Effective June 1, 2023

Table of Contents

Bribery & Corruption

UltraViolet Cyber forbids offering or soliciting bribes, kickbacks or any other illegal or improper payments or transfers of anything else of value to secure or retain business, circumvent competition or in any way receive favorable treatment. UltraViolet Cyber employees may not give or receive, whether directly or indirectly, bribes or other improper advantages for business or financial gain. No employee may offer, give, or receive any gift or payment which is, or may be construed as being, a bribe. Any demand for, or offer of, a bribe must be rejected at once and reported to management. This includes gifts, hospitality, and influence bribery that exceeds a modest level. Exceptions to this rule are allowed which include modest gifts such as refreshments, lunch, certificates, greeting cards, corporate swag, etc., in compliance with the limits established by the Conflict of Interest Policy found within this Handbook.

Further, UltraViolet Cyber employees should not accept any gift, regardless of the value, that could influence his or her decision-making on behalf of UltraViolet Cyber. In addition, no outside consultant, agent or third party shall be used to circumvent this prohibition against bribes, kickbacks and improper payments.

Human Trafficking

It is a condition of employment at UltraViolet Cyber that employees abide by the U.S. Government's Zero Tolerance Policy on Human Trafficking. Employees are strictly prohibited from engaging in severe forms of trafficking in persons, using forced labor or procuring commercial sex acts – defined as any sex act on account of which anything of value is given to or received by any person. Any employee who does not abide by this policy will be subject to disciplinary action. If UltraViolet Cyber learns that any of its employees have violated the U.S. Government's Zero Tolerance Policy on Human Trafficking, UltraViolet Cyber will inform the government's contracting officer immediately. All employees, consultants, contractors and subcontractors working at overseas locations are required to be aware of and comply with that host nation's laws on this subject.

Additionally, employees may report activity inconsistent with the policy prohibiting trafficking in persons to the Global Human Trafficking Hotline at 1–844–888–FREE or via email at help@befree.org. The Company forbids retaliation against anyone for reporting human trafficking, assisting in making a human trafficking complaint or cooperating in a human trafficking investigation.

Any questions regarding this policy should be directed to UltraViolet Cyber's Human Resources Department.

Whistleblower Policy

UltraViolet Cyber is committed to the highest possible standards of ethical, moral, and legal business conduct. In line with this commitment and UltraViolet Cyber's commitment to open communication, this

policy aims to provide an avenue for employees to raise concerns and reassurance that they will be protected from reprisals or victimization for whistleblowing in good faith.

The whistleblowing policy is intended to cover serious concerns that could have a large impact on UltraViolet Cyber, such as actions that may lead to incorrect financial reporting, are unlawful, do not conform to Company or otherwise amount to serious improper conduct.

Harassment or victimization of the complainant will not be tolerated and every effort will be made to protect the complainant's identity as far as the constraints of the investigation allow. Although anonymous allegations will be taken, UltraViolet Cyber encourages employees to put their names to allegations because appropriate follow-up questions and subsequent investigation may not be possible unless the source of the information is identified. Concerns expressed anonymously will be investigated, but consideration given to:

- The seriousness of the issue raised;
- The credibility of the concern; and
- The likelihood of confirming the allegation from attributable sources.

The whistleblowing procedure is intended to be used for serious and sensitive issues. Malicious allegations may result in disciplinary action. Serious concerns relating to financial reporting and unethical or illegal conduct should be reported in directly to the employee's immediate Supervisor, Manager, a Human Resources Representative or any Vice President of the Company.

The earlier a concern is expressed, the easier it is to take action; therefore, prompt reporting is essential to the success of this policy.

The complainant will be given the opportunity to receive follow-up on their concern in a timely fashion. Due to confidentiality issues, at times, the information offered to the complainant will need to be limited. Beyond such constraints, the response will contain an acknowledgement that the concern was received and a brief overview of how the matter will be dealt with, as well as an indication of whether or not further investigation will follow. The amount of contact between the complainant and the department/person(s) investigating the concern will depend on the nature of the issue and the clarity of information provided. Further information may be sought from the complainant. UltraViolet Cyber forbids retaliation, discharge, demotion, suspension, threats, harassment or any other type of discrimination against any employee for making a complaint, assisting in making a complaint, or participating in an investigation stemming from a complaint. Employment-related concerns should continue to be reported via the Complaint Resolution Policy described in this Handbook.

Fraud Policy

Management is responsible for the prevention, deterrence and detection of fraud, misappropriations and other irregularities. By providing employee guidelines and responsibilities to promote honesty and high ethical standards, UltraViolet Cyber intends to prevent, deter and detect fraud. Any fraud that is suspected or detected involving employees, consultants, vendors, customers and/or any other parties with a business relationship with UltraViolet Cyber must be reported immediately to the Human Resources Department. The department treats all information received confidentially. When in doubt, report it. Employees who fail to comply with this policy are subject to disciplinary action, up to and including discharge.

Fraud is defined as any intentional, false representation or concealment of a material fact committed to obtain an unfair or unlawful gain or inducing another to act upon it to his or her injury. Actions constituting fraud include, but are not limited to:

- Any dishonest or fraudulent act;
- Misappropriation of UltraViole Cyber assets;
- Inappropriate or unauthorized use, removal or destruction of UltraViolet Cyber assets;
- Falsification, forgery or alteration of any UltraViolet Cyber records;
- Falsification, forgery or alteration of a check, bank draft or any other financial document;
- Impropriety in the handling or reporting of money or financial transactions;
- Accepting or receiving anything of material value from contractors, vendors, customers or any other persons doing business with UltraViolet Cyber that could influence their decision-making on behalf of UltraViolet Cyber;
- Paying or receiving bribes or kickbacks;
- Disclosing confidential or proprietary information to outside parties;
- Profiting from insider knowledge of UltraViolet Cyber activities;
- Disclosing to other persons securities activities engaged in or contemplated by UltraViolet Cyber;
- Adding dependents to lines of insurance who are not eligible (e.g., fiancé, common-law spouse, parents, etc.);
- Falsifying a Workers' Compensation or personal disability claim; or
- Any similar or related inappropriate conduct.

Employees must cooperate in a complete, accurate and timely manner with any internal investigation. However, employees should not attempt to personally conduct investigations or interviews/interrogations related to any suspected fraudulent act. The reporting employee should not contact the suspected individual or discuss the case, facts, suspicions, or allegations with anyone, unless specifically asked to do so by the Human Resources Department.

UltraViolet Cyber's Human Resources Department, with assistance from other sources, is responsible for investigating all suspected fraudulent acts. If the investigation substantiates that fraudulent activities have occurred, the Human Resources Department will issue reports to appropriate, designated personnel and, if appropriate, to UltraViolet Cyber's Board of Directors. Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with legal counsel and senior management, as will final decisions on disposition of the case.

Ethics & Code of Conduct

UltraViolet Cyber is committed to providing a work environment governed by the highest ethical and legal standards. In all situations you are expected to conduct your activities ethically, lawfully, and with integrity. By deciding to work at UltraViolet Cyber, you agree to follow the Company's rules.

Part of maintaining an ethical workplace is providing employees the opportunity to provide honest feedback. The Company will not tolerate retaliation of any kind against an employee who reports in good faith a violation of law or of this policy. UltraViolet Cyber encourages employees to report any actual or potential violations of applicable laws or regulations and any unethical, dishonest, or improper conduct to

their manager or Human Resources.

Although it is not possible to list every item that could be considered misconduct in the workplace, the following is a list of common-sense infractions that may result in disciplinary action up to and including termination of employment:

- Falsifying employment or other Company records.
- Violating state, federal or local laws and regulations.
- Violating security or safety rules or failing to observe safety rules or safety practices.
- Soliciting gratuities from customers or clients.
- Displaying excessive or unexcused absenteeism or tardiness.
- Possessing firearms, weapons or explosives on Company property without authorization, in violation of policy or while on duty.
- Using the Company's property and supplies, particularly for personal purposes, in an excessive, unnecessary, or unauthorized way.
- Negligent damage of property.
- Committing theft or unauthorized possession of Company property or the property of fellow employees.
- Giving confidential or proprietary information to competitors; working for a competing business while an employee of the Company. Disclosing the confidential personal information of employees, customers, or Company business partners.
- Engaging in abusive or malicious conduct, such as using obscene or threatening language or gestures or other verbal or physical conduct a reasonable person would find threatening, intimidating, or humiliating.
- Interfering with another employee on the job, unwarranted sabotage, or undermining another's work.
- Soliciting, selling, or collecting funds for any purpose while on working time (not including meals and authorized breaks).
- Any violation of the terms of this Handbook.

This policy is not intended to limit the Company's right to discipline or discharge employees for any reason permitted by law. In fact, while we value our employees, the Company retains the right to terminate an employee on an "at-will" basis.

Nothing in this policy is intended to limit employee rights under the National Labor Relations Act or restrict communications or actions protected or required by state or federal law.