



Whistleblowing Policy

Classification: Confidential – Internal Use Only

Effective Date: November 2025

1. Control Page

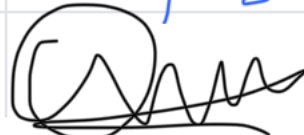
FIELD	DETAILS
Document Title	Whistleblowing Policy
Policy Number	OG-WBP-001
Version	1.0
Effective Date	November 2025
Next Review Date	November 2026 or within 30 days of a major incident, regulatory change, or Board directive
Policy Owner	Chief Security & Compliance Officer (CS&CO)
Prepared By	Compliance & Legal Office
Approved By	CEO, CCO, CS&CO
Document Classification	Confidential – Internal Use Only
Retention Period	7 years from closure of final case, stored securely (encrypted, access-controlled)



Distribution	All employees, directors, contractors, vendors with NDA; accessible via Internal Policy Repository
Related Documents	Code of Conduct, AML/CFT Policy, Risk Assessment Framework, Incident Response Plan, HR Handbook

2. Approvals

This policy has been reviewed and formally approved by the authorized executives of Orchestrate Global. Upon signing, this policy becomes binding and enforceable organization-wide.

NAME	POSITION	SIGNATURE	DATE
Preston Obadan	Chief Executive Officer		8/11/2025
Kevin Kegera	Chief Commercial Officer		8/11/2025
Oleksii Bondarenko	Chief Security & Compliance Officer		8/11/2025

Digital or physical signatures are valid under Orchestrate Global's Electronic Signature Policy.



3. Table of Contents

1. Introduction & Purpose
2. Scope & Applicability
3. Guiding Principles
4. Definitions
5. Types of Reportable Misconduct
6. Rights of Whistleblowers
7. Reporting Channels
8. Confidentiality & Anonymity Mechanisms
9. Roles & Responsibilities
10. Whistleblowing Process Lifecycle
11. Investigation Framework
12. Evidence Handling & Chain of Custody
13. Resolution, Corrective Action & Sanctions
14. Protection Against Retaliation
15. False or Malicious Reporting
16. Documentation, Recordkeeping & Data Security
17. Training, Awareness & Cultural Reinforcement
18. Continuous Monitoring & Audit
19. Policy Review & Amendment Control
20. Appendices



SECTION 1 – Introduction & Purpose

Orchestrate Global fosters a culture of transparency, integrity, and accountability. This Whistleblowing Policy establishes a secure, confidential, and retaliation-free mechanism for reporting actual or suspected misconduct.

Purpose:

- Enable safe reporting by employees, contractors, vendors, and third parties.
- Ensure impartial, timely, and confidential handling of concerns.
- Align with global standards in ethics, fraud prevention, financial crime control, and information security.
- Protect Orchestrate Global's operations, clients, reputation, and regulatory compliance.
- Guarantee consistent, fair investigations and corrective actions.

This policy applies uniformly—regardless of role, location, or employment type.

SECTION 2 – Scope & Applicability

CATEGORY	COVERED INDIVIDUALS
Employees	Full-time, part-time, probationary staff, interns, trainees
Executive & Board	Directors, C-level executives, committee members
Contractors/Vendors	Consultants, tech partners, outsourced providers
Third Parties	Payment processors, banks, KYC/KYB partners, auditors
Former Employees	Individuals aware of misconduct during prior engagement
Applicants	Individuals reporting misconduct during recruitment/onboarding



Geographic & Operational Scope:

All Orchestrate Global entities, subsidiaries, affiliates, digital infrastructure, remote work environments, and third-party systems processing company data or assets.

SECTION 3 – Guiding Principles

PRINCIPLE	DESCRIPTION
Confidentiality	Identity protected via “need-to-know” access, secure channels, anonymized case tracking
Non-Retaliation	Zero tolerance for adverse actions against good-faith reporters; strict sanctions for violations
Impartiality	Investigations conducted without conflict of interest
Fair Treatment	Accused presumed innocent; due process guaranteed
Timeliness	Acknowledgment within 7 days; investigation started within 14 days; resolution as soon as practicable
Legal & Ethical Integrity	Full alignment with Code of Conduct, anti-fraud policies, and ethical norms
Evidence Protection	Tamper-proof preservation of all relevant records and digital artifacts
Accessibility	24/7 reporting options, multilingual support (external portals), inclusive of all stakeholders



SECTION 4 – Definitions

TERM	DEFINITION
Whistleblower	Any person reporting wrongdoing in good faith under this policy
Whistleblowing	Reporting suspected misconduct, unethical behavior, or illegal activity
Report (or Disclosure)	Information alleging wrongdoing (written, verbal, anonymous, or documented)
Good Faith Report	Made with honest belief in accuracy, regardless of final outcome
Retaliation	Adverse action (e.g., termination, harassment) due to a protected disclosure
WBO – Whistleblowing Officer	Designated officer for initial receipt and triage of reports
Whistleblowing Review Committee (WRC)	Cross-functional team (Compliance, Legal, HR) overseeing investigations
Protected Disclosure	Report falling under Section 5, submitted via authorized channels
Anonymous Reporting	Disclosure without revealing identity
Chain of Custody	Chronological documentation of evidence handling to ensure integrity



Case Management System

Encrypted, access-controlled system for logging and managing cases

SECTION 5 – Types of Reportable Misconduct

5.1 Financial & Corporate Misconduct

- Fraud, embezzlement, fund misappropriation
- Falsified accounting or unauthorized transactions
- Unauthorized use of company/client assets
- Concealed conflicts of interest
- Bribery, kickbacks, unethical gifts

5.2 AML/CTF & Sanctions Violations

- Onboarding high-risk clients without due diligence
- Facilitating money laundering or tax evasion
- Failure to report suspicious activity
- Processing transactions for sanctioned entities
- Tampering with KYC/KYB data

5.3 Information Security & Data Protection

- Unauthorized access to systems or cardholder data
- Disabling security tools (SIEM, EDR, firewalls, HSMs)
- Destroying or concealing security logs
- Misuse of personal data or confidentiality breaches

5.4 Cryptographic Infrastructure Misconduct

- Mishandling of keys or HSM secrets
- Disabling MFA or tampering with access controls
- Unauthorized digital signing
- Non-compliance with key lifecycle procedures

5.5 Legal, Ethical & Workplace Violations



- Harassment, discrimination, bullying
- Coercion or abuse of power
- Hiring or procurement corruption
- Violations of Code of Conduct or supplier ethics

5.6 Health, Safety & Public Risk

- Unsafe working conditions
- Environmental or public safety negligence

5.7 Suppression of Information

- Instructing others not to report
- Destroying, altering, or hiding evidence
- Threatening or bribing individuals to stay silent

SECTION 6 – Rights of Whistleblowers

RIGHT	DESCRIPTION
Right to Report	No proof or expertise required to file a report
Right to Anonymity	Option to remain unidentified via approved anonymous channels
Right to Confidentiality	Identity shared only with WBO, WRC, or legal authorities under lawful compulsion
Right to Non-Retaliation	Protected from dismissal, demotion, harassment, or threats
Right to Information	Receive acknowledgment and post-investigation summary (if confidentiality permits)
Right to Fair Treatment	All reports handled respectfully and lawfully



Right to Escalate
Externally

May contact regulators or law enforcement if internal channels are unsafe or ineffective

SECTION 7 – Reporting Channels

7.1 Internal Channels

METHOD	ACCESS	CONFIDENTIALITY LEVEL
Dedicated Email	whistleblowing@orchestrate.global	Encrypted; restricted to CS&CO & WBO
Secure Web Portal	Internal portal (HTTPS, MFA, anonymous option)	Case ID generated; attachments supported
Whistleblowing Officer	Direct encrypted messaging or in-person	Strictly confidential
Physical Mail	“Confidential – Whistleblowing” to CS&CO	Sealed; stored in secured compliance archive

7.2 External Channels (if internal channels are compromised)

- Independent hotline (if available)
- External legal counsel
- Independent auditor or Board Audit Committee
- Law enforcement or regulatory authority (for severe violations)

SECTION 8 – Confidentiality & Anonymity Mechanisms

8.1 Identity Protection

- Shared only with WBO, WRC, or external authorities under legal compulsion.



- Never disclosed to direct managers or implicated parties.

8.2 Anonymous Reporting

- Supported via encrypted web portal or sealed postal mail.
- Updates provided via unique case ID—no identity required.

8.3 Data Security

- Reports encrypted (AES-256 or higher).
- Stored in role-based, access-controlled case management system (Legal, Compliance, HR only).
- SIEM-monitored for tampering.
- Retained 7 years post-case closure; destruction requires CS&CO approval.

SECTION 9 – Roles & Responsibilities

ROLE	RESPONSIBILITIES
Board of Directors	Oversight; receives quarterly anonymized summaries; handles executive-level allegations
CEO	Promotes transparency; ensures resource allocation for investigations
CS&CO	Policy owner; approves escalations; ensures conflict-free process; reports to CEO/Board
Whistleblowing Officer (WBO)	Receives, logs, triages, and secures reports; assigns case IDs; ensures confidentiality
WRC	Investigates (Legal, HR, Compliance, Internal Audit); recommends corrective actions



Internal Audit	Validates process integrity, evidence handling, and policy compliance
Legal Counsel	Advises on legal risks, regulatory obligations, and contractual liabilities
HR Department	Manages disciplinary outcomes; safeguards against retaliation
IT/Security Team	Secures digital evidence (logs, access records) under chain-of-custody protocols

SECTION 10 – Whistleblowing Process Lifecycle

10.1 Process Steps

STEP			
1	Report submission	Whistleblower	Anytime
2	Case logging & ID creation	WBO	Within 48 hours
3	Acknowledgment (non-anonymous)	WBO	Within 7 days
4	Preliminary assessment & classification	WBO + CS&CO	Within 14 days
5	Assignment for investigation	WRC	≤ Day 14
6	Full investigation	Investigation Team	14–60 days
7	Findings & closure report	WRC	≤ Day 90



8	Feedback to whistleblower	WBO	Post-closure
9	Secure archiving	Compliance	Upon case closure

10.2 Case Classification Levels

SEVERITY LEVEL	DESCRIPTION	ESCALATION PATH
Level 1	Minor policy breach; no financial impact	WBO only
Level 2	Misconduct, harassment, non-critical data issue	WRC + HR
Level 3	Financial fraud, data breach, AML failure	CS&CO + CEO
Level 4	Executive misconduct, systemic criminal activity	CEO + Board Audit Committee

SECTION 11 – Investigation Framework

11.1 Core Principles

- Impartiality: No conflict of interest
- Confidentiality: Limited stakeholder awareness
- Evidence-based: Conclusions supported by verifiable data
- Presumption of innocence: Accused may respond to allegations



11.2 Investigation Phases

PHASE	ACTIVITIES
Planning	Scope definition, investigator assignment, evidence source identification
Evidence Preservation	Immediate securing of logs, emails, financial records; freeze deletions
Interviews	Private, consent-recorded; signed statements generated
Analysis	Fact verification, policy breach identification, impact assessment
Review & Outcome	WRC evaluates findings; recommends corrective/disciplinary actions
Reporting	Formal report to CS&CO; Level 3–4 cases escalated to CEO/Board

SECTION 12 – Evidence Handling & Chain of Custody

12.1 Integrity Requirements

- Digital evidence: Forensic images with SHA-256/SHA-3 hash verification
- Physical evidence: Tamper-evident bags, sealed, signed, tracked
- Originals remain unaltered and secured

12.2 Chain of Custody Must Include:

- Item description (content, format, source)
- Date/time obtained
- Collector identity
- Access log (who, when)
- Storage location & method



- Integrity hash value

12.3 Storage Guidelines

EVIDENCE TYPE	STORAGE LOCATION	SECURITY CONTROLS
Digital Logs	Encrypted evidence vault	AES-256, access logs, MFA
Email/Files	Read-only case archive	Tamper-proof logs
Physical Documents	Locked cabinet (Compliance Office)	Dual-control access
Cryptographic Material	Secure HSM or encrypted device	No removal without WRC consent

SECTION 13 – Resolution, Corrective Actions & Sanctions

13.1 Investigation Outcomes

OUTCOME	DESCRIPTION
Substantiated	Evidence confirms misconduct
Partially Substantiated	Some claims validated
Unsubstantiated	No evidence—but report made in good faith
Malicious or False	Report intentionally false or harmful

13.2 Corrective Actions May Include:

- Personnel: Warning, suspension, demotion, termination



- Leadership: Reprimand, authority revocation, Board review
- Vendors: Contract suspension/termination, blacklisting
- Systems: Control enhancements, training, procedural updates
- Regulatory: Mandatory reporting where required
- Legal: Civil/criminal proceedings as warranted

SECTION 14 – Protection Against Retaliation

14.1 Zero-Tolerance Policy

Retaliation is strictly prohibited and subject to disciplinary action.

14.2 Examples of Retaliation

TYPE	EXAMPLES
Employment Retaliation	Termination, demotion, denied promotion, reduced pay
Harassment	Threats, intimidation, exclusion from meetings
Professional Retaliation	Unjustified negative reviews, removal from key projects
Subtle Retaliation	Social isolation, information withholding, excessive workloads

14.3 Reporting Retaliation

- Report via same channels as Section 7
- Treated with same urgency and severity as original misconduct

14.4 Sanctions

- Immediate disciplinary action (up to termination)
- Potential personal liability
- Reporting to authorities if legally warranted



SECTION 15 – False or Malicious Reporting

REPORT TYPE	TREATMENT
Good Faith (even if wrong)	Fully protected; no consequences
Deliberately False/Malicious	Disciplinary action, contract termination, legal liability

A report is deemed malicious if:

- Made with intent to deceive or harm
- Reporter knew information was false
- Motivated by personal gain or retaliation

SECTION 16 – Documentation, Recordkeeping & Data Security

16.1 Case File Contents

- Original report
- Case ID & timestamps
- Anonymity/confidentiality documentation
- Redacted communications
- Evidence & chain-of-custody records
- Interview transcripts & logs
- Final investigation report
- Disciplinary/corrective actions

16.2 Data Security Standards

REQUIREMENT	STANDARD
Data Retention	7 years post-case closure
Encryption	AES-256 at rest; TLS 1.2+ in transit
Access Control	Role-based + MFA



Tamper Detection	SIEM-monitored; no unauthorized deletion
Physical Security	Locked, restricted storage

SECTION 17 – Training, Awareness & Cultural Reinforcement

17.1 Mandatory Training

AUDIENCE	FREQUENCY
All employees	Within 30 days of hire + annually
Executives & People Managers	Annually (advanced ethics training)
HR, Legal, Compliance	Specialized confidentiality & investigation training

17.2 Awareness Activities

- Onboarding inclusion
- Internal portal summaries
- Periodic reminder communications
- Ethics and fraud prevention workshops

17.3 Certifications

- Annual acknowledgment of policy understanding
- Signed declaration of awareness of rights and obligations

SECTION 18 – Continuous Monitoring & Audit

18.1 Internal Audits

- Annual review by Risk & Compliance
- Process adherence and documentation verified



18.2 Key Performance Indicators (KPIs)

KPI	TARGET
Report acknowledgment time	≤ 7 days
Investigation completion	≤ 90 days
Confirmed retaliation cases	Zero tolerance
Annual training participation	100% of employees

18.3 Continuous Improvement

- Policy updated post-incident or based on audit findings
- Root cause analysis for systemic issues

SECTION 19 – Policy Review & Amendment Control

Reviewed annually or earlier if:

- Major whistleblowing case occurs
- Corporate structure or risk profile changes
- Audit identifies policy gaps

All amendments require approval from:

- Chief Security & Compliance Officer
- Chief Executive Officer
- Chief Commercial Officer or Board (for material changes)



SECTION 20 – Appendices

APPENDIX	TITLE
A	Whistleblowing Report Intake Form Template
B	Investigation Log Template
C	Chain of Custody Evidence Register
D	Confidentiality & Non-Retaliation Acknowledgment Form
E	Whistleblower Case Closure Report
F	Secure Recordkeeping File Structure & Retention Table

End of Document

This policy is binding upon approval and supersedes all prior versions.