955</td>
<td>NA</td>
</tr>
</tbody>
</table>
Country | Line Type | Dial-in Number(s) | Access code
--- | --- | --- | ---
Russia | DA | 363 2400 (Moscow or St Petersburg) 8*10 800 110 1011 (^ indicates second dial tone) | 855 862 1160
Serbia | GIS | 0800 190 968 | NA
Slovakia | DA | 0 800 000 101 | 855 862 1160
Switzerland | DA | 0800 890011 | 855 862 1160
Taiwan | | | |
United Kingdom | ITFS | 0808 234 7272 | NA
United States | DD | 855 862 1160 | NA

Note: If the call type is DA, you will first dial a local dial-in number and then at the prompt enter a unique number for your organization (access code). Some countries may have multiple dial in numbers. For DD (Direct Dial), ITFS (International toll free service), and GIS (Global inbound service) lines, you will dial the number and be connected directly to the hotline.

Issues that may be included in a whistleblowing report

Examples of ethical matters which could be reported include the following. This is not intended to be a comprehensive list:

- Abuse of authority
- Inappropriate accounting practices or internal controls
- Provision of incorrect information to public authorities
- Improper use of Company funds
- Manipulation or falsification of company data / records
- Sexual harassment or bullying
- Violation of insider trading laws
- Wastage / misappropriation of company funds or assets
- Violation of the criminal law
- Violation of the Company’s Code of Conduct.

Following up on reports

After receiving a report, Avast will appoint an individual to review your report and decide if an investigation is merited. If it is determined that the report does not have merit, the person reporting the whistleblowing complaint will be informed.

If it is determined that the report needs further investigation, the appropriate personnel will be appointed to conduct the follow up. Avast will investigate every report in an efficient and speedy manner while protecting the dignity of every person involved.

The reporting person will be informed (as appropriate) on the outcome of the investigation and steps taken.

Depending on the nature of the whistleblowing event, a report of the event and its investigation may be provided to the Board.

Confidentiality and disclosure of information

Confidentiality will be maintained to the extent possible, consistent with the need to conduct an adequate investigation of the report.
Where strictly necessary for the purposes of the investigation, the authorised personnel of the investigation team may share a report with, and transfer your personal data, to a limited number of internal and external specialists/experts considering the content of the report, such as outside legal counsel and financial or tax auditors, for resolving any difficult issues or conducting any additional investigations or procedures.

The information collected in the report may also be disclosed to law enforcement or government authorities as necessary to comply with legal requirements. However, personal data relating to the identity of the individual making the report will be kept confidential as far as possible unless the interest of the individual is outweighed by the interest of compliance with the legal requirements.

No retaliation

Avast will not discharge, demote, suspend, threaten, harass or in any manner discriminate against any employee making a good faith report. Furthermore, where reports are made in good faith the employee will be protected from retaliation, even if the investigation determines that the report is groundless.

Responsibilities

Avast will maintain and retain, in accordance with applicable law, a log of all complaints, investigations and resolutions and will prepare periodic summary reports for the Audit Committee of the Avast Board.

Versions and approval

Version / Date: Version 1.0 / October 1, 2018