Alpha Data

networking audio visual cabling telecom enterprise networking audio visual cabling telecom enterprise

WHISTLEBLOWING POLICY
[May 2025]

Version Number:	1
Approved Date:	May 14, 2025
Document Owner:	Board of Directors

UPDATING

The document owner will issue updates to all registered holders of each "hard copy" of this document. The registered holder will be responsible for updating the document by replacing pages or sections as instructed. Printed copies will automatically assume "unmaintained" status.

Table of Contents

1. Introduction **5**

1.1. Document Custodian 5

1.2. Document Maintenance 5

1.3. Document Purpose 5

2. Policy **8**

2.1. Policy Commitment 8

2.2. Reporting 9

2.3. Investigation 10

2.4. Abuse of Reporting Process 12

2.5. Confidentiality 12

2.6. Policy Implementation Training 13

3. Appendices **14**

Appendix 1: Policy Definitions 14

Appendix 2: Abbreviations 16

Appendix 3: Contact Details 16

1. Introduction

1.1. Document Custodian

1.1.1. This Policy is owned by Alpha Data [PJSC] ("**Alpha Data**" or the "**Company**"), which has ultimate responsibility for implementing these policies.

1.2. Document Maintenance

1.2.1. This Policy shall be reviewed annually by Alpha Data to ensure applicability and continuity in line with the approved Delegation of Authority Matrix ("**DoA**").

1.2.2. Any changes to this Policy may be requested to and/or initiated by Alpha Data under the following circumstances:

a) There is a consensus that change is needed, a new Policy direction is required, or that old strategies are not working as well as they could;

b) The current Policy exposes Alpha Data to unnecessary risk;

c) Practical application of this Policy identifies issues and requires appropriate action to remedy these issues;

d) The current Policy does not reflect industry best practice; and/or

e) There are changes to the Applicable Laws and regulations.

1.2.3. Any proposed amendments to this Policy shall be approved by the Board of Directors (the "**Board**") and incorporated into this Policy.

1.2.4. An amendments table will be kept to record the changes in the document, along with an approvals table which will be kept to record the approval of new versions of this Policy from time to time.

1.3. Document Purpose

1.3.1. This Policy shall be adopted to ensure that Concerned Parties are confident that they can raise any matters of genuine concern without fear of retaliation, in the knowledge that they will be taken seriously and that the matters will be investigated appropriately and regarded as confidential.

1.3.2. Whistleblowing shall be distinguished from simply raising a grievance through normal channels. Its aim is to prevent harm to others or to Alpha Data as a whole, rather than to secure Whistleblower's personal interest.

1.3.3. Other forms of complaints shall be directed to the concerned Company division/department. However, complaints (e.g., complaints relating to violence or threatened violence, harassment or bullying, discrimination, sexual harassment, or unsafe workplaces, systems, or practices, etc.) shall be directed to the Company's Internal Audit Department and will be dealt with in accordance with the relevant Company policies and procedures. Accordingly, this Policy is not intended to replace any Employee grievance or other established Company policies and procedures.

1.3.4. Alpha Data is committed to ethical conduct and fair and honest dealing with its customers, Employees, consultants, and contractors.

1.3.5. Alpha Data expects its policies to be respected and applied by all Employees and to be informed of any non-compliance or misconduct.

1.3.6. This Policy sets the framework and the related internal controls to be followed for managing reported irregularities and non-compliance to Alpha Data's policies and procedures. The objective of this Policy is to establish policies and procedures for:

a) The submission of concerns regarding any misconduct or non-compliance with the law, Alpha Data policies, or unethical, unfair or dishonest dealings; and

b) The receipt, retention, and treatment of complaints received;

c) The protection of those reporting any of the above concerns from retaliatory actions or victimization.

1.3.7. This Policy applies to any irregularity, or suspected irregularity, involving Employees, Executive Management, Board Members and Board Committee Members, as well as Shareholders, consultants, contractors, suppliers, and/ or any other parties who have a business relationship with Alpha Data regarding, but not limited to:

a) Financial Fraud (e.g., Incorrect financial reporting, Embezzlement, Misappropriation of funds);

b) Data and Information Security:

- Unauthorized access or disclosure of sensitive information
- Data theft or manipulation
- Cybersecurity breaches

c) Intellectual Property Theft:

- Unauthorized use or theft of intellectual property

- Patent or copyright infringement

d) Human Resources Misconduct:
    - Fraudulent hiring or promotion practices
    - Employee benefit fraud

e) Theft;

f) Corruption and Bribery involving:
    - Illegal gratuities
    - Fraud, kickbacks, bid rigging, etc.
    - Conflict of interest in purchasing or sales

g) Misuse of Company Information;

h) Damage to property;

i) Fraudulent disbursements;

j) Activities that are not in line with Alpha Data's policies and procedures, including Alpha Data's Code of Conduct; or

k) Activities, which otherwise amount to serious improper conduct.

2. Policy

2.1. Policy Commitment

2.1.1. This Policy is intended to encourage and enable all Board and Board Committee Members, Employees, and consultants/contractors of Alpha Data to raise any in-scope concerns within the organization for investigation and appropriate action. With this goal in mind, the ("**complainant**") who, in good faith, reports a concern shall not be subject to any retaliation.

2.1.2. The following safeguards shall be instituted by the Executive Management:

a) Harassment or victimization for reporting concerns under this Policy shall not be tolerated. Victimization could include:

- Threats;
- Harassment;
- Intimidation;
- Discrimination;
- Action causing injury, loss, or damage; and/or
- Adverse treatment in relation to a person's employment, career, profession, trade, or business.

b) Every effort shall be made to treat the complainant's identity with appropriate regard for confidentiality.

c) Concerns expressed anonymously shall be explored appropriately, but consideration will be given to the:

- Seriousness of the issue raised;
- Credibility of the concern; and
- Likelihood of confirming the allegation from attributable sources.

d) Any Board Member or Employee who retaliates against someone who has reported a concern in good faith shall be subject to disciplinary action.

e) Allegations reported in bad faith shall result in disciplinary action.

2.2. Reporting

2.2.1. Any Concerned Party who discovers or suspects any reportable conduct may report their concerns to Alpha Data's Internal Audit Department via phone, email, or letter. Contact details are set out in Appendix 3 of this Policy. This Policy shall be available and posted clearly (along with all other Company policies) on Alpha Data's HR portal.

2.2.2. Reporting via the whistleblowing communication/report channel(s) above can be done anonymously as well. Anonymous reporting shall be made in good faith.

2.2.3. Alpha Data is committed to maintaining the highest standards of ethics and integrity. In line with this commitment, we encourage employees to report any concerns or irregularities they observe. Employees can confidently report such matters through the designated whistleblowing channel: Whistleblowing@alpha.ae.

2.2.4. Alpha Data's Internal Audit Department shall properly and preliminary, screen each report as far as information is reasonably available and in accordance with privacy requirements and may request additional reasonable information from the person making the report through the whistleblowing system/tool while maintaining anonymity.

2.2.5. It shall be noted that the preliminary assessment performed by the Internal Audit Department to any reported breaches, as referred in clause 2.2.4 above, shall categorize the materiality and severity of the breach into two main categories:

- Minor Breach: a breach that does not have a material impact on the company (whether it be financial, reputational, etc.) and in this case, breaches can be resolved with an immediate remediation and action plan accordingly. Examples of minor breaches include, but are not limited to, unauthorized use of Company resources and/or unintentional sharing of non-sensitive company data due to oversight, which can be quickly remediated without causing significant harm.
- Major Breach: a breach that has a material impact on Alpha Data, and in this case, a formal investigation shall be triggered to investigate the issue in line with the procedures set forth in Section 2.3 below. Examples of major breaches include, but are not limited to, Fraud or Theft, Significant Data Breach, and/or Regulatory Non-Compliance.

2.3. Investigation

2.3.1. Compliance breaches may be identified through one of the following channels:

a) Whistleblowing cases filed in line with the whistleblowing channels at Alpha Data.

b) Incidents identified by the Compliance Department as part of the continuous compliance monitoring process.

c) Audit findings observed during regular or special internal audit reviews (as requested by the "**ARCC**"). It shall be noted that the Compliance Department shall be responsible to communicate the related whistleblowing findings to the Internal Audit Department to perform the preliminary assessment in accordance with the procedures set out in clause 2.2.5 above and to the ARCC as applicable.

2.3.2. Following any of the above, the Internal Audit department shall acknowledge the reported incident within (2) two working days and make the appropriate arrangements for investigations as per the below steps (chronologically):

a) Preliminary Assessment: Verify and evaluate reported issues and concerns, determine the necessary next steps accordingly.

b) Investigation: Investigate based on evidence and factual information, in case it has been found after the preliminary assessment to be a major breach.

c) Case Closure: Develop and report conclusions and recommendations and close the case.

2.3.3. All reported incidents shall be dealt with by an Investigation Committee / (team), which is headed by the Head of Internal Audit and reports to the Audit Risk and Compliance Committee. The members of any investigation team/committee shall be decided as per the Delegation of Authority Matrix and shall include the relevant stakeholders based on the job grade of the individual against whom the investigation shall be held and/or the materiality of the reported incident (materiality shall be assessed based on the financial and reputational impact of the reported incident).

2.3.4. All reported incidents shall be disclosed to the Audit Risk and Compliance Committee Chairman, and approval shall be sought for cases requiring further investigations.

2.3.5. Should the matter reported require a qualified Third Party to conduct an investigation, the Audit Risk and Compliance Committee shall appoint an investigation officer for this purpose.

2.3.6. All reported allegations shall be thoroughly investigated to the extent that relevant information is available to the investigating team/committee with the objective of identifying evidence to substantiate or refute the claims.

2.3.7. The length and scope of the investigation shall depend on the subject matter of the disclosure. A report shall be produced, and copies shall be provided to the Audit Risk and Compliance Committee.

2.3.8. If the investigation substantiates that anomalous activities have occurred, a report shall be issued to the CEO to action the recommendations and who shall provide the Audit Risk and Compliance Committee with updates on the implementation of the recommendations.

2.3.9. Decisions on appropriate disciplinary actions following the closure of an investigation including termination shall be initiated by the HR Department in collaboration with the Internal Audit Department after consultation with Executive Management and shall be approved in line with the DoA. The Audit Risk and Compliance Committee shall be informed on the same.

2.3.10. In case an incident is submitted against an employee who has a direct reporting relationship with the CEO or other member of the Executive Management (N-1 or below), the CEO or concerned Executive Management member shall not be involved in any stage or form of the investigation. Decisions on appropriate disciplinary actions against the CEO or concerned Executive Management member, shall be made by the Audit Risk and Compliance Committee with the Board informed as per the DoA.

2.3.11. Decisions to prosecute or refer the investigation results to law enforcement and/or regulatory agencies for independent investigation shall be made by the Internal Audit Department in consultation with the Legal Department, Compliance Department and Human Resource Department following the recommendations of the Audit Risk and Compliance Committee.

2.4. Abuse of Reporting Process

2.4.1. All reports made under this confidential reporting process shall be made in good faith.

2.4.2. Malicious reporting or unfounded allegations shall be treated as a serious breach of Alpha Data's Code of Conduct.

(Refer to Alpha Data's Code of Conduct for further information)

2.5. Confidentiality

2.5.1. Alpha Data recognizes that disclosures made in accordance with this Policy may involve highly confidential and sensitive matters and that Whistleblowers may opt for anonymity. The investigating team shall treat all received information with utmost confidentiality.

2.5.2. The identity of the Whistleblower, as well as any information that could potentially reveal his/her identity, shall not be disclosed to any individual not directly involved in the investigation or resolution of the report. No information regarding the status of an investigation shall be divulged. The proper response to any inquiries shall be, "**I am not at liberty to discuss this matter.**"

2.5.3. Under no circumstances shall any reference be made to "**the allegation**", "**the crime**", "**the fraud**", "**the forgery**", "**the misappropriation**" or any other specific reference.

2.5.4. Investigation results shall remain confidential and shall only be disclosed to individuals with a legitimate need to know. This practice is essential to prevent reputational harm to individuals suspected but later cleared of wrongdoing and to safeguard Alpha Data from potential civil liability as well as provide protection and support for Whistleblowers.

2.5.5. No Employee who raises genuine concerns in good faith under this Policy shall be dismissed or subjected to any form of detriment as a result of their actions. Detriment encompasses unwarranted disciplinary actions and victimization. Should a Whistleblower believe he/she is facing retaliation or detriment in the workplace due to raising concerns under this Policy, he/she is encouraged to promptly inform the ARCC. Employees who engage in victimization or retaliation against Whistleblowers shall be subject to disciplinary action. Those who choose to make disclosures without adhering to this Policy may not benefit from the protections outlined herein.

2.5.6. Depending on the nature of the case and at the discretion of the ARCC, the Company may provide legal support and/or counseling to the Whistleblower. This support is aimed at ensuring the Whistleblower's well-being and protection while upholding the integrity of the whistleblowing process.

2.6. Policy Implementation Training

2.6.1. All the employees and the ARCC shall receive periodic training on the principles set out in this Policy, which may include testing to ensure understanding. Certain high-risk areas of the business may also receive relevant supplemental training as determined by Alpha Data's Internal Audit Department in consultation with the Risk Department.

3. Appendices

Appendix 1: Policy Definitions

Term	Definition
Applicable Laws	All laws, decisions, and regulations of the UAE, the Emirates Securities and Commodities Authority, and any other authority of the UAE relating to the trading, clearance, settlement, transfer of ownership and custody of securities which relate to or regulate the Company's Securities.
Board	The Board of Directors for Alpha Data is appointed by the Shareholders from time to time. Where a Board approval or resolution is required, it shall be deemed to include any Committee duly formed on behalf of the Board whose charter, terms of reference, or similar mandating document provides it authority to exercise certain authorities on behalf of the Board.
Board Member(s)	Any member of the Company's Board of Directors, including the Chairman of the Board of Directors.
Board Committe Member(s)	Any Alpha Data Board Committee Member.
Company	Alpha Data and its Branch, a publicly listed Company on ADX.
Complainant	Any party who works at or related to Alpha data who makes the complaint in a legal action or proceeding.
Concerned Parties	All individuals working for and/or with Alpha Data at all levels and grades including, members of the Executive Management, senior managers, Employees (comprising permanent, temporary, and part-time employees), trainees, suppliers, vendors, and the Company's branches and joint ventures entities.
Employee(s)	An employee of Alpha Data, which includes temporary, permanent, full-time, and part-time employees.
Executive Management	The CEO and his/her direct reports who are responsible for managing the daily operations of Alpha Data and proposing and executing strategic decisions. Currently, it includes, among others, the CEO, CFO, CGO, CPO, and CTO.
N	First grade of Executive Management representing the CEO level of authority.
N-1	Second grade of Executive Management including any CxO reports to the CEO such as: CTO, CFO, CGO, CPO, etc.
Policy	Intentions and directions of an Organization, as formally expressed by its Top Management. (ISO 37301:2021)

Term	Definition
Securities	Financial instruments that hold some type of monetary value and can be traded on the financial markets
Shareholder(s)	Any person or entity who owns at least one share in Alpha Data.
Third Party/Parties	A person or body that is independent of the Organization. (ISO 37301:2021)
Whistleblower(s)	A person who informs on a person or organization regarded as engaging in an unlawful or immoral activity.

Appendix 2: Abbreviations

Abbreviation	Definition
ARCC	Audit, Risk and Compliance Committee
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CGO	Chief Growth Officer
CPO	Chief Product Officer
CTO	Chief Technology Officer
DoA	Delegation of Authority
HR	Human Resources
PJSC	Public Joint Stock Company

Appendix 3: Contact Details

Name:	Alpha Data Internal Audit Department
Address:	Alpha Data HQ Level 7, Addax Tower, Al Reem Island, Abu Dhabi, UAE
Tel:	xxx
Email:	xxx