COC

CODE OF CONDUCT

PREVENTING
AND INVESTIGATING
CYBERCRIME
SINCE 2003

ZERO TOLERANCE
FOR CYBERCRIME

GROUP-IB ®

Contents

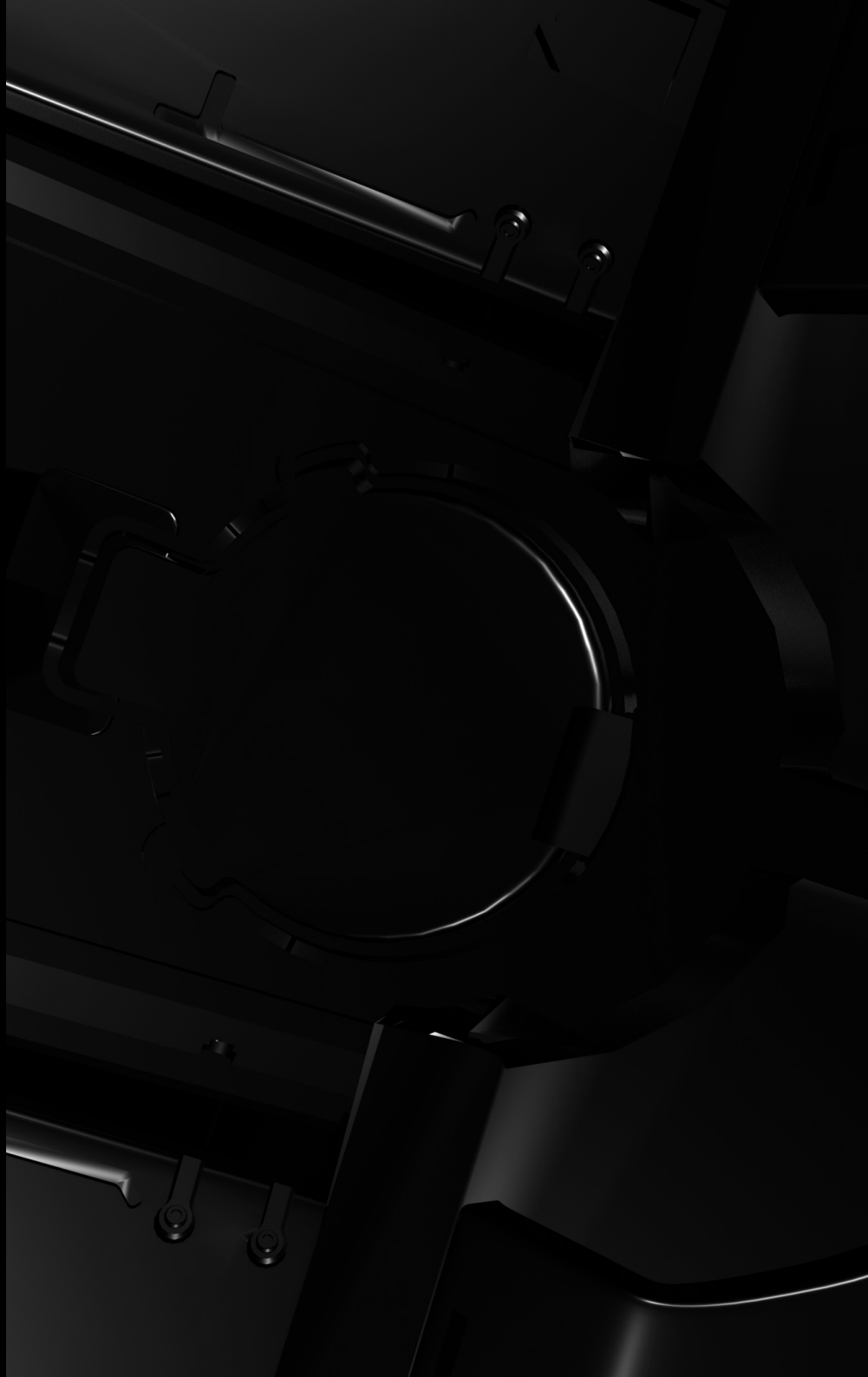
1. Introduction

We should all work in a way that makes us proud of ourselves and our achievements. We undertake new tasks and projects head on, even when skeptics insist they can't be done. We strive to succeed in our mission to protect clients in cyberspace using innovative products and services. As such, we expect all our employees, as well as anyone working for Group-IB or on its behalf, to act lawfully, honestly, ethically, professionally, and in our company's the best interests. At any moment we can find ourselves in a situation where the right thing to do is not obvious, and that is where this Code can help. We cannot promise that the Code will answer your every question, but it might provide guidance when the answer is not clear.

2.Who is covered under the Code?

It does not matter which department you work at or what you do at the Company – we expect you to use your good judgment and comply with the Code. This includes all full-time and part-time employees at every level of the Company, all the way up to the executive level. The Code also applies to controlled subsidiaries and entities in which the Company either owns a majority interest or manages operations (all of the above are referred to throughout this Code as "the Company" and "Group-IB").

Our customers, suppliers, and business partners, as well as anyone else who works on the Company's behalf, must share our commitment to integrity by following our Code's principles when providing goods and services to the Company or acting on its behalf.



3. The Code's purpose

This Code helps:

- Conduct business in an ethical and honest manner
- Uphold our values and protect reputation
- Understand what Group-IB expects from you
- Understand where to seek assistance and guidance if you have questions
- Make the right decisions day by day
- Comply with the laws, regulations and standards that apply to Group-IB

4. Our core values and guidelines

Group-IB is a global threat hunting and intelligence company. Our technological leadership and R&D capabilities are built on the hands-on experience in cybercrime investigations worldwide and cybersecurity incident response accumulated in our leading forensic laboratory and round-the-clock CERT-GIB. Group-IB's experience, and threat hunting and intelligence have been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyber threats.

We have zero tolerance for the development of cyber-weapon and criminal activity of any kind. Some companies may hire talented former black hat hackers, but that's not about us. The Company does not employ people with a criminal past. We hire individuals with extensive knowledge in the field of cybersecurity who are white hats — but only after sophisticated multilayer background security checks. Moreover, we do not help cybercriminals, hackers, or malware developers. When a new client approaches us, the Security Department checks them against various criteria to determine whether they are bona fide. We fight the crime of various kinds and we help honest people stop criminals.

Integrity and honesty toward colleagues, clients, partners, and investors are crucial. You must be honest — though above all with yourself. Only then can you be honest with colleagues, partners, investors, and clients. Respect for others, responsibility for your actions, and teamwork are essential elements of who we are and how we do business.

5. How to make right decisions

When faced with a difficult decision about how to conduct business, ask yourself:

- Am I confident that this course of action is legal?
- Does it comply with our Code?
- Does it reflect our values and ethics?
- Does it benefit the Company as a whole?
- Would I be comfortable if my actions were made public?

If you can confidently answer "YES" to all these questions, the course of action is probably the right one. But if you are unsure about any of the answers, it is likely a signal that you should ask for advice. After all, when you are not sure about the consequences, it is always better to ask before you act.

6. What if you have a Code-related question or concern?

No Code – and ours is no exception – can cover every possible scenario and situation that you might encounter at work. If you cannot find an answer here or have questions about the Code interpretation, seek guidance. Similarly, if you become aware of something that appears to violate the Code or the law, or any other suspicious behavior, you should speak up and report it immediately so we can address it. When you report concerns, you help us handle issues properly, fix problems in a timely manner, and remedy existing situations. You can report violations and share concerns by contacting your manager or your colleagues in the Talent Development and Happiness Department or the Legal Department. Information on reporting channels can be found in section 28 of this Code.

7. Non-retaliation

We encourage our team to ask questions and raise matters without fear of retaliation. We are committed to treating violation reports with care and investigating them thoroughly. We value your help in preventing and uncovering possible misconduct and we do not tolerate retaliation against anyone who reports suspected misconduct or otherwise assists with an investigation or audit. We believe that sharing a good-faith concern about the Code, even if it turns out to be unfounded, is never an excuse for any kind of retaliation.

8. No false accusations

Although we encourage honest reporting, we do not tolerate anyone making false reports knowingly. Making a false accusation could divert investigatory resources away from damage, morale, and credible concerns. Report what you have a reasonable concern in good faith, but never knowingly make a false accusation, lie to investigators, or refuse to cooperate in an investigation as such actions may also violate the Code.

9.Conflicts of interest

We are expected to use our judgment to act at all times and in all ways, in the Company's best interests while performing our job. That means that we should avoid conflicts, or anything that could appear as a conflict, between our own interests and the Company's. We believe that every business decision should be made objectively and with the Company's business interests in mind.

When considering a certain course of action, ask yourself whether the action you are considering could create an incentive for you – or appear to others like it is creating an incentive for you – that would benefit you, your family, or your friends, or an associated business, at the Company's expense. If so, the action you are considering is likely to create a conflict-of-interest situation, which you should avoid. You should keep in mind that even the appearance of a conflict is inappropriate and could damage our reputation that we are building every day. It could also damage the Company's effectiveness, our business, and the team.

You should be aware that conflicts can take many different forms, but very often they involve personal investments, outside employment and advisory roles, personal relationships, and accepting gifts, entertainment, and other business courtesies; information on some actual examples can be found below. Ultimately, however, the distinctive feature of all these situations is someone's personal interest affecting the decision-making process with regards to the business, thereby harming the Company's interests.

The following general rule can be applied to all the situations mentioned above: if you are considering entering into a business situation that creates a conflict of interest, do not do it. If you are in a business situation that may create a conflict of interest – or the appearance of a conflict of interest – review the situation with your manager. It is also important to understand that circumstances can change, and that a situation that previously did not present a conflict of interest could presents one later. As such, it is important for employees to disclose any relationships, associations, or activities that could create actual, potential, or even perceived conflicts of interest to either their manager or the Talent Development and Happiness Department.

10. Personal investments

There are many companies in which you could invest to strengthen your finances and build your investment portfolio. When choosing a company to invest in, you should avoid any that are Group-IB's customers, business partners, or competitors if the investment might cause – or appear to cause – you to act in a way that could harm the Company. If you are not sure whether a company you want to invest in is a competitor, ask your manager or the Chief Financial Officer.

To determine whether a personal investment creates a conflict of interest, you should consider the relationship between the business of the company you want to invest in, Group-IB's business, and what your role entails. When analyzing your job's influence, you need to check whether the company in question has a business relationship with Group-IB that you can guide or influence and the extent to which the company competes with Group-IB.

Investments in venture capital funds or funds that invest in a broad cross-section of companies that may include our competitors or business partners generally do not create conflicts of interest by itself. Moreover, if you own securities of publicly traded companies, everything is in order and you have nothing to worry about. A conflict of interest may exist, however, if you control a fund's investment activity or own a majority stake in a company, for example.

11. Outside employment and advisory roles

Having a second job or consulting role is permitted so long as it does not affect your performance within the Company. If your judgment could be – or could appear to be – influenced in a way that could harm the Company and its business, you should not accept employment or advisory positions with Group-IB's competitors or partners. If you receive a job offer from the Company's former employees or competitors, or you are not sure whether any other received offer is acceptable, we encourage you to ask for guidance from your manager.

12. Personal relationships

You cannot manage or make decisions about Group-IB's business relationships, whether potential or existing, that involve any of your relatives, your spouse, your significant other, or your close friends. For example, you cannot be the hiring manager for a position for which a close friend or relative is being considered or be the manager for a company associated with your spouse or significant other. Of course, the fact that your relative, spouse, significant other, or close friend works at the Company or becomes a business partner, customer or competitor is not enough to create a conflict of interest. However, if you are also involved in that business relationship on the Company's part, it becomes a sensitive issue. In such situations, the right thing to do is to discuss the relationship with your manager and the Head of the Legal Department.

For the purposes of our Code, a relative can also be someone who lives with you, someone who is financially dependent on you, or someone you are financially dependent on, regardless of the familial relationship between you.

13. Gifts, entertainment perks, and other business courtesies

The Company's policy is quite simple: we do not exchange gifts or entertainment perks that looks like an attempt to inappropriately influence a business decision.

No matter if you are the recipient or giver, you must recognize when an offer is excessive. It can sometimes be difficult to tell when a gift crosses a line, and that is where our Code can help.

When it comes to gifts and benefits, use sound judgment and comply with the law. Generally, it is permissible to accept inexpensive, so-called token, non-cash gifts. Infrequent and moderate business meals, attending entertainment events with clients and business partners, occasional invitations to local events, and celebratory meals can all be appropriate aspects of a business relationship as long as they are not excessive and do not create an appearance of impropriety.

Never allow gifts, entertainment perks, or other personal benefits to influence decisions or undermine the integrity of a business relationship, however. Do not accept gifts or benefits that are not available to others, like a special discount, that are illegal and/or immoral, and that could reflect negatively on the Company. You should also not accept cash, cash equivalents, stocks, or other securities.

If you have any doubts about a gift or entertainment perk, you should check with the Legal Department before giving or accepting anything of value. You can learn more on the matter by reading our Anti-bribery Policy.

14. Confidentiality

Information is one of our most valuable assets and we are committed to protecting it and handling it in a confidential manner – whether it is our own information or information entrusted to us. Information within Group-IB is held in many different formats, including on paper and electronically in documents or in IT applications and systems. As such, is important to mention

that our requirements relating to protecting information apply to all formats. You are required to use confidential information for business purposes only and must always keep such information in strict confidence. This responsibility extends to third-party confidential information that we have received under non-disclosure agreements. As a team, we understand that protecting non-public information at the highest level helps us maintain a competitive advantage and preserve our reputation and good name.

Examples of confidential information include customer lists, proprietary data, financial information, budgets, pricing, business plans, trade secrets and know-how such as software and product designs, product plans, inventions, laboratory notebooks, processes, designs, drawings, engineering, employee data, and any other business information – this is not a complete list.

To maintain confidentiality, you cannot share or discuss such information outside the Company unless there is an appropriate non-disclosure agreement in place or unless and until that information is released publicly through a press release, official statement, or formal communication from a senior manager or a spokesperson. As for internal use, although we communicate freely you should avoid sharing or discussing confidential information beyond team members who legitimately need to know it for the purposes of their job. We have no intention to meddle in conversations or interactions between colleagues, but we encourage you to use your best judgment and share only what is appropriate within Group-IB in order to facilitate everyone's jobs. When handling any information, always keep in mind that improper use or disclosure of confidential information could seriously damage Group-IB's reputation among clients, business partners, and the community, harm our business, and expose us to liability. Do your part to keep it safe.

If you have any doubts about how to handle any Group-IB information (restricted or otherwise), you should seek advice from the Legal Department.

15. Privacy

We believe that trust is the basis of any good relationship. Our clients and partners entrust us with their personal information or that of third parties, when they do business with us. Our team members do the same when they join Group-IB. Preserving that trust requires that each of us keeps that information private and secure. Group-IB respects the privacy of all individuals and their personal data, including digital information we hold. The Company follows the legislative rules and best practices to stay in compliance with applicable data protection laws, particularly the GDRP. We understand that keeping personal information secure is very important to our team, business, good name, and reputation, and we take our responsibility and obligations to our clients, business partners, and employees seriously. We collect, use, and process personal information for legitimate business purposes only and we protect it from possible loss, misuse, or unauthorized disclosure.

When collecting, using, or storing personal data, keep in mind that you should collect data that is adequate and relevant and use it solely for the purpose for which it is collected. In accordance with applicable law, we must be transparent about how personal data will be used when obtaining consent from individuals. Never share personal data with unauthorized individuals outside Group-IB or anyone within the Company who does not need the information to do their job – always keep personal data confidential and secure. We expect you to act responsibly and ethically all the while upholding our core values. Always consider the risk to individuals in using their personal data and take steps to minimize such risks. Lastly, do not store personal data for longer than necessary to achieve the business goal or meet legal requirements.

If you are not sure whether you are handling personal information properly or whether you are using it in accordance with our policies and procedures, ask your manager, the Data Protection Officer, or the Legal Department.

16. Responsible use of the collected information

As mentioned above, we believe that our mission is to protect our clients in cyberspace by creating and using innovative products and solutions. Following our mission, we collect data about cyber threats to keep information secure, prevent incidents, and create analytical reports and systems to increase the level of cybersecurity not only for us and our clients but in general.

In doing so, we must stay within the legal field. This means that our team members should be guided by the principle of legality when performing their professional duties. We respect the laws of the countries where we operate, and we have adopted relevant policies to legally carry out business activities worldwide.

Our team members can use data on cyber threats obtained by the Company:

- To ensure our cybersecurity
- To perform analyses and generate analytical and statistical reports so that we can improve security systems and help increase general awareness in the field of information security
- To provide services to our clients in terms of ensuring information security and preventing information security incidents
- As content for our software used to provide information security and incident prevention services

The general rule for working with information – remember about security and privacy. Any data obtained should be processed and stored using technical means and methods that ensure a high level of security. We must exclude unauthorized access, collection, copying, destruction, modification, distribution, and other methods of using data illegally. Above all, to work with a client's data we must first obtain their consent.

We are not engaged in any intelligence or surveillance operations, and neither we detain nor arrest cybercriminals by ourselves. For cyber investigation purposes we identify mechanisms by recreating event sequences and collect digital evidence that will eventually lead us to the perpetrators. We help corporate security services and law enforcement agencies worldwide bring criminals to justice, which is why we need to gather large amounts of data.

17. Governmental customers

Working with any customers connected to a state or governmental structures, we maintain the engineer neutrality and independence: the Company does not use any influence, mechanisms, connections, and contacts that could be provided by such customers to its own advantage.

18. Intellectual property rights

Be aware, that if you create or develop something for Group-IB during working hours as part of your duties or when using the Company's resources, all such creations and developments will belong to the Company. The list of potential creations is broad and includes developing new products, improving existing ones, and producing inventions, algorithms, articles, reports, artwork, and other forms of intellectual property.

Our employees are expected to conduct their work activities, protecting the Company's IP rights. We strongly encourage you to speak up any violations of the Company's IP rights. If you become aware about or suspect any violations of the Company's rights, or if have any questions or doubts, you should seek advice from or report to your colleagues in the Legal Department.

Speaking of intellectual property, it also needs to be noted that our team uses only appropriately licensed software only. You are expected not to make or use illegal or unauthorized copies of any software, whether in the office or at home, since doing so may constitute a copyright infringement and may expose Group-IB to potential legal liabilities, not to mention damage our reputation as the leaders in the field of intellectual property protection.

19. Fair play

Group-IB always competes with integrity and follows applicable antitrust and competition laws. We are committed to outperforming our competitors legally and ethically, within the framework of a free market in all locations where we operate. We strive to avoid even the appearance of unfairly restricting another company's ability to compete against us. We believe there is only one way to build a market share and loyalty to our brand: by delivering high-quality products and services rather than engaging in unfair or anti-competitive practices.

Investigations by competition authorities can result in significant fines, costs, and compensation claims. They can also damage a company's good name, reputation, and commercial relationships, which is why we expect our team to:

- Never enter into anticompetitive agreements, whether formal or informal, written or verbal
- Never set prices or other terms of sale, coordinate bids, or allocate clients, sales territories, or product lines
- Never make inaccurate or untruthful comments about a competitor's products or services
- Never share commercially sensitive information with competitors unless approved by the Legal Department and use only legitimate means of obtaining competitive information
- Never abuse dominant market positions
- Never be part of certain restrictions imposed on or agreed with distributors and other clients
- Respect the confidential information and intellectual property rights of our competitors and other third parties

We encourage you to win business the right way – deal honestly and fairly with our clients and business partners. Together we can promote positive business relationships and never take unfair advantage of anyone by misleading or deceiving them – because we can be truthful about our Company and what kind of business we do. To be on the safe side, however, do not make any claims you cannot substantiate, inaccurate remarks about our competitors, or erroneous comparisons between their products and services and ours. If you have any doubts or questions, reach out to your manager or the Legal Department for guidance.

20. Insider trading

Within the company we share and discuss information (including non-public information) about the Company's business operations and projects relatively freely. Moreover, you might overhear a hallway or phone conversation or come across a document at a copy machine, either of which could involve confidential information. Using such non-public information to buy or sell securities or passing it along to others so that they may do so constitutes insider trading. Employees must not use insider information to buy or sell securities of any publicly traded company. Trading or encouraging others to trade insider information and sharing such information with unauthorized parties are criminal offences in many countries and can lead to fines or even imprisonment.

Inside information is not available to the public, and for a reasonable investor such information would probably be considered important in deciding whether to buy or sell securities. Business results or forecasts for the Company or for our business partners, a new major product or product incident, developments in litigation cases or dealings with regulators or governments – all of these are examples of insider information. We comply with the law and believe everyone should make investment decisions based on the same set of rules, so we do not trade insider information or tip others off so that they may do so.

The general rule here is to play it safe – if you are not sure if information is material and whether it is non-public inside information, treat it as though it is, and ask Legal Department before you act. If you suspect or know about the fact of insider trading, you need to report to Security Department on that.

21. Anti-bribery and facilitation payments

To support global efforts against corruption, many countries have laws that prohibit bribery. All businesses are subject to such laws, and Group-IB is no exception. A breach of anti-bribery laws may result in legal and financial consequences, hence we have one simple but effective rule – do not bribe anybody, anytime, for any reason. Every team member should keep in mind that even the appearance of illegal conduct could significantly damage our reputation. Our success is based on the quality of our products and services – never on unethical or illegal behavior. To uphold our high standards and our values of honesty and integrity, we can take only a zero-tolerance approach toward bribery and corruption of any kind. We never offer or accept anything of value in order to get business, keep business, or gain an unfair advantage.

You must follow anti-bribery and anti-corruption laws wherever you do your job and never offer, pay, promise to pay, or accept anything of value, either directly or indirectly, in order to improperly influence other people's judgment or actions.

22. Prevention of money laundering

Our Company complies with all laws that prohibit money laundering as well as illegal and illegitimate financing. We would never knowingly look the other way when it comes to illegal activities. However, we understand that criminal activity such as money laundering is not always obvious, so it is important that we work together to reduce our risk of exposure to it and speak up about anything suspicious.

In order to protect Group-IB's reputation and avoid any kind of liability, it is important not to become associated with criminal activities undertaken by others. In particular, we must all ensure that the Company does not receive any proceeds from criminal activities as this can amount to money laundering – a criminal offence. Our policy is to take the time to get to know our clients and business partners and their reputations for following the law by performing appropriate due diligence and screenings.

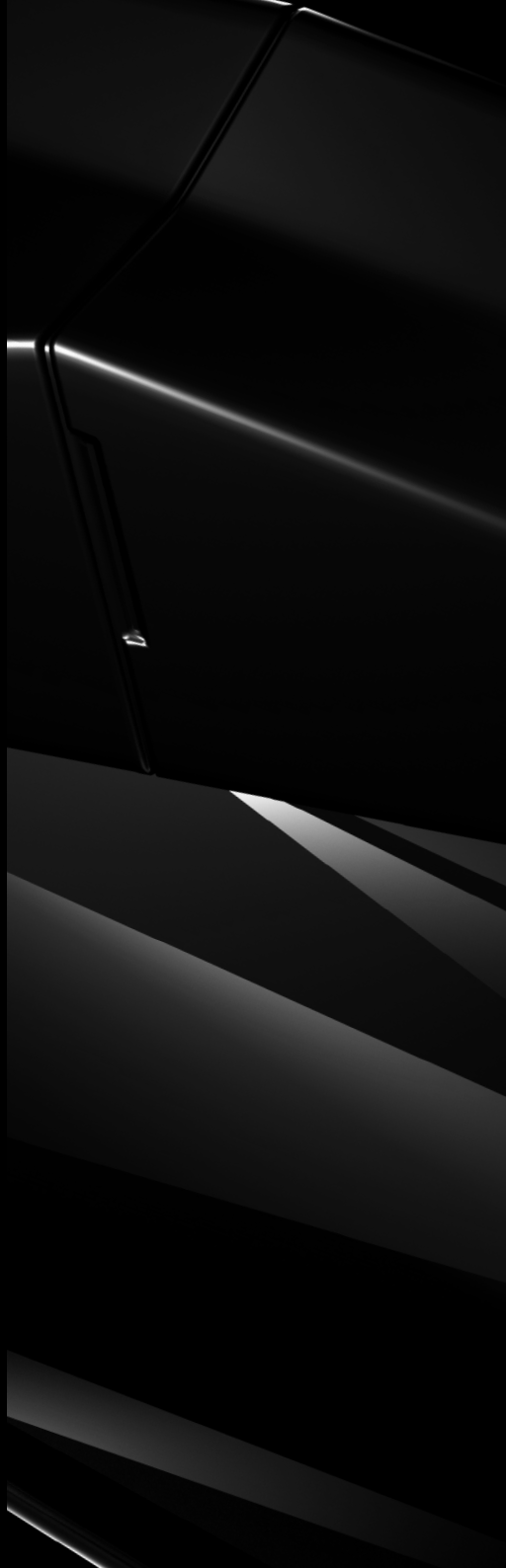
We ask you to be alert and proactive when it comes to spotting financial transactions that might signal a problem. If you notice or suspect an activity or transaction that does not fall under our normal process, report your concern to the Security Department. Potential warning signs include large cash payments and unusual fund transfers to or from foreign countries, clients, or business partners, and suppliers who provide incomplete information or avoid recordkeeping requirements. You should always ensure that you are conducting business with reputable counterparties for legitimate business purposes and with legitimate funds. Keep an eye out for the "red flags" mentioned above. If you suspect prohibited activities are taking place, speak up and report it.

23. External communications policy

Both social and traditional media provide opportunities to network and create exposure for the Company and its brand. All team members should be aware of the risks associated with using them, however. We respect your right to use social media for personal and professional purposes, but we expect you to use such platforms wisely and communicate responsibly.

Any public comments, posts, or any other form of communication on social networks about business-related issues, including simple statements of opinion that could be perceived as expert based on the workplace indicated in your profile should be coordinated with Group-IB's Communications Department first. If your profile states that you are a Group-IB employee, remember that all the information you publish may be perceived not as the opinion of a private individual, but as that of an expert at our Company. If you want to have a link to Group-IB in your profile but you are not an official spokesperson for the company, you must include a disclaimer that all opinions are your own. If your social media profile has no indication that you are a Group-IB employee and the subject of Group-IB comes up on social media, make it clear in any posts that your views are your own and that you are not speaking on the Company's behalf.

Under no circumstances should you disclose confidential or non-public information about the Company, our customers, suppliers, competitors, or business partners. You should also refrain from posting anything that might constitute a threat, harassment or bullying, and from publishing posts that are contrary to the company's information policy. We expect the same from our customers, suppliers, and business partners.



If you think that you may have sounded as though you were speaking on behalf of the Company in a post, it is important that you immediately contact your manager and the Corporate Communications Department so that they can help respond appropriately and minimize any damage that may have been done.

Traditional and digital media regularly cover Group-IB, so it is no surprise that our employees receive calls and emails or are approached via social media by journalists asking for comments. It is important to remember that all interactions with the media should be made through Group-IB's Communications Department. In case of any direct contact with a journalist, you should politely explain that all press requests must be made through the press service. If you are given a journalist's contact details, share all the information with Group-IB's Communications Department as soon as you can. Remember that only authorized Company spokespeople are allowed to communicate with journalists.

If you are an authorized spokesperson and are asked a question that is not related to your field, you should inform the journalist that you are not an official spokesperson on this issue and forward the request to Group-IB's Communications Department so that they can refer the journalist to the right expert to make a comment. If you are unsure about your answer, it is better to say nothing than to make false or misleading statements.

Any mentions of Group-IB in social and traditional/digital media by the Company's customers, business partners, and contractors should first be coordinated with Group-IB's Communications Department.

24. Political contributions

Group-IB does not make political contributions. We do not support any political party or candidate. Our employees are free to support any political party or entity on a personal level, but never on behalf of Group-IB. Such activities must be kept separate from the job and company business.

25. Protection and proper use of Group-IB assets

Group-IB's intellectual property (trademarks, logos, copyrights, trade secrets and patents) are among our most valuable assets. It is important to use them correctly as unauthorized use can lead to their loss or a serious loss in their value. You must respect all copyright and other intellectual property laws, including laws governing the fair use of copyrights, trademarks, and brands. You must never use the Company's logos, trademarks, or other protected information or property for any business venture without checking with the Legal team first. We strongly encourage every team member to report any suspected misuse of trademarks, logos, or other Group-IB intellectual property.

Naturally, we cannot respect our own intellectual property rights without respecting those of others. Inappropriate use of others' intellectual property could expose both you and the Company to fines and penalties. If you need to solicit, accept, or use proprietary information from third parties or let them use information from Group-IB, you must ask the Legal Department for advice before taking any action. You should also check with the Legal Department if you are developing a product involving content that does not belong to the Company.

Moreover, we provide our team with a wide range of valuable assets to help perform work on behalf of Group-IB at the highest level. Such assets include computers, mobile devices, communications platforms and equipment, software, office and electronic equipment, and facilities. We expect you to treat all these assets with care and use them with the Company's interests in mind and in accordance with our internal policies. Assets should be well maintained and not subject to unreasonable use, damage, or waste. If something you are using is damaged, please ensure that it gets fixed if possible. In addition, you should use your judgment in using company assets for personal matters – such use should not be excessive and should not interfere with performing your job. If you are unsure whether a certain use of company assets is acceptable, please ask your manager or the Talent Development and Happiness Department.

26. Respect and equal opportunity

We believe that each person is an important player within our team and should be respected and treated with dignity, honesty, and fairness. We are strongly against discrimination, harassment, bullying, and any other form of abuse – whether verbal, physical, or visual. We expect you to respect the skills, cultures, and backgrounds of your colleagues. All our employees, at any level, should be fair in making decisions and base them only on factors such as skills, qualifications, performance, and business needs

– never on personal characteristics. Everyone should be treated fairly and equally, without discrimination on the grounds of race, age, role, gender, gender identity, color, religion, country of origin, sexual orientation, marital status, dependents, disability, social class, or political views.

If you notice, experience, or suspect harassment or discrimination, speak up immediately – either directly to the person or through your manager, the Talent Development and Happiness Department, or the Legal Department. We take inappropriate behavior seriously and do not tolerate retaliation against anyone who reports it.

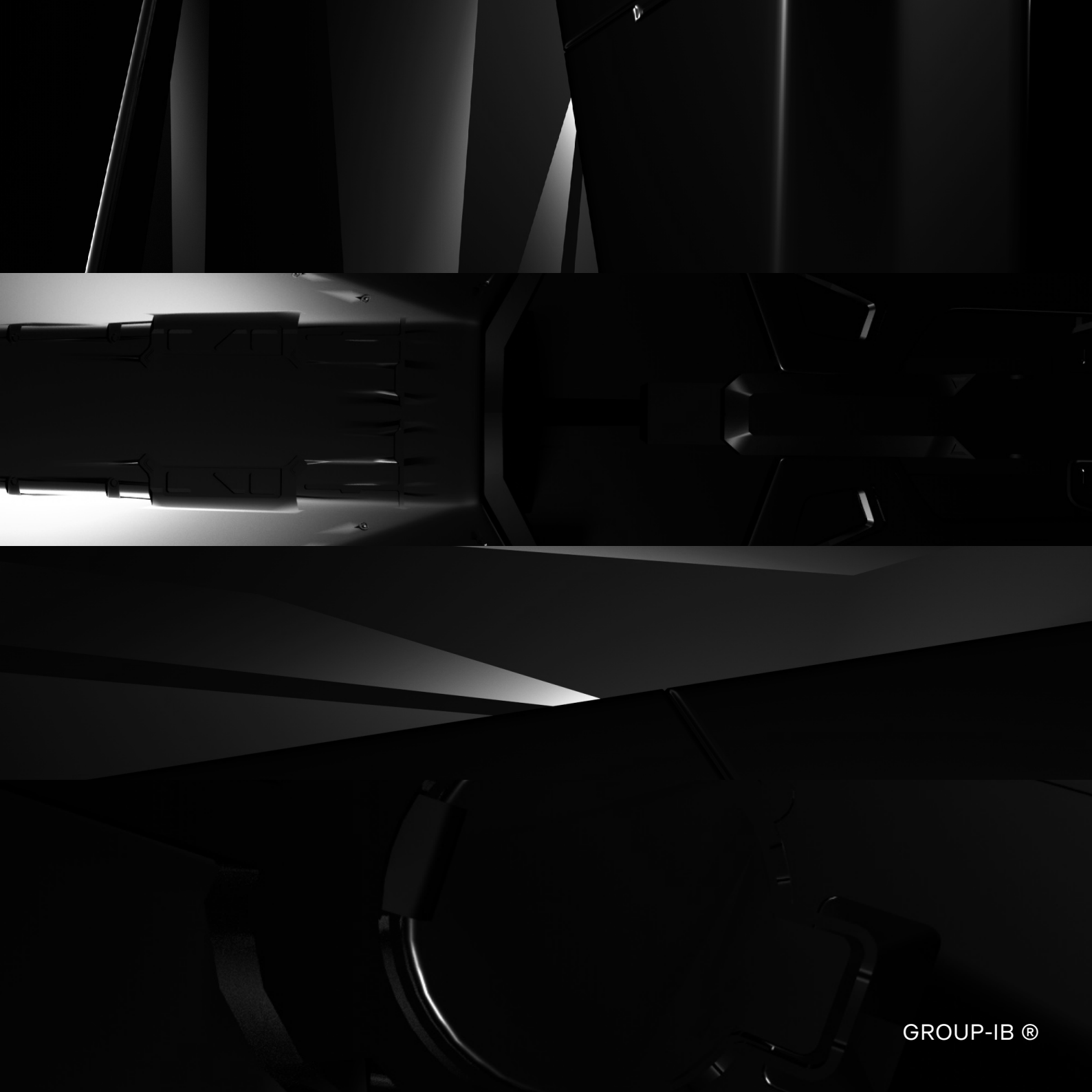
27. Safe workplace

We conduct our business in accordance with applicable health and safety requirements, and we strive to continuously improve our health and safety policies and procedures. We expect you to report workplace injuries, illnesses, and unsafe conditions.

We are committed to a violence-free work environment, so no level of violence – or even the threat of violence – will be tolerated at our offices. Under no circumstances can anyone bring a weapon to work. If you become aware of a violation of this policy, you should immediately report it to the Security Department and the Talent Development and Happiness Department.

28. Reporting channels

If you have any questions about this Code or think that it is being violated in any way, it is important that you discuss your doubts and report your concerns. Based on the Code's recommendations, you have the following options: discuss the issue with your manager or draw attention to it by sending a message to **codeofconduct@group-ib.com**, with the name of the department to which it is addressed in the subject line.


GROUP-IB ®