



# CODE OF CONDUCT

Type	Policy
Scope of validity	ThreatMark Inc., ThreatMark s.r.o.
Classification	<b>T1 - Public</b>
Date of approval	January 31, 2025
Authors	Lukáš Jakubiček, Hana Vystavělová
Version	2.1

## Version History

Version	Author	Changes
1.0	Lukáš Jakubíček	New release
2.0	Hana Vystavělová	New release
2.1	Hana Vystavělová	Chapter 1 – updates, new chapter 1.2 Breach of the Policy, Chapter 2 – reviewed and updated; new chapter 3 – DEI policy; new chapter 10 – Grieving and Disciplinary Procedure

# Table of Contents

<b>Version History .....</b>	<b>2</b>
<b>Table of Contents .....</b>	<b>3</b>
<b>1. Purpose of the Document .....</b>	<b>5</b>
1.1. Responsibilities.....	5
1.2. Breach of the Policy .....	6
<b>2. Human and Labor Rights .....</b>	<b>7</b>
2.1. Equal Opportunities.....	7
2.2. Non-Discrimination.....	7
2.3. Recruitment and Selection .....	8
2.4. Part-time and temporary employees .....	8
2.5. Disability .....	9
2.6. Fair Working Conditions .....	9
2.7. Bullying and Harassment .....	10
2.8. Work Hours and Benefits .....	12
2.9. Safe, Healthy, and Secure Workplace .....	12
2.10. Flexibility and Work-Life Balance .....	12
2.11. Right to Privacy.....	12
2.12. Health Promotion.....	13
2.13. Anti-slavery and Human Trafficking.....	13
2.14. Child Labor Policy.....	14
2.15. Social Dialogue and Involvement of Workers.....	15
2.16. Remuneration and Reward Policy.....	15
<b>3. Diversity, Equality, and Inclusion Policy .....</b>	<b>16</b>
<b>4. Anti-Corruption .....</b>	<b>18</b>
4.1. Anti-Bribery .....	18
4.2. Gifts & Entertainment.....	21
4.3. Accepting Gifts (Non-Government Officials) .....	21
4.4. Conflict of Interest.....	22
<b>5. Anti-Money Laundering / Anti-Terrorism Financing.....</b>	<b>24</b>
5.1. Culture and Values.....	24
5.2. Allocation of Responsibilities .....	24

5.3. Risk Identification and Assessment .....	25
5.4. Customer Due Diligence (CDD), Record Keeping and Ongoing Monitoring.....	25
5.5. Cooperation with Regulators and Law Enforcement Agencies .....	25
<b>6. Third-party Due Diligence .....</b>	<b>26</b>
<b>7. Segregation of Duties .....</b>	<b>27</b>
<b>8. Environmental obligations .....</b>	<b>28</b>
<b>9. Social Responsibility (CSR) .....</b>	<b>29</b>
<b>10. Grieving and Disciplinary Procedure.....</b>	<b>30</b>
10.1. Grieving Procedure .....	30
10.2. Disciplinary Procedure .....	31
<b>11. Reporting and Monitoring System.....</b>	<b>33</b>
11.1. Compliance Manager.....	33
11.2. Protection of Reporting Person.....	33
11.3. Internal Reporting System .....	34
11.4. External Reporting .....	35
11.5. Procedure For Handling Reports.....	35
<b>12. Final Provisions.....</b>	<b>36</b>

# 1. Purpose of the Document

ThreatMark commitment to ethical conduct and integrity is at the forefront of our organizational principles. The Code of Conduct serves as the foundational document outlining the standards and expectations that define our work culture. This policy is a reflection of our dedication to fostering an environment of fairness, honesty, and respect in all our interactions, both within the company and in our engagements with clients, partners, and the wider community.

At ThreatMark, we recognize the profound impact our actions can have on individuals and organizations. With this awareness, our Code of Conduct establishes a commitment to social and ethical responsibility and sustainable business practices that not only govern our day-to-day operations but also underscore our responsibility to customers, their clients, and the broader stakeholders we engage with.

This policy applies to everyone who works for or cooperates with ThreatMark, or who acts on ThreatMark's behalf, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, agents, contractors and suppliers. We encourage all employees, partners, and stakeholders to familiarize themselves with the principles outlined in this Code of Conduct and to integrate them into their professional endeavors. By upholding these standards, we collectively contribute to the preservation of our company's reputation as a trustworthy, transparent, and ethically responsible entity.

This policy does not form part of your contract of employment, and we may amend it at any time.

## 1.1. Responsibilities

### **All company members**

All company members have a role in ensuring that this Code of Conduct is promoted at work. All have a personal responsibility to comply with this policy and to ensure, as far as possible, that others do the same.

### **Compliance Manager**

ThreatMark appoints a Compliance Manager as a central reference point for reporting any suspicious or unlawful actions, transactions, or breach of law or this Code of Conduct. The responsibilities of a Compliance Manager are described in the chapter 11.1 – Compliance Manager fulfills the role of a Competent Person according to the Czech Whistleblowing Act no. 171/2023 Coll.

**Managers have a responsibility to:**

- Set a good example by their own behavior.
- Actively support and contribute to the implementation of this policy and the strategies within.
- Take positive steps to promote equality at work, ensure supportive working environment in their team.
- Monitor compliance with this policy and ensure action is issued in the case of non-compliance,

This Policy imposes on all personnel specific responsibilities and obligations that will be enforced through standard disciplinary measures and reflected in personnel evaluations. All managers, employees, and contractors are responsible for understanding and complying with the policy related to their jobs, namely are obliged to:

- Be familiar with applicable aspects of the policy and communicate them to subordinates.
- Ask questions if the policy or action required to take in a particular situation is unclear.
- Properly manage and monitor business activities conducted through third parties.
- Be alert to indications or evidence of possible wrongdoing.
- Promptly report violations or suspected violations through appropriate channels (see chapter 11 – Reporting and Monitoring System).
- Consider this policy while completing work-related duties and when representing ThreatMark.
- Support colleagues in their awareness of this policy.
- Support and contribute to ThreatMark's aim of implementing this policy in practice.

## **1.2. Breach of the Policy**

Employees who violate this policy will be subject to disciplinary procedure as a case of possible misconduct or gross misconduct. Serious cases of deliberate breach may amount to gross misconduct. A disciplinary penalty may be imposed up to and including dismissal, depending on the seriousness of the offence and all relevant circumstances. Some violations may constitute a criminal offence, punishable by a fine and/or imprisonment. Disciplinary procedure is governed mainly by local legislation, its general steps are described in the chapter 10.2 – Disciplinary Procedure.

If we find that individuals or organizations cooperating with us or working on our behalf have breached this policy we will ensure that we take appropriate action. This may range from considering the possibility of breaches being remediated and whether that might represent the best outcome for those individuals impacted by the breach to terminating such relationships.

## 2. Human and Labor Rights

We align our practices with the principles outlined in the Universal Declaration of Human Rights. This includes recognizing the inherent dignity, equality, and inalienable rights of all individuals. Our approach to Human Rights includes:

### 2.1. Equal Opportunities

ThreatMark aims at all times to promote equality and diversity in the workplace and to provide a working environment that is free from discrimination. We wish to ensure that all of our team members feel respected and valued, that they can achieve their full potential, and that all employment decisions are taken without reference to irrelevant or discriminatory criteria. Detailed equality, diversity and inclusion policy is described in chapter 3 – Diversity, Equality, and Inclusion Policy.

### 2.2. Non-Discrimination

We are committed to maintaining a safe and respectful workplace for all employees. Harassment or discrimination, whether active or by means of passive support, based on Protected Characteristics such as ethnicity, gender, gender identity, national origin, disability, sexual orientation, religion, unionization, employee representation, political affiliation, parenthood, age, or any other characteristic, is strictly prohibited, and we have mechanisms in place to address and prevent such behaviors.

Special protective, supportive, and advancement measures may be extended to disadvantaged groups when either mandated or permitted by local legislation.

There are four types of unlawful discrimination

Direct Discrimination – treating someone unfairly because of a Protected Characteristic, such as their religion, sexuality, or race. This includes assumptions about someone’s characteristics or their association with others who have these traits. For example, not hiring someone because they are Jewish or not promoting someone because they are gay.

Indirect Discrimination – applying policies or rules that seem neutral but disadvantage people with a specific Protected Characteristic. For instance, requiring employees to work on Sundays may disadvantage Christians, or insisting on full-time work might impact women with childcare responsibilities. Such practices can be considered unlawful unless they can be reasonably justified.

Harassment – unwanted behavior related to a Protected Characteristic that violates a person’s dignity or creates an intimidating, hostile, or offensive environment. A single incident of this nature can amount to harassment if sufficiently serious. Refer to our Bullying and Harassment Policy in the chapter 2.7 Bullying and Harassment for further guidance if you experience harassment.

Victimization – treating someone unfairly because they asserted their legal rights under discrimination law or supported someone else in doing so. For example, excluding a disabled employee from meetings after they filed a grievance about workplace adjustments.

If you believe that you have suffered discrimination you can raise the matter through our grievance procedure (see chapter 10 – Grieving and Disciplinary Procedure), or you can talk to your manager, HR person or a trusted colleague in the first instance if you feel more comfortable doing this. Complaints will be treated in confidence and investigated as appropriate.

You must not be victimized or retaliated against for complaining about discrimination. However, making a false allegation deliberately and in bad faith will be treated as misconduct.

## **2.3. Recruitment and Selection**

Person and Job specifications are limited to those requirements that are necessary for the effective performance of the job. Candidates for employment or promotion are assessed objectively against the requirements for the position, and on the basis of merit. Similarly other selection exercises such as redundancy selection is conducted against objective criteria. A person’s personal or home commitments will not form the basis of employment decisions except where justified and necessary.

We generally advertise vacancies to a diverse section of the labor market. Our advertisements should avoid any kind of stereotyping or wording that may discourage particular groups from applying.

Job applicants should never be asked questions which might suggest an intention to discriminate on grounds of a Protected Characteristic (for example if they plan to have children).

## **2.4. Part-time and temporary employees**

We will treat part-time and fixed-term employees the same as comparable full-time or permanent employees, and will ensure that that they enjoy no less favorable terms and conditions (albeit on a pro-rata basis where appropriate), unless different treatment is justified.



## 2.5. Disability

We will not ask job applicants about their health or any disability before offering them a position, unless it is to check that they can perform an intrinsic part of the job, or to see if we need to make any particular arrangements to accommodate them at interview. Where necessary, job offers can be made conditional to a satisfactory medical check. Health or disability questions may be included in equal opportunities monitoring forms - these must not be used for selection or decision-making purposes.

If you are disabled or become disabled, we would ask you to tell us about your condition, in strict confidence, so that we can support you as much as possible, and discuss with you any adjustments that may help you.

## 2.6. Fair Working Conditions

We commit to avoiding unlawful discrimination in all aspects of employment including recruitment, promotion, opportunities for training, pay and benefits, discipline, and selection for redundancy.

Employees have employment terms/contracts in a language they understand specifying their terms of employment and termination.

Employees with the same qualifications, experience, and performance receive equal pay for equal work. Employees are under no circumstances subject to corporal punishment, unlawful detentions, violence, threats, coercion, or verbal or sexual harassment.

New forms of flexible employment require additional care to specify the nature, volume, or duration of work. Decentralized, self-organized forms of work can increase worker autonomy, boost business development, and lead to lower awareness of rights and unclear information requirements for employers.

ThreatMark respects and recognizes, in accordance with the laws of the country in which employees are employed, the right to freedom of association and collective bargaining, and employees will be free to terminate their employment under established rules.

We do not engage in forced labor, slave labor, or other non-voluntary labor in our company and its value chain.

## 2.7. Bullying and Harassment

The ThreatMark stance is that harassment is unacceptable, whether or not it is targeted at any of Protected Characteristics (age, disability, gender reassignment, marital or civil partner status, pregnancy or maternity, race, color, nationality, ethnic or national origin, religion or belief, sex or sexual orientation).

Examples of harassment may include (but are not limited to) the following:

- Display or circulation of sexually suggestive material or material with racial overtones.
- Use of slang names for racial groups, or age groups, or for disabled persons.
- Professional or social exclusion.
- Unwanted physical conduct, such as touching, pinching, pushing and grabbing.
- Unwelcome sexual advances or suggestive behavior.
- Offensive emails, text messages or social media content.

It is important to note that harassment occurs even if the harasser perceives his/her behavior as being harmless and without malice, or 'just a bit of fun'. What matters is how the behavior makes the recipient feel, and not what the perpetrator's intentions were. Also, a person may be harassed even if they were not the intended 'target' of the behavior.

Bullying is a sustained form of psychological abuse. It is defined as offensive, intimidating, malicious or insulting behavior, involving the abuse or misuse of power, which has the purpose or effect of belittling, humiliating or threatening the recipient.

Workplace bullying usually takes one of three forms: physical, verbal or indirect. It can range from extreme forms such as violence and intimidation, to less obvious actions, such as professional or social exclusion.

Examples of bullying may include (but are not limited to) the following:

- Shouting or swearing at people in public or private.
- Spreading malicious rumors.
- Inappropriate derogatory remarks about someone's performance.
- Physical or psychological threats.
- Constantly undervaluing effort.
- Rages, often over trivial matters.
- Ignoring or deliberately excluding people.
- Overbearing and intimidating levels of supervision.

- Deliberately sabotaging or impeding work performance.

Please note that managers are duty-bound to give their team members feedback and to generally manage their performance. Legitimate, reasonable and constructive criticism of a team member's performance or behavior, or reasonable instructions given to an employee in the course of their employment, will not amount to bullying on their own.

### **What to do if you are being harassed or bullied**

#### Informal Approach

- Firstly, you may be able to sort out matters informally. The person may not realize their behavior is upsetting.
- Politely explain what behavior you find offensive and ask them to stop immediately. Keep a record of the date and what was said in case the behavior continues and you wish to make a formal complaint.
- If speaking to them directly feels difficult, talk to your manager or a trusted colleague for support. They can advise you, speak on your behalf, or accompany you in addressing the issue.

If the informal approach doesn't work or isn't suitable, raise a formal grievance (see chapter 10 – Grieving and Disciplinary Procedure) or report (see chapter 11 – Reporting and Monitoring System).

Where it is found that an employee has been harassed by a third party, such as a customer, supplier or independent contractor, the Company will take such steps as are reasonably practicable to prevent any recurrence.

Team members who make complaints in good faith, or who participate in any investigation must not suffer any form of retaliation or victimization as a result. Any employee engaged in retaliation will be subject to disciplinary action.

If someone makes a complaint which is not upheld, and ThreatMark has good grounds for believing that the complaint was not made in good faith, ThreatMark will take disciplinary action against the person making the false complaint.

### **How we can all help to stop bullying and harassment**

We all create a working environment free of bullying and harassment by:

- Considering how our own behavior may affect others, and changing it.
- Being receptive, rather than defensive, if asked to change our behavior.

- Treating our colleagues with dignity and respect.
- Taking a stand if we think inappropriate jokes or comments are being made.
- Making it clear to others when we find their behavior unacceptable.
- Intervening, if possible, to stop harassment or bullying, and giving support to victims.
- Reporting harassment or bullying to your manager or Compliance Manager.
- Being open, honest and objective in any investigation of complaints.

## **2.8. Work Hours and Benefits**

Our operations strictly adhere to all relevant laws governing wages, work hours, overtime, and benefits, ensuring full compliance. We will consider any possible indirectly discriminatory effect of our standard working practices, including the number of hours to be worked, the times at which these are to be worked and the place at which the work is to be carried out. When considering requests for variations to these working practices we will only refuse these if we have good reasons for doing so.

## **2.9. Safe, Healthy, and Secure Workplace**

Injuries and accidents occurring at work are logged, investigated and preventive measures are introduced.

Ensuring protection against occupational injuries and ill-health to all workers offers an important way to reduce precariousness, and social costs and improve firms' productivity. Reinforcing reintegration and rehabilitation efforts requires more involvement of the employers for re-training or workplace adaptation.

## **2.10. Flexibility and Work-Life Balance**

We acknowledge the significance of achieving work-life balance and provide flexibility in work arrangements to cater to the diverse needs of our employees. This encompasses flexible schedules, remote work alternatives, and family-friendly policies.

## **2.11. Right to Privacy**

Following relevant laws and global best practices, data pertaining to employees and customers within the company is considered confidential. As a result, special attention and security measures are implemented during the handling, processing (including storage and deletion), transfer, disclosure, and sharing of such

data. All individuals working with employee or customer data are mandated to adhere to data protection policies.

## 2.12. Health Promotion

An unhealthy lifestyle may contribute to ill health, sick leave, lost productivity, and reduced ability to work. Our health promotion program aims to improve the lifestyle of our staff and consequently improve their health and prevent chronic diseases. ThreatMark is committed to creating a workplace environment that supports and encourages healthy lifestyles and to supporting and encouraging workers to participate in education and activities that improve their health.

## 2.13. Anti-slavery and Human Trafficking

ThreatMark strictly prohibits the use of modern slavery and human trafficking in our operations and supply chain. We have and will continue to be committed to implementing systems and controls aimed at ensuring that modern slavery is not taking place anywhere within our organization or in any of our supply chains. We expect that our suppliers will hold their own suppliers to the same high standards. Modern slavery is a crime and a violation of fundamental human rights.

We are committed to safeguarding against modern slavery and expect everyone working with us or on our behalf to uphold the following:

- **Zero Tolerance:** We have a zero-tolerance approach to modern slavery in our organization and supply chains.
- **Responsibility:** All those working for us or on our behalf must prevent, detect, and report any activity that could breach this policy. Engaging in or failing to report modern slavery is prohibited.
- **Stakeholder Engagement:** We actively work with stakeholders and suppliers to address modern slavery risks.
- **Risk-Based Approach:** We take a risk-based approach to our contracting processes and keep them under review. We assess whether the circumstances warrant the inclusion of specific prohibitions against the use of modern slavery and trafficked labor in our contracts with third parties. Using our risk-based approach, we will also assess the merits of writing to suppliers requiring them to comply with our Code of Conduct, which sets out the minimum standards required to combat modern slavery and trafficking.

- Third-Party Compliance: Consistent with our risk based approach we may require employment and recruitment agencies and other third parties supplying workers to our organization to confirm their compliance with our Code of Conduct.
- Audits and Action: Based on risk assessment and due diligence process we may include supplier audits to verify compliance.

## 2.14. Child Labor Policy

Child labor refers to work that deprives children of their childhood and affects their schooling, potential, and dignity. It's work that's harmful to them mentally, physically and socially.

ThreatMark ensures that our company, its subsidiaries, and everyone we're connected with (suppliers, vendors, and contractors) follows the law and cares for children's interests.

To make sure we enforce this policy and help eliminate child labor, we're committed to:

- Follow the stricter law if more than one law applies (e.g., state and federal, local and international).
- Require suppliers, partners, and vendors to follow the stricter applicable laws and recognize children's rights. They must also require their suppliers, subcontractors, and stakeholders to do the same.
- Working with governments and other organizations to end child labor.
- Educating our staff on youth work and showing them how to report child labor if they see or suspect it.
- Requiring hiring managers and HR to avoid hiring minors under the legal age for work.
- Keeping and validating documentation verifying our employees' age after they're hired. If we discover that we've employed a minor under 18, we'll review applicable laws and adjust working hours accordingly. If we need to let the child go, we'll assess their situation and make sure to provide for them to the best of our ability (e.g., pay them their would-be salary for a couple of months) when necessary.
- Communicating our no child labor policy to organizations we're connected with and ensuring our contracts have the right stipulations.
- Auditing suppliers and partners with high child labor risk to ensure they aren't involved in child labor, possibly with unannounced onsite visits. If we discover hidden business sites that employ children, we'll dissolve our contract immediately.
- Demanding and monitoring an elimination plan in cases where suppliers discover child labor in their business.

- Employing or consulting with experts on child labor, health, and safety standards, or corporate social responsibility.

## 2.15. Social Dialogue and Involvement of Workers

We prioritize open social dialogue and actively involve our workforce in decision-making processes. This commitment fosters collaboration, ensuring that the perspectives and insights of our employees contribute to a positive and inclusive work environment.

## 2.16. Remuneration and Reward Policy

ThreatMark provides competitive employee compensation packages that are aligned with company profitability. Our policy is designed to attract, retain, and motivate top talent. We strive for competitive and equitable compensation, aligning with industry standards. Our policy emphasizes performance-based incentives, recognizing and rewarding exceptional contributions. We are committed to transparency, ensuring that our employees understand the criteria for remuneration decisions.

Pension insurance aims at ensuring an appropriate standard of living for employees after retirement. Pension insurance is in accordance with local laws, regulations, and market practice.

ThreatMark provides benefits to employees as a component of the comprehensive reward package, which is determined either through individual agreements or influenced by local regulations, market norms, and company-established practices.

To effectively motivate and reward employees ThreatMark has implemented the Employees Stock Option Plan.

### 3. Diversity, Equality, and Inclusion Policy

ThreatMark is committed to encouraging equality, diversity and inclusion among our workforce, and eliminating unlawful discrimination. The aim is for our workforce to be truly representative of all sections of society and our customers, and for each employee to feel respected and able to give their best.

The organization – in providing services – is also committed against unlawful discrimination of customers or the public.

The policy's purpose is to:

- provide equality, fairness and respect for all in our employment, whether temporary, part-time or full-time;
- not unlawfully discriminate because protected characteristics of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race (including color, nationality, and ethnic or national origin), religion or belief, sex and sexual orientation. Special protective, supportive, and advancement measures may be extended to disadvantaged groups when either mandated or permitted by local legislation.
- oppose and avoid all forms of unlawful discrimination. This includes in pay and benefits, terms and conditions of employment, dealing with grievances and discipline, dismissal, redundancy, leave for parents, requests for flexible working, and selection for employment, promotion, training or other developmental opportunities.

ThreatMark commits to:

- Encourage equality, diversity and inclusion in the workplace as they are good practice and make business sense.
- Create a working environment free of bullying, harassment, victimization and unlawful discrimination, promoting dignity and respect for all, and where individual differences and the contributions of all staff are recognized and valued.

This commitment includes training managers and all other employees about their rights and responsibilities under the equality, diversity and inclusion policy. Responsibilities include staff conducting themselves to help ThreatMark provide equal opportunities in employment, and prevent bullying, harassment, victimization and unlawful discrimination.



All staff should understand they, as well as their employer, can be held liable for acts of bullying, harassment, victimization and unlawful discrimination, in the course of their employment, against fellow employees, customers, suppliers and the public.

- Take seriously complaints of bullying, harassment, victimization and unlawful discrimination by fellow employees, customers, suppliers, visitors, the public and any others in the course of the organization's work activities.

Such acts will be dealt with as misconduct under the organization's grievance and/or disciplinary procedures, and appropriate action will be taken. Particularly serious complaints could amount to gross misconduct and lead to dismissal without notice.

Further, sexual harassment may amount to both an employment rights matter and a criminal matter, such as in sexual assault allegations. In addition, harassment under the local regulation – which is not limited to circumstances where harassment relates to a protected characteristic – is a criminal offence.

- Make opportunities for training, development and progress available to all staff, who will be helped and encouraged to develop their full potential, so their talents and resources can be fully utilized to maximize the efficiency of ThreatMark.
- Decisions concerning staff being based on merit (apart from in any necessary and limited exemptions and exceptions allowed under the local regulation e.g. UK Equality Act).
- Review employment practices and procedures when necessary to ensure fairness, and also update them and the policy to take account of changes in the law.
- Monitor the make-up of the workforce regarding information such as age, sex, ethnic background, sexual orientation, religion or belief, and disability in encouraging equality, diversity and inclusion, and in meeting the aims and commitments set out in the equality, diversity and inclusion policy.

Monitoring will also include assessing how the equality, diversity and inclusion policy, and any supporting action plan, are working in practice, reviewing them annually, and considering and taking action to address any issues.

The equality, diversity and inclusion policy is fully supported by senior management.

Use of the organization's grievance and/or disciplinary procedures does not affect an employee's right to make a claim to an employment tribunal within three months of the alleged discrimination.

## 4. Anti-Corruption

ThreatMark adheres to the following core principles regarding anti-corruption:

- Zero tolerance towards corruption, including but not limited to Bribery, Extortion, and Fraud.
- Requirement to uphold the highest ethical standards and act with integrity when doing business.
- Prohibition of the offer or acceptance of business courtesies – gifts, hospitality, expenses, or other benefit – if they could constitute, or appear to constitute, an undue influence.
- Establishing appropriate policies and processes to prevent, detect, and tackle financial crime, including but not limited to corruption, fraud, extortion, tax evasion, sanctions violations, and money laundering in all its business arrangements.
- Taking effective measures to avoid, or when necessary mitigate, possible and actual conflicts of interest.
- Prohibition to enter into discussions or agreements with competitors regarding price fixing, market sharing, bid rigging, or other similar activities.

### 4.1. Anti-Bribery

Bribery means to promise/request, offer/accept, or transfer an item (material or non-material) of value (financial or non-financial) to induce or reward improper performance related to a commercial arrangement or public affairs. It also includes an unofficial payment made to secure or expedite a performance of a routine or necessary action to which the payer has legal entitlement.

ThreatMark is committed to conducting its business ethically and in compliance with applicable laws and regulations, e.g. the U.S. Foreign Corrupt Practices Act (FCPA), the United Kingdom Bribery Act (UKBA), and similar laws in other countries that prohibit improper payments from obtaining a business advantage.

ThreatMark strictly prohibits bribery or other improper payments in any of its business operations. This prohibition applies to all business activities, anywhere globally, whether involving government officials or other commercial enterprises. A bribe or other improper payment to secure a business advantage is never acceptable. It can expose individuals and ThreatMark to possible criminal prosecution, reputational harm, or other serious consequences. This policy applies to everyone at ThreatMark, including all officers, employees, contractors, or other intermediaries acting on ThreatMark's behalf. Each officer and employee of ThreatMark has a personal responsibility and obligation to conduct ThreatMark business activities ethically and in

compliance with all applicable laws based on the countries wherein ThreatMark does business. Failure to do so may result in disciplinary action, up to and including dismissal.

Improper payments prohibited by this policy include bribes, kickbacks, excessive gifts or entertainment, or any other payment made or offered to obtain an undue business advantage. These payments should not be confused with reasonable and limited expenditures for gifts, business entertainment, and other legitimate activities directly related to the conduct of ThreatMark business.

ThreatMark has developed a comprehensive program for implementing this policy through appropriate guidance, training, investigation, and oversight. ThreatMark's Compliance Manager has overall responsibility for the program, supported by the executive leadership of ThreatMark.

ThreatMark's Compliance Manager is responsible for giving advice on the interpretation and application of this policy, supporting training and education, and responding to the prohibition on bribery and other improper payments that apply to all business activities. Still, it is particularly important when dealing with government officials. The U.S. Foreign Corrupt Practices Act and similar laws in other countries strictly prohibit improper payments from gaining a business advantage and impose severe penalties for violations. The following summary is intended to provide personnel engaged in international activities with a basic familiarity with applicable rules so that inadvertent violations can be avoided and potential issues recognized in time to be properly addressed.

### **Common Questions About Anti-Bribery Laws**

The FCPA, UKBA, and other anti-bribery laws make it unlawful to bribe a foreign official to gain an "improper business advantage." A violation can occur even if an improper payment is only offered or promised and not made. Still, it fails to achieve the desired result, or the result benefits someone other than the giver (for example, directing business to a third party).

A "foreign official" can be essentially anyone who exercises governmental authority. This includes any officer or employee of a foreign government department or agency, whether in the executive, legislative, or judicial branch of government, and whether at the national, state, or local level. Officials and government-owned or controlled enterprises are also covered, as are private citizens who act in an official governmental capacity. Foreign official status often will be apparent, but not always. In some instances, individuals may not consider themselves officials or be treated as such by their governments but exercise authority that would make them a "foreign official" for anti-bribery laws. Personnel engaged in international activities are responsible under this policy for inquiring whether a proposed activity could involve a foreign official or an entity owned or

controlled by a foreign government and should consult with ThreatMark's Compliance Manager when questions about status arise.

ThreatMark prohibits offering, promising, or giving "anything of value" to a foreign official to gain an improper business advantage. In addition to cash payments, "anything of value" may include:

- Gifts, entertainment, or other business promotional activities.
- Covering or reimbursing an official's expenses.
- Offers of employment or other benefits to a family member or friend of a foreign official.
- Political party and candidate contributions.
- Charitable contributions and sponsorships.

Other less obvious items provided to a foreign official can also violate anti-bribery laws. Examples include in-kind contributions, investment opportunities, stock options or positions in joint ventures, and favorable or steered subcontracts. The prohibition applies whether an item would benefit the office directly or another person, such as a family member, friend, or business associate.

Under the law, ThreatMark and individual officials or employees may be held liable for improper payments by an agent or another intermediary if there is actual knowledge or reason to know that a bribe will be paid. Willful ignorance – which includes not making reasonable inquiries when in suspicious circumstances – is not a defense. It also does not matter whether the intermediary is itself subject to anti-bribery laws. All employees, therefore, must be alert to potential "red flags" in transactions with third parties.

ThreatMark and its affiliates must keep accurate books and records that reflect transactions and asset dispositions in reasonable detail, supported by a proper system of internal accounting controls. These requirements are implemented through ThreatMark accounting rules and procedures, which all personnel are required to follow without exception. Special care must be exercised when transactions may involve payments to foreign officials. Off-the-books accounts should never be used. Facilitation or other payments to foreign officials should be promptly reported and properly recorded regarding purpose, amount, and other relevant factors. Requests for false invoices or payment of unusual, excessive, or inadequately described expenses must be rejected and promptly reported. Misleading, incomplete, or false entries in ThreatMark books and records are never acceptable.

## 4.2. Gifts & Entertainment

On a modest scale, business gifts and entertainment are commonly used to build goodwill and strengthen working relationships among business associates. Providing or accepting occasional meals, small company mementos, and tickets to sporting and cultural events may be appropriate in certain circumstances. Occasionally, it may also be applicable to accept or provide offers involving travel with our business associates for business events. However, if offers of gifts, entertainment, or travel are frequent or of substantial value, they may create the appearance of, or an actual, conflict of interest or illicit payment.

ThreatMark has developed this policy to help employees make the right decisions when providing or accepting gifts, entertainment, or travel while conducting business on behalf of ThreatMark.

## 4.3. Accepting Gifts (Non-Government Officials)

ThreatMark recognizes that it is customary for some of its suppliers, customers, and other business associates to occasionally give small gifts to those with whom they do business. However, these gifts must not affect an employee's business judgment or give the appearance that judgment may be affected and must follow the customer's gift policy.

Accordingly, ThreatMark and its employees must be very careful when it comes to accepting gifts. As a rule, ThreatMark employees may accept gifts from suppliers, customers, or other business associates, provided the gift:

- does not create the appearance (or an implied obligation) that the gift giver is entitled to preferential treatment, an award of business;
- better prices or improved terms of sale;
- would not embarrass ThreatMark or the gift giver if disclosed publicly;
- if valued **US\$100 or above** (even if promotional), is reported to the recipient first and evidenced in the internal system (Compliance Service Desk on [help.threatmark.com](https://help.threatmark.com));
- does not exceed any specific limits established by local management; and
- would not prevent the recipient from awarding ThreatMark business to one of the gift giver's competitors.

The following gifts are *never* appropriate:

- cash or cash equivalent (such as gift cards or gift certificates);
- gifts that are prohibited by local law;

- gifts were given as a bribe, payoff, or kickback (e.g., to obtain or retain business, or to secure an improper advantage, such as securing favorable tax treatment);
- the gift giver's organization prohibits gifts the recipient knows; and
- gifts are given in the form of services.

Employees who receive a gift at an event of a ceremonial nature (e.g., a customer outing or a commemoration of a business transaction) that might not be appropriate under these guidelines, but is impractical or offensive to refuse, may accept the gift and then promptly report it to their supervisor and to Compliance Service Desk on [help.threatmark.com](https://help.threatmark.com). The employee and supervisor can then discuss the appropriate response. *ThreatMark employees must never ask for gifts, gratuities, or other items that benefit them personally, regardless of value.* Employees are expected to exercise good judgment in accepting gifts from suppliers, customers, or other business associates. Employees should talk to their supervisor when in doubt as to whether a gift is appropriate.

#### 4.4. Conflict of Interest

A conflict of interest occurs when an individual's personal interests could compromise his or her judgment, decisions, or actions in the workplace. Any case of conflict of interest must be immediately reported (see Chapter 11 – Reporting and Monitoring System).

Examples of conflict of interest:

- Starting a business that competes with ThreatMark business.
- Hiring an unqualified relative or friend.
- Failing to disclose that you're related to a job candidate ThreatMark is considering hiring,
- Making arrangements to work for a vendor or client at a future date while continuing to do business with them.
- Posting to social media about the company's weaknesses.
- Offering paid services on your time off to a company customer or supplier.
- Working (even part-time) at a company that sells a competing product or service as ThreatMark.
- Accepting payment from another company for information about ThreatMark or its business.
- Failing to investigate a subordinate or coworker's wrongdoing because they are a friend.
- Sharing confidential information about ThreatMark, its business or products with a competitor.
- Making a purchase or business choice to boost a business that you have a stake in.

- Accepting a favor or a gift from a client above the amount or not in a form specified as acceptable by ThreatMark.
- Owning part of a business that sells goods or services to ThreatMark.
- Doing business or working for a competitor.
- Accepting consulting fees and providing advice to another company for personal gain.
- Sharing information about ThreatMark activities or plans that were not made public.
- Taking advantage of confidential information learned on the job for your benefit.
- Cashing in on a business opportunity that ThreatMark might have pursued.
- When a decision-maker at ThreatMark is closely related to a person, who is involved on a customer side. Closely related persons are spouses, children, parents, and other close family members.
- You are a politically exposed person (it means a natural person who is or who has been entrusted with prominent public functions).

## 5. Anti-Money Laundering / Anti-Terrorism

### Financing

ThreatMark implements the following procedures and controls to mitigate the risks of money laundering and terrorist financing.

“Money Laundering (ML)” means any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources i.e. the concealment, acquisition, use, or possession of criminal property.

“Terrorist financing (TF)” encompasses the means and methods used by terrorist organizations to finance their activities. This money can come from legitimate sources, for example from business profits and charitable organizations, or from illegal activities.

#### 5.1. Culture and Values

ThreatMark takes all reasonable measures to ensure that proper safeguards exist to mitigate the risks of Money Laundering (ML) and Terrorist Financing (TF) and to prevent a contravention of any requirement under the Guideline on Anti-Money Laundering and Counter-Terrorist Financing (AML Guideline).

ThreatMark implements adequate and appropriate Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) policies, procedures, and controls, considering factors including types of customers, products, and services offered, delivery channels, and geographical locations involved.

#### 5.2. Allocation of Responsibilities

ThreatMark senior management assesses the risks the firm faces and how the ML/TF risks are to be managed and ensures all relevant staff is trained and made aware of the law and their obligations under it.

ThreatMark senior management (C-level) oversees all activities relating to ML/ the prevention and detection of ML/TF and provides support and guidance to ensure that ML/TF risks are adequately managed.



### **5.3. Risk Identification and Assessment**

ThreatMark applies a risk-based approach to assess which customers are to be of higher risk of ML/TF. The following are some risk factors to be identified:

- types of customers and behavior;
- products and services offered;
- delivery channels; and
- customer's business organization/geographical locations involved.

ThreatMark takes enhanced measures (including customer due diligence and ongoing monitoring) to manage those customers with higher risks and knows that simplified measures may be applied to customers with lower risks.

### **5.4. Customer Due Diligence (CDD), Record Keeping and Ongoing Monitoring**

ThreatMark carries out CDD according to the conditions as stated in the AML Guideline. ThreatMark adopts a risk-based approach to use appropriate controls and oversight and accordingly determines the extent of due diligence to be performed and the level of ongoing monitoring to be applied.

ThreatMark monitors the business relationships with its customers under the conditions and keeps the documents obtained in the course of identifying and verifying the customer's identity and maintains the documents obtained in connection with the transactions for six years.

### **5.5. Cooperation with Regulators and Law Enforcement Agencies**

ThreatMark will cooperate with law enforcement agencies (e.g. Customs & Excise Department) in case of their routine inspection or investigation.

## 6. Third-party Due Diligence

ThreatMark has established standards and procedures for selecting, appointing, and monitoring partners, consultants, and other third parties. In all cases, these standards and procedures must be followed, with particular attention to “red flags” that may indicate possible legal or ethical violations. Due diligence ordinarily will include appropriate reference and background checks, written contract provisions that confirm a business partner’s responsibilities, and appropriate monitoring controls. Personnel working with third parties should pay particular attention to unusual or suspicious circumstances that may indicate possible legal or ethical concerns, commonly referred to as “red flags.” The presence of red flags in a relationship or transaction requires greater scrutiny and implementation of safeguards to prevent and detect improper conduct. Appointment of a partner or another third party ordinarily requires prior approval by an appropriate senior manager, a description of the nature and scope of services provided in a written contract, and appropriate contractual safeguards against potential violations of law or ThreatMark policy.

## 7. Segregation of Duties

At ThreatMark, we ensure the proper distribution of responsibilities within our organization. This principle is fundamental to maintaining internal controls, preventing conflicts of interest, and safeguarding against potential misconduct. Employees are assigned tasks in a manner that minimizes the risk of any single individual having control over multiple stages of a process, thus promoting transparency, accountability, and the integrity of our operations.

Task Allocation – responsibilities are distributed to different individuals or departments to create a system of checks and balances. This helps prevent the concentration of power and reduces the risk of errors or fraudulent activities.

Conflict Prevention – we mitigate conflicts of interest by ensuring that no single individual has unchecked authority over a critical business process. This measure is essential in maintaining ethical conduct and protecting the interests of our stakeholders.

Internal Controls – we implement internal controls to enforce the segregation of duties effectively. Regular rights reviews and assessments are conducted to identify and address any potential weaknesses.

Chinese wall arrangement – the purpose of a Chinese wall is to maintain confidentiality and prevent conflicts of interest that involve handling sensitive or privileged information. ThreatMark access management policy ensures that individuals within one part of the organization do not have unauthorized access to information held by another part without the proper reason. Thus minimizing the risk of insider trading, conflicts, or the misuse of privileged information.

## 8. Environmental obligations

ThreatMark conducts its activities with due respect for the environment and takes initiatives to reduce its ecological footprint by the following:

- Actively supports activities that promote health and contribute to cleaner air and more pleasant, safer, and healthier cities where we live and work.– e.g. [Bike to work challenge](#).
- Promotes eco-friendly technologies, products, and services, with the aim of contributing to sustainable development.
- Implement appropriate measures to prevent and/or minimize consequences while continually striving to enhance environmental performance.
- Support the objectives outlined in the Paris Agreement.

## **9. Social Responsibility (CSR)**

As part of our commitment to Corporate Social Responsibility (CSR), we recognize the profound impact we can have on the community and the environment, and thus, we collaborate with ADRA, a distinguished charity organization. Throughout the year, our team engages in meaningful volunteering activities, dedicating our time and resources to make a positive difference in the lives of those in need. Through these initiatives, we aim to foster a culture of compassion, community engagement, and environmental consciousness within our organization, embodying our commitment to social responsibility and more sustainable future for all.

## 10. Grieving and Disciplinary Procedure

A Grieving and Disciplinary Procedures are formal processes used to handle complaints, grievances, or conflicts in a systematic way.

### 10.1. Grieving Procedure

Dealing with grievances informally – If a grievance or complaint related to work or colleagues arises, it should, wherever possible, first be discussed with the manager. A solution may be agreed upon informally between the parties involved.

Formal grievance – If the matter is serious and/or is to be raised formally, the grievance should be set out in writing and provided to the manager. Facts should be stated, and language that is insulting or abusive should be avoided.

Where the grievance concerns the manager, and approaching them is not feasible, another manager or the owner should be approached.

#### **Grievance hearing**

A meeting to discuss the grievance will be arranged by the manager, normally within five days. The right to be accompanied by a colleague at this meeting is granted, provided a reasonable request is made.

Following the meeting, a decision will be communicated in writing by the manager, normally within 24 hours.

If additional information is required before a decision can be made, the manager will inform the employee, along with the expected timescale for gathering the information.

#### **Appeal**

If the decision made by the manager is unsatisfactory, an appeal should be communicated to the manager.

An appeal meeting will be scheduled, normally within five days, and will be heard by a more senior manager or the company owner. The right to be accompanied by a colleague at this meeting is granted, provided a reasonable request is made.

After the meeting, a final decision will be communicated by the senior manager or owner, normally within 24 hours. This decision is final.

## Record Keeping

Information about a complaint by or about an employee may be placed on either party's personnel file, along with a record of the outcome and any other notes or documents compiled during the process. These will be processed in accordance with our Information Security Policy.

## 10.2. Disciplinary Procedure

The aim of the Disciplinary procedure is to ensure consistent and fair treatment for all in the organization.

### Principles

- Informal action will be considered, where appropriate, to resolve problems.
- No disciplinary action will be taken against without a full investigation.
- Employees will be informed of any complaints against them and given a chance to respond before a decision is made.
- Written evidence and witness statements will be provided when relevant.
- At all stages the employee can be accompanied by a work colleague.
- No employee will be dismissed for a first offence unless it is **gross misconduct**, which may result in dismissal without notice.
- An employee have the right to appeal against any disciplinary action.
- The procedure may start at any stage if the employee's alleged misconduct warrants this.

### The Procedure

The Procedure will be performed in compliance with applicable legislation (e.g. violations of labor discipline under the Labour Code) and may include:

- In case of Performance issue: An improvement note outlining the problem, required improvement, timeline, and support available.
- In case of Misconduct: A written warning will outline the issue, required change, and the right to appeal. It will state that further misconduct may result in a final warning that dismissal may follow.
- Dismissal or Other Sanctions: If misconduct continues, dismissal or other actions (such as demotion or suspension) may follow. Only senior managers can make dismissal decisions.

## **Gross misconduct**

The following list provides some examples of offences which are normally regarded as gross misconduct:

- theft or fraud;
- physical violence or bullying;
- deliberate and serious damage to property or misuse of ThreatMark's name;
- unlawful discrimination or harassment;
- a serious breach of Code of Conduct, health and safety rules;
- a serious breach of information security rules, Information Security Policy or the guidelines and procedures implementing the policy.

## **Appeals**

An employee who wishes to appeal against a disciplinary decision must do so within five working days. The senior manager will hear all appeals and his/her decision is final. At the appeal any disciplinary penalty imposed will be reviewed.



# 11. Reporting and Monitoring System

ThreatMark appoints a Compliance Manager as a central reference point for reporting any suspicious or unlawful actions, transactions, or breach of law or this Code of Conduct.

## 11.1. Compliance Manager

For receiving and assessing reports of possible infringements within the company is responsible Compliance Manager, who is

**Veronika Zelinko, HR & Back Office Manager, [veronika.zelinko@threatmark.com](mailto:veronika.zelinko@threatmark.com).**

In carrying out his/her activities under this Policy, the Compliance Manager shall be impartial and shall observe confidentiality of the facts of which he/she becomes aware in the performance of his/her duties.

Compliance Manager shall maintain strict confidentiality about the identity of the reporting person (whistleblower), the details of other natural persons, and in relation to the information contained in the received report. ThreatMark declares that the Compliance Manager will not be penalized in any way for the proper performance of his or her activities according to this Policy.

Responsibilities and duties:

- Notify the CEO within 10 days that he/she has ceased to meet the integrity requirement.
- Not to disclose information that could undermine or jeopardize the reporting process.
- Must not provide information on the identity of the Reporting Person (without the written consent of the whistleblower), unless they're obliged to provide this information to the competent (public) authorities under other legislation.
- Keep a record of reports and documentation received for at least 5 years after receipt of the report.
- Recommend remedial action.
- Compliance Manager shall submit to his/her immediate superior by 1 March of the following calendar year, a written report of his/her activities for the preceding calendar year.

## 11.2. Protection of Reporting Person

Any natural person who has reason to believe that a violation of this policy or any law has occurred, or may occur, must promptly report this information through an internal or external reporting system.

The person who reports or publicly discloses information on breaches acquired in the context of his or her work-related activities is referred to as a Reporting person, also known as a whistleblower. It can be a current, former, or future employee, job applicant, contractor, partner, member of ThreatMark's governing bodies, contractors, or subcontractors.

Retaliation in any form against an employee who has, in good faith, reported a violation or possible violation of this policy is strictly prohibited. ThreatMark declares that it will protect the reporting persons and will not retaliate against him/her. Retaliation means any direct or indirect act or omission which occurs in a work-related context, is prompted by reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.

This protection includes also third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and legal entities that the reporting persons own, work for, or are otherwise connected within a work-related context.

The protection does not apply to persons who knowingly make false accusations or deliberately provide false information.

### 11.3. Internal Reporting System

A report can be made by the following means:

- By grieving procedure described in the chapter 10 – Grieving and Disciplinary Procedure (if relevant to the reporting issue).
- Compliance Service Desk on [help.threatmark.com](https://help.threatmark.com).
- By email to [whistleblowing@threatmark.com](mailto:whistleblowing@threatmark.com).
- By phone to Compliance Manager. The phone call will not be recorded. Phone call minutes will be made by a Compliance Manager. The Reporting Person is entitled to check, correct, and approve the call minutes with his/her signature.
- In writing by letter labeled as „Whistleblower Protection“ or „Ochrana oznamovatele“ to the Compliance Manager sent to the address ThreatMark s.r.o., Hlinky 505/118, 603 00 Brno, Czech Republic.
- In person to the Compliance Manager – based on a request Compliance Manager is obliged to meet the Reporting Person in person within 10 working days from the request date. An audio recording will be made from this meeting. If the Reporting Person does not agree to the recording, the Compliance

Manager shall make a meeting minutes of the meeting. In such a case, the Reporting person shall be entitled to check the record, verify it, and approve it by his/her signature.

- Via a web form on the company website [www.threatmark.com](http://www.threatmark.com).

The report may also be made anonymously (for example from an anonymous email or by sending a letter), in which case ThreatMark declares that it will not seek the identity of the notifier.

## 11.4. External Reporting

The Reporting Person can also make a report to the [Ministry of Justice Czech Republic](#).

## 11.5. Procedure For Handling Reports

The report is accepted in any form (written, oral, or in person). Compliance Manager informs the Reporting Person within 7 days of receipt of the report. Compliance Manager assesses the validity of the report and notifies the Reporting Person within 30 days of the results of the assessment of the report. In legally and factually complex cases, this time limit may be extended by up to 30 days.

If Compliance Manager finds the notification to be justified, he/she shall propose to remedy the situation or procedure to prevent and mitigate the unlawful situation.

## 12. Final Provisions


ThreatMark provides training to all relevant staff (including new staff) to ensure they are made aware of the Code of Conduct facilitating them to recognize suspicious activities/transactions. ThreatMark keeps training records/records of relevant courses or seminars attended.

ThreatMark keeps this policy and procedures under regular review and assesses that the risk mitigation procedures and controls are working effectively.

Questions about the policy or its applicability should be directed to ThreatMark's Compliance Manager.

Approving authority

Effective date January 31, 2025

DocuSigned by:  
  
.....45264D4325F6415.....

Michal Tresner, CEO