Ultraviolet Cyber Inc

Anti-Human-Trafficking and Modern Slavery Policy

ID:	**ISMS-POL-AHT/MSP**
Version #:	**1.0**
Document No:	**UVCyber-DOC**
Owner(s):	
Approved for Publication By:	
Date Approved for Publication:	
Effective Date:	

Table of Contents

Revision History

Revision	Date	Author	Status	Description/Comment
0.1	12/22/2023	Ratish Kumar Mandal	Draft	Initial draft written/reviewed
1.0	1/22/2024		Final	Official Version

1. Purpose

Ultraviolet Cyber ("the Company") is committed to conducting business ethically, responsibly, and in full compliance with international human rights principles.

This policy establishes the Company's **zero-tolerance approach** to human trafficking, modern slavery, forced labour, servitude, debt bondage, and the procurement of commercial sex acts.

The purpose of this policy is to:

- Prevent human trafficking and modern slavery in all Company operations, supply chains, and partner relationships
- Ensure compliance with **UK Modern Slavery Act 2015**, **US Government Trafficking in Persons Policy**, and all applicable international and host-nation laws
- Provide employees with clear behavioral expectations
- Establish reporting mechanisms and protections against retaliation
- Promote transparency, accountability, and responsible corporate conduct

This policy is a condition of employment and applies globally.

2. Scope

This policy applies to all individuals working for or on behalf of Ultraviolet Cyber, including:

- All employees (full-time, part-time, temporary, and fixed term)
- Contractors, consultants, agency workers, and subcontractors
- Suppliers, service providers, and external business partners
- Any individual or entity representing Ultraviolet Cyber in any capacity

This policy applies to all jurisdictions where the Company operates, including the UK, US, and all overseas or remote locations.

3. Policy Statement

Ultraviolet Cyber maintains **zero tolerance** for:

- Human trafficking
- Modern slavery
- Forced or compulsory labour

- Child labour
- Involuntary servitude or bonded labour
- Coercion, threats, or manipulation for labour or services
- Procurement, solicitation, or engagement in commercial sex acts
- Transporting, harbouring, recruiting, or obtaining persons for exploitation

A *commercial sex act* is defined as:
Any sex act for which anything of value is given to or received by any person.

Ultraviolet Cyber strictly prohibits:

- Using Company funds, assets, or premises for any form of trafficking activity
- Employing or contracting with individuals or organisations known to participate in trafficking
- Destroying, concealing, or confiscating identity documents or immigration papers
- Charging recruitment fees to workers
- Knowingly sourcing goods or services linked to forced or exploitative labour

Any violation will result in disciplinary action, up to termination of employment, contract suspension, supplier termination, and referral to law enforcement.

4. Legal and Regulatory Compliance

Ultraviolet Cyber complies with the following laws and regulations:

4.1 UK Laws

- **Modern Slavery Act 2015**
- UK Immigration and labour laws
- UK Government Supplier Code of Conduct

4.2 US Government Requirements

- **FAR 52.222-50: Combating Trafficking in Persons**
- **22 U.S.C. Chapter 78: Trafficking Victims Protection Act (TVPA)**

Ultraviolet Cyber is required to **immediately notify relevant authorities**, including US contracting officers, if an employee or supplier violates anti-trafficking laws.

4.3 Host-Nation Laws

Employees, consultants, contractors, and subcontractors working in overseas locations must comply with **all local anti-trafficking and labour laws**, regardless of local cultural practices.

5. Prohibited Conduct

The following activities are strictly prohibited under this policy:

5.1 Human Trafficking

- Recruiting, transporting, transferring, harbouring, or receiving individuals through force, fraud, coercion, or deception

5.2 Modern Slavery and Forced Labour

- Work performed involuntarily, under threat, debt bondage, or without free and informed consent

5.3 Exploitation of Vulnerable Persons

- Exploiting migrant workers, minors, or economically disadvantaged individuals

5.4 Procurement of Commercial Sex Acts

- Engaging in or facilitating commercial sexual services

5.5 Abuse of Worker Rights

Including but not limited to:

- Withholding wages
- Confiscating passports or identity documents
- Restricting freedom of movement
- Limiting access to medical care
- Misrepresenting terms of employment

Any employee found participating in these behaviours will face immediate disciplinary action.

6. Responsibilities

6.1 Employees

All employees must:

- Abide by this policy as a condition of employment
- Immediately report any suspicious activity or violations
- Participate in required training
- Not engage in any trafficking-related conduct

6.2 Managers and Supervisors

Managers must:

- Ensure employees understand this policy
- Monitor compliance in their teams
- Escalate concerns immediately to HR or Compliance
- Support investigations without interference

6.3 Contractors & Suppliers

All external parties must:

- Comply with this policy and relevant anti-trafficking laws
- Maintain compliance programmes that prevent trafficking in supply chains
- Notify UltraViolet Cyber of any concerns or confirmed violations

6.4 Human Resources & Compliance

Responsible for:

- Policy maintenance and communication
- Training and awareness programmes
- Receiving and investigating reports
- Liaising with legal authorities when necessary

7. Recruitment & Employment Practices

Ultraviolet Cyber maintains ethical recruitment practices, including:

- No recruitment fees charged to workers
- No retention of passports, visas, or identification documents
- Clear written contracts in the worker's native language
- Fair wages compliant with local law
- Voluntary employment with freedom to leave

Third-party recruitment agencies must undergo due diligence and must legally certify that they comply with anti-trafficking requirements.

8. Supply Chain and Vendor Due Diligence

The Company takes a risk-based approach to evaluating suppliers, including:

- Screening for trafficking-related violations
- Requiring contractual compliance with anti-trafficking laws
- Conducting periodic audits when necessary
- Reviewing high-risk supply chains for red flags
- Requiring suppliers to investigate concerns and implement corrective actions

9. Reporting Suspected Violations

Ultraviolet Cyber encourages all employees and contractors to report concerns immediately.

9.1 Internal Reporting

Reports may be made to:

- Human Resources
- Line Manager
- Compliance or Legal
- Anonymous reporting channel (ReportIt)

9.2 External Reporting

Employees may also report directly to:

Global Human Trafficking Hotline:
📞 **+1-844-888-FREE (3733)**
📧 **help@befree.org**

Employees are **not required** to obtain approval before contacting external authorities.

10. Non-Retaliation Protection

Ultraviolet Cyber prohibits retaliation against anyone who:

- Reports possible violations in good faith
- Assists another individual in making a report
- Participates in an internal or external investigation

Retaliation includes termination, demotion, intimidation, discrimination, or harassment. Any retaliation will result in disciplinary action.

11. Investigation and Corrective Action

When a concern is raised:

1. The Company will acknowledge receipt and initiate a confidential investigation.
2. Evidence will be reviewed by HR, Legal, or Compliance.
3. Appropriate corrective actions will be taken, which may include:
    - Termination of employment
    - Contractor or supplier suspension or removal
    - Mandatory retraining
    - Reporting to authorities
    - Contracting officer notification (US Government)

Findings will be recorded and retained per legal requirements.

12. Training and Awareness

Ultraviolet Cyber provides periodic training to employees, including:

- Recognizing signs of trafficking
- Reporting obligations
- Responsibilities under UK and US law
- Supplier and labour risk indicators

High-risk departments may receive enhanced training.

13. Record Keeping

The Company maintains secure records of:

- Reports and investigations
- Supplier due-diligence outcomes
- Staff training completion
- Policy review and updates

All records will be retained in accordance with Company retention schedules and applicable laws.

14. Policy Review

This policy will be reviewed:

- Annually
- After significant legal or regulatory changes
- Following any incident or investigation
- As part of the Company's ISO 27001:2022 ISMS review process

Updates will be approved by Executive Leadership and Human Resources.

15. Questions

Any questions regarding this policy should be directed to:

UltraViolet Cyber – Human Resources Department

📧 *HR@uvcyber.com*

📞 *+1-443-351-7630*