

Septimius Security Code of Conduct

Administration Department

Primary contact:
a.alakhdar@septimiussecurity.com

AD-COC-V1-25

Form Issued Date: 31- December-2024

Form Next Planned Update: 31- December-2025



Revisions

Specify the significance from previous versions of the document

Rev.	Date	Revision Description
00	01/01/2022	Initial release of the document.
01	31/12/2023	Comprehensive review and updates, including layout improvements.
02	31/12/2024	Revisions to align with company standards, enhance document quality, and update layout.



Code of Conduct

Table of Contents

1. INTRODUCTION	4
2. HUMAN RIGHTS & ETHICAL CONDUCT COMMITMENT	4
3. PROFESSIONAL CONDUCT	5
4. PRINCIPLES OF USE OF FORCE	5
5. WHISTLEBLOWER PROTECTION & REPORTING VIOLATIONS.....	5
6. ANTI-BRIBERY & ANTI-CORRUPTION POLICY	6
7. CONFIDENTIALITY & IT SECURITY	6
8. WORKPLACE HARASSMENT & DISCRIMINATION PREVENTION	7
9. SOCIAL MEDIA & PUBLIC COMMUNICATIONS.....	7
10. EMPLOYEE ACCOUNTABILITY & DISCIPLINARY ACTION	7
11. COMPLIANCE, MONITORING & ANNUAL REVIEW.....	8
12. CONCLUSION	8



Code of Conduct

1. Introduction

The Septimius Security Code of Conduct defines the principles and ethical standards that govern our operations. This policy applies to all employees, contractors, subcontractors, and business partners.

Purpose of this Code

- Promote a culture of integrity, professionalism, and transparency.
- Ensure adherence to international security standards and human rights principles.
- Protect the reputation of Septimius Security and its stakeholders.
- Establish clear guidelines for ethical decision-making.
- Encourage employees to report misconduct and violations without fear of retaliation.

Core Values

- **Integrity** – We uphold honesty and ethical conduct in all actions.
- **Professionalism** – We maintain the highest standards in security services.
- **Respect** – We treat all individuals with dignity and fairness.
- **Compliance** – We follow all laws, regulations, and internal policies.
- **Continuous Improvement** – We consistently enhance our security practices.

2. Human Rights & Ethical Conduct Commitment

Septimius Security is committed to protecting human rights and ensuring all security operations align with:

- International Code of Conduct for Private Security Providers (ICoCA)
- United Nations Guiding Principles on Business & Human Rights (UNGPs)
- Libyan labor laws and international legal standards

Human Rights Standards

- Employees must respect human dignity and avoid any form of abuse, harassment, or discrimination.
- Security personnel must not participate in torture, inhumane treatment, forced labor, or any actions that violate international human rights law.
- Employees must report any suspected human rights violations immediately.



Code of Conduct

Non-Discrimination & Equal Treatment

- Discrimination based on race, gender, age, religion, disability, or any other protected category is strictly prohibited.
- Harassment, bullying, or intimidation in any form will not be tolerated.
- Employees are encouraged to report discrimination or harassment incidents confidentially.

3. Professional Conduct

All employees must conduct themselves professionally in their interactions with colleagues, clients, and stakeholders. This includes:

- Maintaining honesty and transparency in all business dealings.
- Protecting confidential company and client information.
- Avoiding conflicts of interest and disclosing any personal relationships that could impact business integrity.
- Ensuring a professional appearance and behavior at all times.

Crisis Management & Business Continuity

- Employees must follow emergency response protocols and support crisis management efforts.
- Personnel must be prepared for business continuity plans in case of security threats or disruptions.

4. Principles of Use of Force

- Force must always be a last resort and should only be used when necessary to prevent harm, protect assets, or ensure public safety.
- De-escalation techniques must be prioritized before considering any physical intervention.
- Any use of force must be reasonable, proportionate, and in compliance with international and local laws.
- Employees must follow strict reporting procedures for any incidents involving the use of force, including proper documentation and internal review.

5. Whistleblower Protection & Reporting Violations

Employees must report any violations of laws, human rights, or company policies.

Internal Reporting Channels:

- Direct manager, General Manager, Department Director, or CEO.
- Email: info@septimiussecurity.com or libya@septimiussecurity.com.



External Reporting Options:

- If internal mechanisms fail, employees may escalate concerns to legal authorities, regulatory bodies, or ICoCA oversight organizations.

Confidentiality & Non-Retaliation Measures:

- Whistleblowers are fully protected from retaliation, termination, or any form of harassment.
- Reports will be handled confidentially, and only those necessary for the investigation will have access to information.

6. Anti-Bribery & Anti-Corruption Policy

Septimius Security has a **zero-tolerance policy** for bribery and corruption.

Prohibited Practices

- Offering or accepting **bribes, facilitation payments, or kickbacks**.
- Engaging in **fraudulent business practices**.
- Making **political contributions** on behalf of the company.

Employee Responsibilities:

- Report any requests for bribes or suspicious activities immediately.
- Refuse any gifts or hospitality that could influence business decisions.
- Ensure all financial transactions are transparent and properly recorded.

7. Confidentiality & IT Security

Confidentiality Commitment

Employees must protect:

- Client data and operational intelligence.
- Employee personal information.
- Company trade secrets and financial information.

IT Security Measures:

- No unauthorized use of personal email accounts or external storage devices.
- Report any cybersecurity threats immediately.
- Use only company-approved communication tools for business matters.



8. Workplace Harassment & Discrimination Prevention

- All employees have the right to a safe and respectful workplace.
- Harassment, bullying, and discrimination will not be tolerated.
- Employees can report workplace issues confidentially.

Investigation & Resolution Process:

- Complaints will be investigated impartially.
- Disciplinary actions will be taken against violators.

Training & Awareness:

- Annual refresher training on workplace conduct.
- Managers are responsible for enforcing anti-harassment policies.

9. Social Media & Public Communications

- Employees must not post confidential company or client information on social media.
- Negative comments about Septimius Security, clients, or employees must be avoided.
- Only authorized employees may speak on behalf of the company.
- Employees must respect brand reputation in all communications.

10. Employee Accountability & Disciplinary Action

Violations of this Code will result in:

- Formal warnings.
- Suspension or termination.
- Legal action if violations breach national or international laws.

Disciplinary Process:

- Initial Review – Report reviewed by HR and management.
- Investigation – Evidence gathered and employee interviewed.
- Resolution – Decision on disciplinary action taken.
- Appeal Process – Employees can challenge decisions.



11. Compliance, Monitoring & Annual Review

- Annual employee certification of compliance with this Code.
- Regular audits and risk assessments to ensure adherence.
- The Code is reviewed and updated annually to reflect legal and operational changes.


12. Conclusion

Adherence to the **Septimius Security Code of Conduct** is a condition of employment. Employees must:

- Read and understand this Code.
- Comply with all policies and reporting obligations.
- Uphold the highest ethical and professional standards.

Failure to comply will result in disciplinary action.

Contact Us

 +218 21 711 4727

 Libya@septimiussecurity.com

 Next to the Peacock Compound, Tajora, Tripoli.

 www.septimiussecurity.com