

A10 NETWORKS, INC.
POLICY REGARDING REPORTING OF
ACCOUNTING AND AUDITING MATTERS

(Adopted as of May 18, 2018)

A10 Networks, Inc. (the “**Company**”) is committed to maintaining high standards of financial integrity, and the Audit Committee of the Board of Directors of the Company takes very seriously all complaints and concerns regarding accounting, internal accounting controls and auditing matters. The Company’s financial information guides the decisions of the Board of Directors and management and is relied upon by the Company’s stockholders, employees and business partners. The Company’s policies and practices have been developed to maintain the highest business, legal and ethical standards.

For these reasons, the Company must maintain a workplace environment where employees who reasonably believe that they are aware of questionable accounting, internal accounting controls or auditing matters, or of the reporting of fraudulent financial information, can raise these concerns free of any harassment, discrimination or retaliation. It is the Company’s policy to encourage its employees to report those concerns as soon as possible after discovery. The Company strives to encourage open communication so that such concerns may be raised without fear of retaliation in any manner.

Accordingly, the Audit Committee has established the following procedures for:

- The receipt, retention and treatment of complaints regarding accounting, internal accounting controls, or auditing matters; and
- The confidential, anonymous submission by the Company’s employees of concerns regarding accounting or auditing matters they believe to be questionable.

The Audit Committee is committed to continuously reviewing and updating its policies and procedures. Therefore, these procedures are subject to modification. Please note that a jurisdiction-specific Policy regarding Reporting of Accounting and Auditing Matters may provide additional guidance regarding the subject matter of this document in your jurisdiction. In the event of a conflict between this document and any such jurisdiction-specific policy, the jurisdiction-specific policy shall take precedence to the extent of the conflict.

A. Receipt of Complaints

1. Non-employees may submit complaints regarding accounting, internal accounting controls, or auditing matters by mail to:

A10 Networks, Inc.
3 West Plumeria Drive
San Jose, CA 95134
Attn: General Counsel

2. Employees may submit concerns regarding accounting, internal accounting controls, or auditing matters they believe to be questionable (confidentially and anonymously, if they wish) in one of the following ways:

- Via electronic mail to the General Counsel [at generalcounsel@a10networks.com](mailto:generalcounsel@a10networks.com);
- Via the Company's third party hotline vendor at the telephone number shown in the Company's Employee Handbook, on its internal WIKI, or intranet;
- Via the website of A10's hotline vendor, at the website shown in the Company's Employee Handbook, on its internal WIKI, or intranet;
- Via regular mail as set forth above; or
- Via electronic mail to the Audit Committee at the email address published for this purpose in the Company's Employee Handbook, on its internal WIKI, or intranet.

3. The methods of submitting complaints shall be published on the Company's external and internal websites in such manner as the General Counsel, in consultation with the Audit Committee, deems appropriate. It shall be emphasized to employees that each of the methods of submitting complaints listed above may be used anonymously and that such complaints shall be treated confidentially.

4. Except for complaints sent directly to the Audit Committee, all complaints will be forwarded to the General Counsel's office for coordination of their treatment as set forth below.

C. Treatment of Complaints

1. All accounting and auditing complaints received shall be entered on an accounting and auditing matters log, which shall include, among other things, information regarding the date the complaint was received, a description of the complaint, the submitter (if provided), and the status and disposition of an investigation of the complaint. Receipt of the complaint will be acknowledged to the sender, within a reasonable period following receipt, if appropriate information for response is supplied.

2. Non-accounting or non-auditing complaints shall be logged separately and will be forwarded to the appropriate person or department for investigation (e.g., human resources or legal), unless the General Counsel deems other treatment is necessary (e.g., such complaint involves a finance employee or executive officer).

3. With respect to complaints not initially directed to the Audit Committee regarding accounting or auditing matters, the General Counsel and/or internal audit or compliance function will report immediately to the Audit Committee matters he deems significant (e.g., allegations of fraud or allegations of accounting or auditing matters it believes to be questionable involving executive officers). The Audit Committee shall direct and oversee an investigation of such complaints, as well as any complaints initially directed to the Audit Committee, as it determines to be appropriate.

4. All other complaints regarding accounting or auditing matters shall be reviewed under the direction and oversight of the General Counsel, who will involve such other parties (e.g., members of the finance department or outside advisors) as deemed appropriate. The General Counsel shall provide the Audit Committee with a quarterly report of all accounting or auditing complaints received and an update of pending investigations. The Audit Committee may request special treatment for any complaint and may assume the direction and oversight of an investigation of any such complaint.

5. Confidentiality will be maintained to the fullest extent possible, consistent with the need to conduct an adequate review.

6. In all cases, prompt and appropriate corrective action shall be taken as determined by the Audit Committee. An employee may be subject to disciplinary action, which may include the termination of his or her employment, if the employee fails to cooperate in an investigation or deliberately provides false or misleading information during an investigation. The specific action that will be taken in response to a report will depend on the nature and gravity of the conduct or circumstances reported and the quality of the information provided. Where questionable accounting, internal accounting controls or auditing matters or the reporting of fraudulent financial information is verified, corrective action will be taken and, if appropriate, the persons responsible will be disciplined.

7. Reprisal, threats, retribution or retaliation in any way against any person who has in good faith made a complaint or reported a concern, or against any person who assists in any investigation or process with respect to such a complaint or concern, is prohibited. Employees who believe that they have been subjected to any discrimination, retaliation or harassment for having submitted a complaint regarding questionable accounting, internal accounting controls or auditing matters, or the reporting of fraudulent financial information under this policy or participating in an investigation relating to such a complaint, should immediately report the concern to the General Counsel or to any of his supervisors. Any complaint that such discrimination, retaliation or harassment has occurred will be promptly and thoroughly investigated. If such a complaint is substantiated, appropriate disciplinary action will be taken, up to and including termination.

6. When appropriate, the General Counsel or Audit Committee will report the results of any investigation regarding a complaint, including any corrective actions taken, to the person making the complaint, if appropriate information for response was supplied, maintaining the anonymity of the person making the complaint to the fullest extent possible.

B. Retention of Complaints

The General Counsel shall retain written complaints, the accounting and auditing matters log and all related documentation as required under applicable law.

C. Supplemental European Privacy Notice

1. European Union Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“**EU GDPR**”) requires the Company as the data controller to provide certain information about its data processing practices to individuals in the European Economic Area (“**EEA**”). If you are located in the EEA and report an individual or are the subject of a report pursuant to the procedures outlined herein, this Supplemental European Privacy Notice applies to you. The Company’s representative in the EEA for the purposes of the EU GDPR is A10 Networks Limited, Reading Green Park, 450 Brook Drive, Green Park, Reading, Berkshire, RG2 6UU.

2. The following categories of personal data may be processed in connection with the procedures outlined in this policy:

- Identity, functions and contact details of the reporter;
- Identity, functions and contact details of the person or persons who are the subject of the reporting;
- Personal data contained in the reported facts; and
- Personal data collected in connection with the investigation of the reported facts.

3. The Company processes your personal data in connection with its review and consideration of reports submitted pursuant to this policy, and the determination of appropriate actions to be taken in response to such reports. The Company processes your personal data on several different legal bases, as follows:

- **Based on compliance with legal obligations (per Article 6(1)(c) of the EU GDPR):** The Company processes your personal data to comply with relevant laws, regulatory requirements and to respond to lawful requests, court orders, and legal process.
- **Based on legitimate interests (per Article 6(1)(f) of the EU GDPR):** The Company processes your personal data to realize a justified interest based on an assessment of the Company's legitimate interests and the data subject's privacy and other fundamental interests. Such legitimate interests may include investigating and taking appropriate action related to a potential breach of an agreement, the Company's business, legal or ethical standards, or a potential contravention of applicable laws that has been, is being or will be committed.

4. The information collected in the report may be disclosed to advisors (such as legal, auditing, finance and accounting advisors or consultants) to pursue the legitimate interests outlined above, law enforcement or government authorities as necessary to comply with legal requirements or in the course of a legal action, and to legitimate recipients of communications under applicable laws, where required by law or necessary for the purpose of, or in connection with, any legal proceedings. The information may also be provided to service providers acting as data processors for the Company (*e.g.*, an IT services provider) where required for the performance of their services.

5. Depending on the situation, some recipients located outside of the EEA may be located in countries for which the European Commission has issued adequacy decisions. In each case, the transfer is thereby recognized as providing an adequate level of data protection from a European data protection law perspective (per Article 45 of the EU GDPR).

6. Depending on the situation, some recipients may be located in countries for which the European Commission has not issued an adequacy decision in respect of the level of data protection provided therein. By entering into appropriate data transfer agreements based on Standard Contractual Clauses (2010/87/EU and/or 2004/915/EC) as referred to in Article 46(5) of the EU GDPR or other adequate means, the Company has established that all such recipients will provide an adequate level of data protection and that appropriate technical and organizational security measures are in place to protect personal data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure or access, and against all other unlawful forms of processing. Any onward transfer is subject to appropriate onward transfer requirements as required by applicable law. A copy of any such data transfer agreement may be requested by writing to the contact details below.

7. Any information collected as a result of a report using the procedures outlined herein will be kept only as long as necessary and for the purpose for which it has been collected in compliance with applicable law.

8. Under the conditions and circumstances set out under the EU GDPR, you have the following rights:

- **Right of access:** You have the right to obtain from the Company confirmation as to whether your personal data is being processed, and, where that is the case, to request access to and information about the processing of such personal data.
- **Right to rectification:** You have the right to obtain from the Company the rectification of inaccurate personal data concerning you. Depending on the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- **Right to erasure (to be forgotten):** You have the right to ask the Company to erase your personal data.

- **Right to restriction of processing:** You have the right to request restriction of processing of your personal data, in which case, it would be marked and processed by the Company only for certain purposes.
- **Right to data portability:** You have the right to receive your personal data which you have provided to the Company in a structured, commonly used and machine-readable format and you have the right to transmit the personal data to another entity without hindrance from the Company.
- **Right to object:** You have the right to object, on grounds relating to your particular situation, to the processing of your personal data by the Company and the Company can be required to no longer process your personal data.

Please note that these rights might be limited under the applicable national data protection law. You also have the right to lodge a complaint with the competent supervisory authority.

9. Unless prohibited by local law, your provision of personal data as a reporter in accordance with the procedures outlined herein is voluntary. Failing to provide certain or any personal data may delay or make it impossible for the Company to act upon any report you submit. If you are the subject of a report, the collection of your personal data under the procedures herein may take place without your knowledge or consent. We only process such personal data in accordance with applicable laws.

10. If you would like more information about our use of your personal data, or if you have any other questions concerning this Supplemental European Privacy Notice, you may contact dataprivacy@a10networks.com.