Global Whistleblowing Policy

Effective Date: March 2024

1. Statement of policy

Integrity, honesty, and accountability are key to Splunk's success and form the basis of how we operate. We are all key to this success and are counted on to instill our values in the work we do, and in the interactions we have with customers, partners, colleagues, and others on Splunk's behalf.

Each of us has a responsibility to speak up if we see something unethical, unsafe, or that constitutes a potential violation of our Code of Business Conduct and Ethics policy (the "Code") or other policies or laws. Splunk is committed to open communication and encourages employees with any concerns to bring their concerns to Splunk's attention. You can do so without any fear of retaliation. If you observe behavior that concerns you, or that you think may be a violation of our Code, Splunk policies or applicable laws, or if you have a question about any of these things, you have multiple options for raising issues and concerns. Those options are set out in this policy.

No retaliation: Splunk will not tolerate any form of retaliation against any person who in good faith: (1) makes a complaint, including, for example, by using Splunk's complaint procedure described below, (2) reports or assists anyone in making a report under this policy, (3) files, testifies, assists or participates in any investigation, proceeding, or hearing (including those conducted by a government agency) regarding any potential violation of law or policy, or (4) engages in any activity protected under applicable law. Prohibited retaliation includes but is not limited to, termination, demotion, suspension, or taking any other adverse employment action, including with respect to the terms or conditions of employment because an employee engaged in a protected activity. Retaliation is not tolerated and is a form of misconduct that may result in disciplinary action, up to and including termination of employment.

1.1 What should be reported?

Splunk expects you to speak up when you know or suspect that there has been or there may be a violation of our Code, Splunk policies or applicable laws, or when you know or suspect that there has been or may be conduct that is improper or unethical, or might compromise Splunk's reputation or the interests of its customers ("Reportable Conduct"). Examples of Reportable Conduct can include *but are not limited to* concerns regarding:

- legal or regulatory compliance;
- breaches of Splunk's policies and/or procedures;
- sales practice and/or market conduct violations;
- bribery or other improper payments or gifts;
- fraudulent activity;
- compliance with antitrust or competition laws;
- potential conflicts of interest;
- the integrity of Splunk's accounting practices, internal controls, auditing matters or public filings;
- human rights violations;
- discrimination, harassment, or retaliation; and
- potentially unsafe or dangerous practices or workplace conditions, including those which may threaten public health, safety, or the environment.

If, on the other hand, you have a concern regarding managing and/or coaching that includes counseling, performance management and the legitimate imposition of discipline, these issues should be raised with the People Team using this link.

If you raise a concern that the People Team reasonably believe should be addressed under this policy, then the People Team may refer this matter to the appropriate department so that it may be dealt with under this policy instead.

1.2 What should a report include?

A report should be as detailed as possible to facilitate its thorough review and investigation. If possible, a report should include the following details (to the extent known or suspected by you):

- your relationship with Splunk;
- a description of relevant events and how they came to your attention, including date, time and place;
- the names and job positions of the people involved, or other information that helps to identify those people;
- the names of other people, if any, who were witnesses to or who otherwise may have information about the relevant events; and
- any other information, documentation or evidence that could help those who investigate the report to verify the relevant events. You are also encouraged to provide your name in the report so we can follow-up with you as necessary, but this is not mandatory.

1.3 How can reports be made?

What channels can be used? You can make a report in writing or orally, and in the following ways:

- calling the Ethics and Compliance Hotline for the country in which you are located which can be found here;
- accessing the Ethics and Compliance website at EthicsPoint - Splunk, Inc. and raising your concern directly through this website. The Ethics and Compliance Hotline is available 24 hours a day, seven days a week and enables you to file a report in your own language. You will receive a report key and password which you may use to check the status of your report, provide additional information, or respond to any questions; or
- contacting your manager, Splunk's Legal Department (Legal@splunk.com), our Chief Ethics and Compliance Officer ("CECO") (ceco_office@splunk.com), or the People Team (including your HRBP or SPOT) (spot@splunk.com), to raise your report directly.

While we strongly encourage you to report any concerns internally before reporting concerns externally, nothing in this policy prohibits or is intended to restrict you from disclosing information to external reporting agencies in accordance with applicable law or regulation. Details of the external reporting procedures relevant to your jurisdiction are available at Pwny Portal.

1.4 Confidentiality and anonymous reports

Confidentiality: Splunk will endeavor to manage all reports raised under this policy confidentially (regardless of whether the report is made anonymously or not). This means that Splunk will seek to protect the identity of any person who is subject to or named in a report or connected with Reportable Conduct as appropriate under the circumstances and subject to applicable law.

Splunk will also endeavor to keep confidential any information that you provide as part of a report (to the extent possible under Splunk's legal and regulatory obligations). Splunk will share information only on a need-to-know basis with those who are involved in investigating, reporting or resolving the matter (except where information sharing is either prohibited or required by law or regulation).

Anonymous reports: Anonymous reports can be made, subject to applicable law and regulation. Making a report anonymously may affect your ability to receive feedback on the status of any investigation and Splunk's ability to effectively investigate the matter or offer protection to you.

1.5 Investigating a Reportable Conduct

All reports made under this policy will be taken seriously. Once you have raised a Reportable Conduct, the matter will be reviewed and assessed to decide if an investigation is appropriate, who should investigate and what action, if any, should be taken.

All employees, directors, officers, interns, and any agency or contingent workers engaged by Splunk are required to cooperate truthfully and responsively in any internal investigation. Anyone who fails to cooperate (e.g. by not providing complete and truthful information or intentionally providing misleading information) may be subject to disciplinary action, up to and including termination of employment.

1.6 How do we follow-up on reports?

Feedback: Within seven days of receiving a report, an acknowledgement of receipt will be sent to the reporter (including to an anonymous reporter where this is possible).

We will provide the reporter, where possible, with updates about the status of the investigation of their report, no later than three months after the acknowledgement of receipt. Investigations are sensitive and the information that Splunk can provide may be subject to certain limitations to protect the integrity of the investigation, including under applicable law and regulation. A reporter must treat any information provided by Splunk about the investigation as confidential. The reporter will also, where possible, be informed in writing when the investigation or file closes.

Remedial and disciplinary action: The action taken,if any, will depend on the nature and gravity of the Reportable Conduct and the results of the investigation. If the investigation finds a violation of any law or policy, or any other form of misconduct, Splunk will take prompt remedial action which is proportionate to the seriousness of the misconduct and in accordance with its procedures and practices and applicable law. Such remedial action may include disciplinary action, up to and including termination of employment, and/or other legal proceedings.

A person who knowingly and intentionally or negligently makes a false report, or provides false or deliberately misleading information in connection with an investigation of a report, may face disciplinary action up to and including termination of employment.

1.7 Data privacy

In receiving information and investigating reports under this policy, Splunk will collect and process personal data.

Any processing of personal data in relation to the operation of this policy (including any international transfers of personal data) will be carried out in accordance with applicable law and regulation, and with Splunk's own policies and procedures. Please refer to Splunk's Employee Data Protection Notice and the Data Privacy Policy: Processing Personal Data Under Splunk's Control for further details.

2. Definitions

- **Reportable Conduct:** Conduct that is improper or unethical, or might compromise Splunk's reputation or the interests of its customers as defined in section 1.1.

3. Scope of policy

3.1 This policy applies to the entire Splunk organization globally, i.e. Splunk Inc. and its U.S. and international subsidiaries.

3.2 This policy encompasses activities conducted remotely or on Splunk's premises.

3.3 Please see the Country provisions below in respect of your applicable jurisdiction (as set out in Appendices 1 – 4) and the referenced Splunk policies for more details that may apply in your jurisdiction. For the avoidance of doubt, to the extent there are any inconsistencies between this policy or any other policy and a jurisdiction-specific appendix, the jurisdiction-specific appendix will prevail.

4. Purpose of Policy

To enable and empower you to report concerns in a safe and reliable way, Splunk has implemented this policy, which outlines Splunk's procedures for receiving, assessing and investigating reports. You can submit reports confidentially, and if you wish, anonymously. Retaliation to reporting concerns is not tolerated and is a form of misconduct that will result in disciplinary action, up to and including termination of employment.

5. Exceptions

Exceptions to this policy must be escalated and approved by Splunk's Chief Ethics & Compliance Officer. Submit any exception requests to ceco_office@splunk.com.

6. Compliance

Employee concerns related to potential violations of this Policy may be reported through our Ethics and Compliance hotline. Any Splunk employee who violates this Policy may be subject to disciplinary action up to and including termination.

7. Related Policies, Procedures and Guidelines

Splunk Code of Business Conduct & Ethics

Global Preventing Harassment, Discrimination and Retaliation Policy

US Employee Handbook

International Employee Handbook

Splunk's Employee Data Protection Notice

Data Privacy Policy: Processing Personal Data Under Splunk's Control

Appendix 1
Australia

This appendix sets out Australian specific requirements and protections with respect to whistleblowing.

To the extent there are any inconsistencies between this appendix and the policy or any other policy, this appendix will prevail.

1. When is a report protected by Australian law?

An Eligible Whistleblower (defined below) who makes a report of information relating to Reportable Conduct directly to an Eligible Recipient (see paragraph 2 below) ("Protected Report") will be subject to protections under Australian law and as outlined in this appendix.

You are an Eligible Whistleblower if you are a current or former:

- officer, employee, associate (i.e. a director or secretary of Splunk Australia or of a related body corporate to Splunk Australia), contractor, consultant, secondee or volunteer or (paid or unpaid) supplier (including any employee of such a contractor or supplier) of Splunk Australia; or
- relative or dependent of any of these persons, or their spouse.

A report concerns Reportable Conduct if you have reasonable grounds to suspect that the information indicates the matters discussed at paragraph 1.1 of the policy. In Australia, there is no requirement for a report to be made in good faith, however, you may still be pursued for having made an intentionally false report.

As set out in paragraph 1.1 of the policy, a personal work-related grievance is not Reportable Conduct. However, reports of threatened or actual detriment/ retaliation as a result of making a personal work-related grievance are Reportable Conduct.

The protections in paragraph 6 of this Appendix apply only to Reportable Conduct.

Eligible Recipients

In addition to the Eligible Recipients set out in section 1.3 of the policy, the following are also Eligible Recipients:

- officer or senior manager of Splunk Australia or other corporate entity related to Splunk Australia;
- Splunk Ethics and Compliance Hotline which is available 24 hours, 7 days a week by phone: 1-800-551-155 or 1-800-881-011 (at the prompt, dial 844-649-6910) or you can access the website at splunk.ethicspoint.com; and
- auditors (including any member of the audit team) or actuaries of Splunk Australia.

You are encouraged to first make the report to one of the Eligible Recipients listed above. Where necessary, reports may also be made to the Australian Securities and Investment Commission ("ASIC"), Australian Prudential Regulation Authority ("APRA") and the Commissioner of Taxation.

You may make a report to a lawyer for the purpose of obtaining legal advice or legal representation in relation to your rights at law in relation to whistleblowing and it will be a Protected Report.

2. Public Interest Disclosure and Emergency Disclosure

In certain circumstances, 90 days after you have made a report in accordance with this policy to a relevant external regulator such as ASIC or APRA, and provided that you have reasonable grounds to believe that:

- no action is being, or has been, taken by the initial recipient of your report to address the matters you raised in your report; and
- the making of a further disclosure would be in the public interest, then,

subject to you first giving written notice to the initial recipient of your report at the end of the 90 day period and informing them of your intention to make a public interest disclosure, you may give limited disclosure of the matter to a member of Parliament or a journalist (“Public interest disclosure”).

In certain circumstances where you have made a report to a relevant external regulator such as ASIC or APRA and provided you have:

- reasonable grounds to believe that the information concerns a substantial and imminent danger to health or safety of one or more persons or to the natural environment; and
- given written notice to the initial recipient of your report that informs them of your intention to make an emergency disclosure,

you may give limited disclosure of the matter to a member of Parliament or a journalist (“Emergency disclosure").

Making a Public Interest Disclosure or Emergency Disclosure is a serious matter and, to ensure you are protected by law, you should obtain independent legal advice before taking any such step.

3. How will Protected Reports be investigated?

In addition to the matters discussed at paragraphs 1.5 and 1.6 of the policy, as a general guide and subject to the particular circumstances, the steps in the investigation process will include the following:

- to ask you if you consent to the disclosure of your identity for the purposes of the investigation. If you provide your consent, Splunk Australia will keep a written record of that consent;
- interview you to obtain relevant information;
- interview any alleged wrongdoer to obtain a response to the report in so far as it relates to the alleged wrongdoer. Inform the alleged wrongdoer of the substance of the report, as far as it applies to them;
- interview any relevant witnesses regarding relevant matters arising from the report. Inform the witnesses of the substance of the report, as far as it applies to them;
- review any documents or other material relevant to the report;
- if necessary, conduct further interview/s with you to obtain further information or a response to material arising from the investigation;
- if necessary, conduct further interview/s with any alleged wrongdoer regarding further material arising from the investigation;
- provide the alleged wrongdoer with a reasonable opportunity to respond to any matter referred to in the report relating to them and any potential adverse finding, before the investigation is finalised; and
- prepare a report making findings of fact and determine whether a disclosure has been substantiated or not substantiated, in whole or part. The report may also include recommendations arising from any factual findings.

The investigator will strive to conclude the investigation within a reasonable timeframe and will update you in accordance with section 1.6 of the policy.

4. Fair treatment

Splunk Australia will ensure fair treatment of employees mentioned or implicated in a Protected Report or to whom a Protected Report relates such as a witness ("Relevant Employee") by, in accordance with paragraph 1.4. of the policy, keeping the identity of the Relevant Employee confidential to the extent practicable and applying the following principles:

- Investigations will be conducted in a fair and impartial manner. An investigator must declare to Splunk Australia any material personal interest they have in any matter relevant to the investigation and then take no further part in the investigation unless directed otherwise.
- An investigation into a report will follow a fair process as outlined at paragraph 4 above.

5. Protections available to whistleblowers

If you make a Protected Report in accordance with this policy and appendix, you will receive the protections available by law including under the Corporations Act 2001 (Cth). These protections include:

6.1 Protection of Identity (Confidentiality)

In accordance with paragraph 1.4 of the policy, you are not required to provide your name or any other identifying information when making a Protected Report. If you provide such details in connection with a Protected Report, you are entitled to have your identity (including any information that is likely to lead to your identification) kept confidential, subject to applicable law.

Your identity may be disclosed with your consent. Your identity may be disclosed without consent to ASIC, APRA, a member of the Australian Federal Police or to a lawyer for the purpose of obtaining legal advice or representation in connection with the operation of whistleblower laws.

Information may also be disclosed so long as the information is not your identity, it was reasonably necessary to disclose the information for the purpose of investigating the Protected Report, and all reasonable steps were taken to reduce the risk that you would be identified.

6.2 Protection against retaliation

You are entitled to protection from any actual or threatened detriment to yourself or to a third person (e.g. a friend, colleague, or family member) for making a Protected Report. In relation to section 1 of the policy, in Australia, there is no requirement for you to make the report in good faith to be protected from retaliation, however, you may still be pursued for having intentionally made a false report.

In Australia, detriment is legally defined as including dismissal from employment, injury in employment, disadvantageous alteration to your position or duties, discrimination, harassment or intimidation, harm or injury (including psychological harm), or damage of any kind (including damage to property, reputation, business or financial position).

Splunk Australia will endeavor to protect you from any actual or threatened detriment arising from your Protected Report. If you believe that you have been subjected to, or threatened with being subjected to, detriment in connection with a Protected Report, you should immediately report the alleged detrimental conduct to Splunk Australia.

Under applicable legislation, you may be able to seek compensation and other remedies through the courts if you suffer loss, damage or injury because you made a Protected Report or if Splunk Australia fails to take reasonable precautions and exercise due diligence to prevent you from suffering detriment.

6.3 Other immunities

If you make a Protected Report, you are entitled to certain statutory immunities, including:

- immunity from any civil, criminal or administrative legal action (including disciplinary action for making the Protected Report);
- no contractual or other remedy may be enforced, and no contractual or other right may be exercised against you on the basis of the Protected Report;
- in some circumstances, the information disclosed will not be admissible in evidence against you in criminal proceedings or in proceedings for the imposition of a penalty.

However, you may still be pursued for having intentionally made a false report or in connection with your own conduct which is revealed by the matters highlighted in the disclosed information (i.e. your own conduct in the misconduct, improper affairs or other circumstances which are revealed by the protected disclosure).

6.4 Protection of records

Splunk Australia will take reasonable precautions to securely store any records relating to a report of wrongdoing and permit access to authorized persons only. You can be assured that an unauthorized release of information in breach of this policy will be regarded as a serious matter.

6. Support for whistleblowers

If you make a Protected Report, you will have reasonable access to support made available by Splunk Australia such as contact with a nominated person and access to Splunk's Employee Assistance Program (“EAP”).

7. Access to policy

A copy of this policy and this appendix will be made available via Splunk’s Legal Pwny Portal Site. Splunk Australia will take steps to ensure that its employees are made aware of this policy and appendix.

Appendix 2
France

Employees in France are bound by Splunk France's Whistleblowing Policy and must follow that at all times.

For the avoidance of doubt, to the extent there are any inconsistencies between the French Whistleblowing Policy and the policy or any other policy, the French Whistleblowing Policy will prevail.

Appendix 3
Japan

This appendix sets out Japanese specific requirements and protections with respect to whistleblowing.

To the extent there are any inconsistencies between this appendix and the policy or any other policy, this appendix will prevail.

1. Scope of this policy

In addition to the list included in paragraph 3.1 of the policy, in Japan, this policy will also apply to the following:

- former directors, former officers, former employees and former dispatch workers who retired or resigned from Splunk within one year of the date on which the Reportable Conduct is reported; and
- any agency or contingent workers (including dispatch workers) who have worked for Splunk within one year of the date on which the Reportable Conduct is reported.

Appendix 4
Netherlands

This appendix sets out Dutch specific requirements and protections with respect to whistleblowing.

For the avoidance of doubt, to the extent there are any inconsistencies between this appendix and the policy or any other policy, this appendix will prevail.

1. Who can report Reportable Conduct?

In addition to the list included in paragraph 2.1 of the policy, in the Netherlands, this policy will also apply to the following:

- any former employees, board members, directors, officers, contractors, consultants and interns previously engaged by Splunk;
- any shareholders, members and holders of voting rights in shareholders' meetings and job applicants; and
- any (sub)contactors, including their members and staff, engaged by Splunk.

2. Raising a concern through a physical meeting

In addition to reporting Reportable Conduct through the reporting channels as set out in paragraph 1.3 of the policy, you may request a physical meeting. In such a meeting, your report is recorded through a recording of the conversation or through minutes of the meeting (in which case, you will be given the opportunity to review, correct and sign such minutes).

3. Legal Advice

In the Netherlands, you may consult an external legal advisor in confidence about a suspected Reportable Conduct at your own expense. Any such external legal advisor is obliged to keep any information shared by you confidential and any such third party legal advisor may report Reportable Conduct on your behalf, following the procedure as set out in paragraph 1.3 of this policy.

4. No Retaliation of any persons assisting you

The protection of a whistleblower as referred to in paragraph 1 of this policy is extended to any person assisting or advising you when reporting Reportable Conduct, including any legal entities controlled by you, for which you work, or to which you are linked in a professional context.