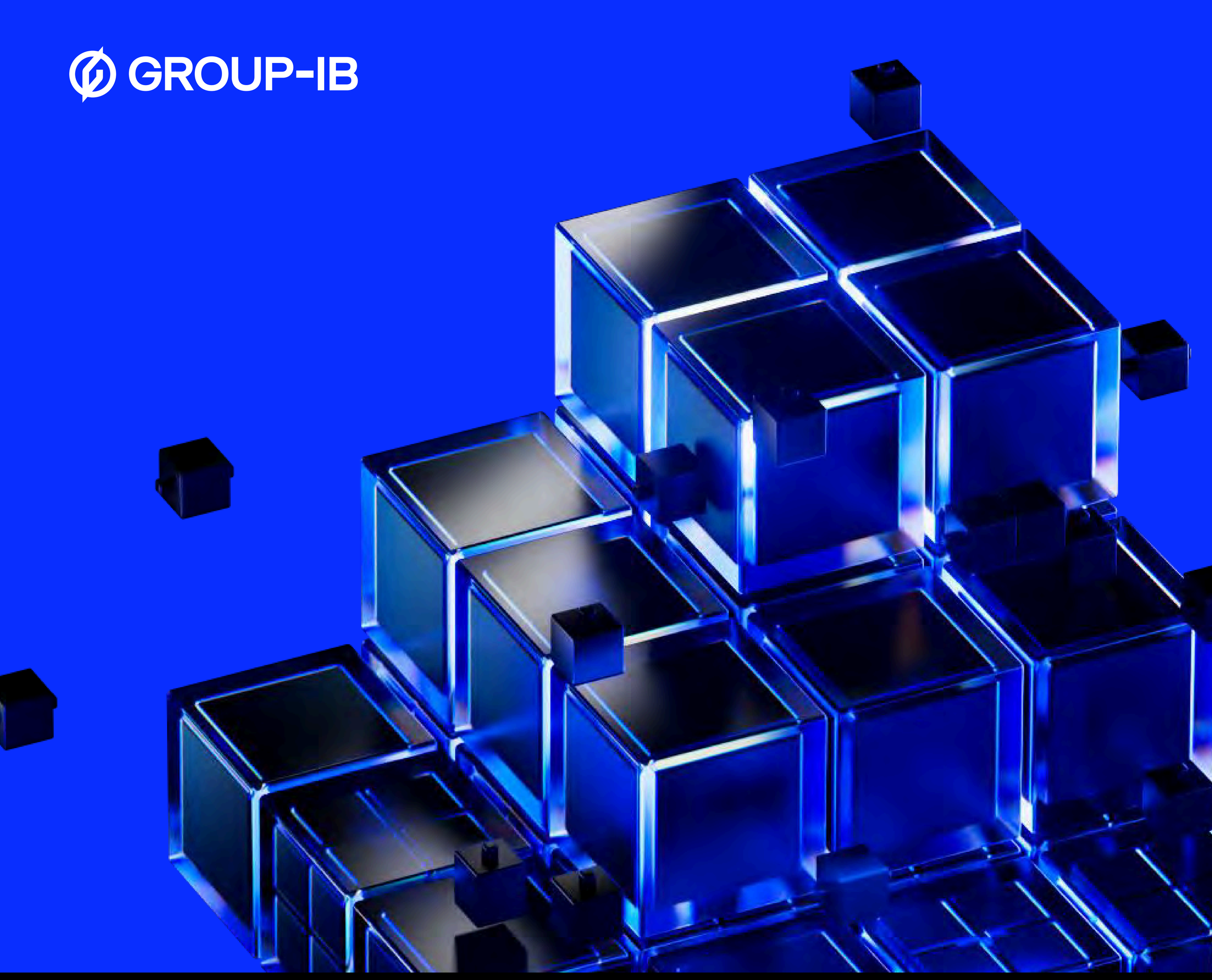
GROUP-IB



Code of conduct

Fight against cybercrime

GROUP-IB.COM

01 Introduction

We should all work in a way that makes us proud of ourselves and our achievements. We're eager to take on new challenges and make bold decisions to grow and innovate. We are united in our mission to combat cybercrime worldwide.

With that in mind, we expect everyone at Group-IB—including employees, contractors, consultants, and anyone working on our behalf—to act lawfully, honestly, ethically, and professionally, always in the best interests of the company.

There may be moments when the right course of action isn't immediately clear. That’s where this Code comes in. While it may not answer every question, it’s here to guide you when the path forward is uncertain.

02 Who is this Code for?

It doesn’t matter which team you work in or what your role is—we expect everyone to exercise good judgment and comply with this Code. This applies to all full-time and part-time employees, contractors, and team members at every level of the Company, including executive leadership.

The Code also applies to Group-IB’s global structure, including all Digital Crime Resistance Centers (DCRCs), branches and affiliated entities in which the Company holds a majority interest or exercises operational or management control —regardless of jurisdiction. Collectively, these entities are referred to throughout the Code as “the Company” or “Group-IB.”

We also expect our customers, suppliers, business partners, and anyone acting on the Company’s behalf to share our commitment to integrity by following the principles of this Code when providing goods or services or representing us in any capacity.

03 The Code’s purpose

This Code helps you to:

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

The Code is a binding framework for ethical conduct and policy compliance across the Company. Violations may result in disciplinary action, contractual consequences, or legal exposure.

04 Our core values and guidelines

Group-IB is a global cybersecurity powerhouse. Our technological leadership and R&D capabilities are grounded in hands-on experience from cybercrime investigations and cybersecurity incident response around the world—all accumulated through our cutting-edge forensic laboratory and 24/7 CERT team.

Group-IB's deep knowledge base, combined with the talent of our engineers and developers, has evolved into a suite of software solutions that offer a holistic approach to fighting cybercrime and fraud.

We have zero tolerance for the development or use of cyberweapons or any form of criminal activity. While some companies may choose to hire talented former black hat hackers, that is not the case at Group-IB. We do not employ individuals with a criminal background. Instead, we hire cybersecurity professionals with deep expertise who are ethical, white-hat experts—and only after they pass rigorous, multi-layered background checks.

The same high standards for integrity and compliance apply to our partners, clients, and suppliers. When a new client approaches us, our Security team conducts thorough checks against multiple criteria to ensure they are legitimate and trustworthy.

Integrity and honesty toward colleagues, clients, partners, and investors are non-negotiable. You must first be honest with yourself—only then can you truly be honest with others. Respect, personal responsibility, and teamwork are essential to who we are and how we work.

05 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 correlate with Group-IB mission?
- 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 of these questions, the course of action is likely the right one. But if you're uncertain about any of the answers, take it as a sign to seek guidance.

When in doubt, always ask before you act.

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

No Code—including ours—can anticipate every situation you may encounter at work.

If you can't find an answer here or have questions about how to interpret the Code, seek guidance.

Likewise, if you become aware of behavior that may violate this Code, the law, or any internal policy—or if you notice something suspicious—speak up and report it immediately so we can take appropriate action.

By reporting concerns, you help us address issues properly, resolve problems quickly, and prevent further harm.

You can report violations or share concerns by contacting:

- Your manager
- Your Chief Regional Officer (CRO)
- Your HR Business Partner (HRBP)
- Chief Security Officer
- The Legal team

Information on available reporting channels can be found in Section 30 of this Code.

07 Non-retaliation

We encourage our team to ask questions and raise concerns without fear of retaliation.
We are committed to treating all reports of violations seriously and investigating them thoroughly. Your help in preventing and uncovering potential misconduct is highly valued.

Group-IB does not tolerate retaliation against anyone who reports suspected misconduct or assists in an investigation or audit.

Raising a concern in good faith—even if it turns out to be unfounded—is always the right thing to do, and never a reason for any form of retaliation.

08 No false accusations

While we encourage honest reporting, we do not tolerate knowingly false reports. Deliberately making a false accusation can divert valuable resources, harm morale, and undermine credible concerns.

Always report your concerns in good faith—but never knowingly make a false claim, lie to investigators, or refuse to cooperate during an investigation.
Such actions may themselves constitute a violation of this Code.

09 Conflicts of interest

We are all expected to use sound judgment and act in the Company's best interests at all times.

This means avoiding conflicts of interest—or even situations that could appear as a conflict between personal interests and those of the Company. At Group-IB, we believe every business decision should be made objectively, with the Company's success as the top priority.

When considering a course of action, ask yourself:
Could this action create—or appear to create—an incentive that benefits me, my family, my friends, or an associated business at the Company's expense?
If the answer is yes, the situation likely constitutes a conflict of interest and should be avoided.

Even the appearance of a conflict can damage our reputation, reduce our effectiveness, and harm the team or the business as a whole.

Conflicts of interest can take many forms. Common examples include:

- Personal investments
- Outside employment or advisory roles
- Personal relationships that intersect with work responsibilities
- Accepting gifts, entertainment, or other business courtesies

What unites all these examples is a personal interest interfering with—or influencing—objective decision-making.

A simple rule applies:

- If you are considering entering into a business situation that creates a conflict of interest—don't.
- If you're already in a situation that may create an actual or perceived conflict—discuss it with your manager.

Keep in mind that circumstances change. A situation that once posed no risk may later become problematic. That's why it's important to proactively disclose any relationships, associations, or outside activities that could present actual, potential, or perceived conflicts of interest — to your manager, the Security team and HRBP. Failure to promptly disclose an actual or potential conflict of interest is itself a violation of this Code and may result in disciplinary action.

10 Personal investments

There are many companies you can invest in to strengthen your finances and build your portfolio. However, when choosing where to invest, you should avoid companies that are Group-IB's customers, business partners, or competitors—if the investment might create, or appear to create, a conflict of interest or cause you to act in a way that could harm the Company.

If you're unsure whether a company is considered a competitor, consult your manager or your Chief Regional Officer (CRO) before proceeding.

To determine whether a personal investment creates a conflict of interest, consider the relationship between the business of the company you want to invest in, Group-IB's business, and the nature of your role.

Ask yourself:

- Does the company have a business relationship with Group-IB that I can influence or guide?
- To what extent does the company compete with Group-IB?

In general, investments in venture capital funds or other funds that invest in a broad cross-section of companies—including potential competitors or business partners—typically do not create a conflict of interest on their own.

Likewise, owning publicly traded securities is generally not a concern. However, a conflict of interest may still arise if:

- You control or influence the fund's investment decisions, or
- You hold a majority stake (more than 25%) in a publicly traded company

In such cases, the appearance or reality of a conflict may exist, and you should disclose the investment and seek guidance.

11 Outside employment and advisory roles

Any commercial employment or entrepreneurial activity while being employed at Group-IB is strictly prohibited.

Non-commercial activities—such as education, research, scientific work, or charitable initiatives—may be permitted. However, you are expected to use sound judgment and ensure that such involvement does not conflict with Group-IB's interests or harm the Company's reputation in any way.

If you receive an offer to participate in any external activity and are unsure whether it complies with our policies, consult your manager and the Chief Security Officer before proceeding.

12 Personal relationships

You must not manage or make decisions about Group-IB's business relationships—whether current or potential—if they involve your relatives, spouse, significant other, or close friends.

For example, you cannot serve as the hiring manager for a role in which a close friend or family member is a candidate, or manage a company that is associated with your spouse or significant other.

That said, simply having a relative, partner, or friend who works at Group-IB—or who becomes a customer, business partner, or even a competitor—does not automatically create a conflict of interest. However, if you are involved in that business relationship on behalf of the Company, it becomes a sensitive matter.

In such cases, the right course of action is to proactively disclose the relationship to your manager and HR Business Partner (HRBP).

For the purposes of this Code, we define a “close personal relationship” as anyone who:

- Lives with you
- Is financially dependent on you
- Or on whom you are financially dependent

— regardless of whether a formal familial relationship exists.

13 Gifts, Entertainment, and Business Courtesies

At Group-IB, we recognize that modest gifts and reasonable hospitality can sometimes be a customary way to build professional relationships. However, they must never be offered or accepted to improperly influence a business decision or create a sense of obligation.

To ensure full compliance with anti-bribery laws and uphold Group-IB’s ethical standards:

- Never offer or accept gifts, entertainment, or hospitality that could be perceived as a bribe or as an attempt to influence someone’s decisions or actions.
- Gifts and hospitality must be reasonable in value, infrequent, and clearly not intended to secure any business advantage.
- Lavish, frequent, or poorly timed gifts—especially those offered before or during contract negotiations—are strictly prohibited.
- Cash, cash equivalents (such as gift cards), stocks, or other securities must never be given or received under any circumstances.
- Anything illegal, immoral, or damaging to your or Group-IB’s reputation must be avoided.
- Offers to government officials are subject to stricter rules and are generally prohibited—always consult the Legal or Compliance team in such cases.

General rule: Gifts like token non-cash items, occasional business meals, or local event invitations can be appropriate—as long as they are not excessive and do not create the appearance of impropriety.

Transparency is key: all employees must report gifts or hospitality exceeding the defined threshold at USD 50 to ensure proper oversight and transparency.

When in doubt, always check with your manager, the Legal team, or the Security team before giving or accepting anything of value.

You can learn more in Group-IB’s Anti-Bribery Policy.

14 Confidentiality

Information is one of Group-IB's most valuable assets, and we are committed to protecting it—whether it belongs to us or has been entrusted to us by others.

Confidential information exists in many formats: on paper, in digital documents, within IT systems, or embedded in applications. Our responsibility to protect this information applies regardless of the format. You must use confidential information strictly for business purposes and always maintain strict confidentiality.

This duty extends to third-party information entrusted to Group-IB—whether protected by a non-disclosure agreements (NDAs) or clearly understood to be confidential based on its nature, origin, or context.

As a team, we understand that protecting non-public information helps preserve our competitive advantage, reputation, and trust with clients and partners.

Examples of confidential information include (but are not limited to):

- Customer lists
- Proprietary data
- Financial and budget information
- Pricing strategies
- Business plans
- Trade secrets and know-how
- Product and software designs
- Inventions, processes, and engineering plans
- Employee data and internal reports

Confidential information must not be shared or discussed outside the Company, unless:

- A valid NDA is in place, or
- The information has been made public via an official press release, corporate statement, or communication from a senior manager or spokesperson

Internally, although open communication is encouraged, you should only share confidential information with team members who genuinely need it for their work. Use your best judgment to strike the right balance between collaboration and discretion.

We do not intend to interfere in day-to-day interactions, but we count on every team member to act responsibly and thoughtfully when sharing internal information.

Improper use or disclosure of confidential information can seriously harm Group-IB's reputation, damage business relationships, and expose the Company to legal and financial risks. Do your part to keep it safe.This includes forwarding confidential material via unauthorized platforms, uploading to personal drives, or discussing sensitive matters in insecure locations.

Your obligation to protect confidential information continues even after your employment or engagement with Group-IB ends.

If you are ever unsure about how to handle restricted or confidential information, contact the Legal team for guidance.

15 Privacy

At Group-IB, trust is the foundation of everything we do. Our clients, partners, and team members entrust us with their personal information—and we are committed to protecting that trust through the highest standards of privacy and security. We handle personal data in strict compliance with all applicable data protection laws of the countries where we operate. In addition, we implement the most rigorous global standards and best practices for data handling, regardless of location.

Group-IB respects the privacy rights of all individuals, whether the data belongs to those outside the Company or to our own team members. We collect, use, store and process personal data only for legitimate business purposes, and take all necessary measures to protect it from loss, misuse, or unauthorized access or disclosure.

When handling personal data, you must:

- Collect only data that is adequate, relevant, and limited to what is necessary
- Use the data solely for its specified and legitimate purpose
- Be transparent about the purpose and the intended use of data when obtaining consent or using any other processing basis
- Never share data with unauthorized persons outside Group-IB, or with anyone internally who does not have a legitimate need to know. Limit access to personal data strictly to those who need it to perform their job responsibilities
- Always maintain confidentiality and security
- Retain personal data only as long as necessary to achieve a declared business purpose or comply with legal requirements
- Continuously assess and minimize potential risks to individuals associated with the use or processing of their data
- Keep data accurate and up to date, correcting it without undue delay when mistakes are identified
- Respect data subject rights, including, without limitation, rights to access, correction, objection, erasure, and data portability, where applicable
- Ensure that third parties processing personal data on our behalf are subject to appropriate contractual obligations
- Apply appropriate security measures, including encryption, access controls, and anonymization or pseudonymization where required
- Report any actual or suspected data breaches or security incidents without delay by contacting privacy@group-ib.com

We expect every team member to act responsibly and ethically, and in line with our core values, when handling personal data.

If you suspect that personal data has been lost, stolen, or otherwise compromised, you must report it immediately to the Security team.

For any privacy-related inquiries or concerns, please immediately contact: privacy@group-ib.com

16 Governmental Customers

When working with customers affiliated with governments or state structures, Group-IB maintains strict engineering neutrality and independence.

The Company does not use any influence, mechanisms, connections, or contacts that could be provided by such customers for its own benefit.

17 Intellectual Property Rights

Be aware that if you create or develop anything for Group-IB as part of your job duties—including during work hours or while using the Company's resources—all such creations and developments belong to the Company.

This includes, but is not limited to:

- Developing new products
- Improving existing products
- Producing inventions, algorithms, or technical solutions
- Writing articles or reports
- Creating artwork or designs
- Any other form of intellectual property

All employees are expected to protect Group-IB's intellectual property (IP) rights in the course of their work. If you become aware of—or suspect—a violation of the Company's IP rights, or if you have any related questions, please contact the IP Management team immediately.

Use of Software and Open-Source Materials

Group-IB is committed to using only properly licensed software. You are not permitted to make or use illegal or unauthorized software copies, whether at work or at home. Doing so may result in copyright infringement, legal consequences for the Company, and damage to Group-IB's reputation as a leader in IP protection.

Additionally, if your work involves the use of open-source materials, you must:

- Obtain prior approval from the Company before incorporating any open-source components
- Ensure all use of open-source content complies with Group-IB's internal policies

If you have any questions or doubts about IP, software licensing, or open-source usage, seek guidance from the IP Management team.

18 Fair Play

At Group-IB, we compete with integrity and are committed to following all applicable antitrust and competition laws. We strive to outperform our competitors legally and ethically, within the framework of a free and fair market wherever we operate.

We aim to avoid even the appearance of unfairly restricting another company's ability to compete. For us, there is only one way to build market share and earn loyalty: by delivering best-in-class products and services.

Violations of competition laws can lead to severe consequences—including significant fines, legal costs, damage to our reputation, and broken commercial relationships. That's why we expect all team members to follow these principles:

Never:

- Enter into anti-competitive agreements—formal or informal, written or verbal
- Agree formally or informally to fix prices, coordinate bidding strategies, or divide up clients, markets, territories, or product lines
- Make inaccurate or misleading claims about a competitor's products or services
- Share commercially sensitive information with competitors unless specifically authorized by the Legal team
- Use improper or unethical means to obtain competitive intelligence
- Abuse a dominant market position
- Agree to unfair restrictions with distributors or clients
- Infringe on the confidentiality or intellectual property rights of competitors or third parties

Always:

- Compete honestly and fairly
- Win business through value, trust, and performance
- Treat clients, partners, and even competitors with respect
- Make only accurate, substantiated claims about our products and services
- Reach out to your manager or the Legal team if you're unsure whether a business practice complies with competition laws

We're proud of our technological leadership, deep expertise, and reputation. We believe we have everything it takes to win fairly—and we're committed to doing exactly that.

19

Insider Trading

At Group-IB, we often share and discuss sensitive business information—including non-public information—as part of our day-to-day work. You might also overhear a hallway or phone conversation, or come across internal documents that contain confidential data.

Using non-public information to buy or sell securities—or passing it along to others for that purpose — is considered insider trading. This is illegal in many countries and can result in severe penalties, including hefty fines and imprisonment.

Employees must not use insider information to trade in the securities of any publicly traded company, nor may they encourage others to do so or share such information with anyone who is not authorized to receive it.

What Is Insider Information?

Insider information is material, non-public information that could influence a reasonable investor's decision to buy or sell securities. Examples include:

- Group-IB's or a partner's financial results or forecasts
- Information about a new major product or service
- Details of a cybersecurity incident
- Developments in litigation or regulatory matters
- Planned mergers, acquisitions, or strategic changes

Our Commitment

We comply fully with insider trading laws and believe that everyone should make investment decisions based on equal access to information. For that reason, we do not use, trade, or tip others off using insider information.

When in Doubt—Pause and Ask

If you are unsure whether the information you have is material or non-public, treat it as insider information and consult the Legal team before taking any action.
If you know or suspect a case of insider trading, you must report it immediately to the Security team.

20

Anti-Bribery and Facilitation Payments

Group-IB supports global efforts to fight corruption and strictly complies with all applicable anti-bribery laws. These laws apply to all businesses—and Group-IB is no exception. A violation can result in serious legal and financial consequences, and may cause significant damage to our reputation.

That’s why we follow one clear and simple rule: Never bribe anyone, at any time, for any reason.

Our success is built on the quality of our products and services, not on unethical or illegal behavior. To uphold our values of honesty, integrity, and accountability, we maintain a zero-tolerance policy toward all forms of bribery and corruption.

We never offer or accept anything of value—whether money, gifts, services, or favors—to:

- Win business
- Retain business
- Gain any kind of improper advantage

This applies whether the offer is made directly or indirectly, and regardless of local customs or practices.

You must:

- Comply with anti-bribery and anti-corruption laws in every country where you operate
- Never offer, promise, give, or accept anything of value to improperly influence someone’s decisions or actions

Even the appearance of bribery or unethical conduct can be damaging. If you are unsure whether something might cross the line, ask the Legal team and Security team before taking any action.

Likewise, if you become aware of any facts or suspicions related to corruption or unethical behavior within the company, it is your responsibility to report them to the Security team immediately. Early reporting helps prevent further harm, protects the organization’s integrity, and ensures that appropriate steps can be taken to investigate and address the issue in a timely and confidential manner.

21 Prevention of Money Laundering

Group-IB strictly complies with all laws prohibiting money laundering, illegal financing, and other forms of financial crime. We do not, under any circumstances, knowingly ignore or enable illegal activity.

That said, money laundering and related crimes are not always obvious. It’s critical that we work together to reduce our risk of exposure and speak up if anything seems suspicious.

To protect Group-IB’s reputation and avoid potential liability, we must avoid any association with criminal activity—even if it's carried out by others. Our policy is to perform due diligence and screening on all clients, partners, and suppliers to ensure they are reputable and operate legitimately.

Your Responsibilities

Be alert and proactive when reviewing financial transactions and business relationships. If something doesn’t look right—even if you’re unsure—report it to the Security team.

Potential warning signs (red flags) include:

- Large or unexplained cash payments
- Unusual fund transfers to or from foreign countries
- Business partners or clients who provide incomplete or inconsistent information
- Counterparties who resist documentation or recordkeeping requirements
- Transactions that don’t align with the nature of the business relationship

Always ensure that:

- You’re working with reputable counterparties
- Business is conducted for legitimate purposes
- All funds involved are lawful and properly documented

If you suspect or notice any activity that could be linked to money laundering or other illegal practices, speak up immediately.

22 External Communications Policy

Both traditional and social media offer valuable opportunities to promote Group-IB and expand our professional networks. However, they also come with risks. While we respect your right to use social media for personal and professional purposes, we expect all team members to communicate responsibly and use good judgment when doing so.

Representing Group-IB Online

If your profile identifies you as a Group-IB employee, be aware that your posts may be perceived as expert opinions, or as representation of Group-IB's official position—not just personal views. For this reason:

- Any public comments, posts, or other communications about business-related topics—including opinions that could be seen as professional expertise—must be coordinated with the Public Relations (PR) team before publishing.
- If you are not an official spokesperson but still mention your affiliation with Group-IB in your profile, include a disclaimer such as: "The views expressed here are my own and do not represent those of Group-IB."
- If your social media profile does not mention your affiliation with Group-IB but the company or its business is discussed, clearly state that your views are personal and you are not speaking on behalf of the Company.

Protecting Information and Conducting Yourself Professionally

You must never disclose any confidential, proprietary, or non-public information about:

- Group-IB
- Our customers or partners
- Suppliers
- Competitors

Additionally, you must not post or share any content that:

- Could be seen as threatening, harassing, or discriminatory
- Violates Group-IB's information policies
- Harms the Company's reputation or professional and business relationships

We expect the same level of responsibility from customers, suppliers, and business partners when referencing Group-IB in any public communications.

Interacting with Media and Speaking on Behalf of the Company

If you believe something you posted may have given the impression that you were speaking on behalf of Group-IB, it is important to immediately contact your manager and the PR team. They will help assess the situation and respond appropriately to minimize any potential impact.

Media Inquiries

Group-IB frequently appears in both traditional and digital media. As a result, it's not uncommon for journalists to reach out to our employees via phone, email, or social media.

Please remember: All media interactions must be handled through Group-IB's PR team.

If you're contacted directly by a journalist:

- Politely inform them that all press inquiries must go through the PR team
- Do not provide comments or statements on behalf of the Company
- If you receive a journalist’s contact details, forward them to the PR team as soon as possible

Only authorized Company spokespeople are permitted to communicate with the media.

If you are an authorized spokesperson but are asked a question outside your area of expertise, inform the journalist that you are not the appropriate contact for that topic and refer them to the PR team, who will direct them to the relevant expert.

If you are unsure about your answer, it is better to say nothing than to risk providing incorrect or misleading information.

Mentions of Group-IB by Third Parties

Any references to Group-IB made by customers, partners, or contractors—whether in traditional, digital, or social media—must be coordinated in advance with the PR team.

23 Political Contributions

Group-IB does not make political contributions or support any political party, candidate, or political initiative.

Employees are free to engage in political activities in a personal capacity, but such involvement must be strictly separate from their role at Group-IB.

You may not:

- Make political donations on behalf of the Company
- Use Group-IB’s name, resources, or branding in connection with any political cause or campaign
- Represent your personal political views as those of the Company

We respect your right to participate in political life—just remember to keep your political activities personal and independent of Group-IB.

24

Protection and Proper Use of Group-IB Assets

Group-IB's assets—including intellectual property, equipment, and technology—are essential to our success and must be used responsibly and with care.

Proper Use of Intellectual Property

Group-IB's intellectual property—including trademarks, copyrights, exclusive rights in works of authorship, trade secrets, patents, and other forms of IP—is among our most valuable assets.

It is essential to use these assets correctly. Unauthorized use can lead to the loss of rights or a significant reduction in their value. All employees must respect applicable intellectual property laws, including those governing copyright, trademarks, and fair use of brands.

You must never use the Company's logos, trademarks, or other protected materials for personal projects or business ventures without first obtaining approval from the IP Management team.

We strongly encourage everyone to report any suspected misuse of the Company's trademarks, logos, or other IP.

Respecting Third-Party Intellectual Property

Just as we protect our own IP, we are equally committed to respecting the intellectual property rights of others. Inappropriate use of third-party IP can expose both you and Group-IB to legal penalties and reputational damage.

If you plan to:

- Solicit, accept, or use proprietary information from a third party,
- Allow a third party to use Group-IB's proprietary materials,

You must first seek guidance from the IP Management team before taking any action.

Physical and Digital Assets

Group-IB provides a variety of tools and resources to help you perform your job effectively—including computers, mobile devices, software, office equipment, and communications platforms.

We expect you to:

- Use Company assets responsibly and in line with internal policies
- Never install unapproved or unlicensed software on Company equipment
- Never disable or bypass any security controls on Company devices
- Keep assets in good condition and avoid unreasonable use, damage, or waste
- Arrange for repair or replacement if an asset is damaged. Any damage, loss, or malfunction should be reported to the IT team immediately
- Company devices should be used exclusively for work purposes whenever possible

If you're ever unsure whether a certain use of Company assets is appropriate, ask your manager or your HR Business Partner (HRBP).

25 Respect and Equal Opportunity

At Group-IB, we believe that every person is a valued member of our team and should be treated with respect, dignity, honesty, and fairness.

We have zero tolerance for discrimination, harassment, bullying, or any form of abuse—whether verbal, physical, or visual. We expect all employees to respect the skills, cultures, and backgrounds of their colleagues and to foster a professional environment where everyone feels safe and supported.

All decisions—at every level—must be based on objective criteria, such as skills, qualifications, performance, and business needs. Personal characteristics should never be a factor.

Discrimination of any kind is prohibited, including—but not limited to—discrimination based on:

- Race or ethnicity
- Age
- Role or position
- Gender or gender identity
- Religion or beliefs
- Country of origin
- Sexual orientation
- Marital status or family responsibilities
- Disability
- Social background
- Political views

Speak Up

If you experience, witness, or suspect harassment or discrimination, we urge you to speak up immediately.

You can:

- Address the issue directly (if safe to do so)
- Report it to your manager, Chief Regional Officer (CRO), or HR Business Partner (HRBP)

Group-IB takes all reports seriously. We do not tolerate retaliation against anyone who raises concerns in good faith.

Together, we are responsible for creating a workplace where respect, inclusion, and fairness are the norm—not the exception.

26

Health, Safety, and Workplace Violence Policy

Group-IB is committed to conducting business in full compliance with all applicable health and safety regulations. We continuously strive to improve our health and safety policies, procedures, and practices to ensure a safe and healthy environment for all employees, contractors, and visitors.

All employees are expected to:

- Promptly report any workplace injuries, illnesses, hazardous conditions, or unsafe practices to their Chief Regional Officer (CRO) or HR Business Partner (HRBP)
- Follow all safety guidelines and take personal responsibility for maintaining a safe workplace

Zero Tolerance for Workplace Violence

We maintain a strict zero-tolerance policy for workplace violence. This includes:

- Any act or threat of violence, regardless of severity
- The possession of weapons of any kind on company premises, under any circumstances

If you become aware of any actual or potential violation of this policy—including threats, aggressive behavior, or the presence of weapons—you are required to report it immediately to the Security team.

27

Drugs and Alcohol Policy

Employees are strictly prohibited from using, being under the influence of, possessing, buying, or selling alcohol, drugs, or any intoxicating substances while at work.

Employees with a company-leased vehicle are not permitted to drive under the influence of alcohol, drugs, or impairing medication—whether during work or personal time. All other employees are also strongly advised not to drive under such influence, as it compromises safety.

Violations of this policy may result in disciplinary action, including suspension or dismissal. Serious breaches may lead to immediate termination.

If an employee is struggling with alcohol or drug dependency, Group-IB is committed to offering support, such as access to rehabilitation clinics or substance abuse programs. Support will be provided only if the employee:

- Acknowledges the issue
- Reports it voluntarily to the employer
- Actively participates in the rehabilitation process

If you need to report an issue related to drug or alcohol abuse, please contact the Chief Security Officer.

28 Conduct at Corporate Events

Corporate events and celebrations are an opportunity to connect with colleagues, build team spirit, and celebrate our shared achievements. While the atmosphere at such events may be more relaxed than in day-to-day work, all employees are expected to maintain respectful, professional, and inclusive behavior in line with Group-IB's values.

Please remember that corporate events are organized and overseen by the Internal Communications (IC) team. If you wish to initiate or propose an event, contact the IC team and your Chief Regional Officer (CRO) for approval and coordination.

It is not permitted to use office premises for personal gatherings or events. This ensures our workspaces remain safe, secure, and professional at all times.

29 Remote Work Regulation

To support flexibility while maintaining productivity, security, and professionalism, the following guidelines apply to all employees working remotely:

Working Hours & Availability

- Remote employees are expected to align their working hours with their designated time zones and team schedules, unless otherwise agreed upon with their manager.
- Core collaboration hours must be respected to support efficient teamwork, communication, and accountability.

Communication & Responsiveness

- Team members must remain reachable and responsive during working hours via approved communication platforms (e.g., Slack, email, Google Calendar).
- Use status indicators appropriately and inform your manager if you will be unavailable for an extended period.

Professional Conduct in Virtual Meetings

- The same standards of professionalism apply in virtual meetings as in in-person settings. This includes:
- Being on time and well-prepared
- Dressing appropriately when using video
- Participating from a quiet, distraction-free environment

Data Security & Confidentiality

Remote employees are required to follow all company security protocols when accessing systems or handling confidential data. This includes:

- Connecting only through secure, encrypted Wi-Fi networks
- Using a company-approved VPN at all times
- Ensuring devices used for work are:
  - Company-issued, whenever possible
  - Equipped with up-to-date antivirus software
  - Regularly updated with the latest OS and application patches
- Locking devices when unattended
- Using strong, unique passwords and enabling multi-factor authentication (MFA)
- Avoiding use of:
  - Public or shared computers
  - Unauthorized USB drives
  - Personal cloud storage for work files
- Never printing or storing confidential information on non-company-managed devices
- Conducting screen sharing and confidential discussions only in private, secure environments
- Reporting any suspected security incident, phishing attempt, or data breach immediately to the Security team for timely response and containment

By adhering to these guidelines, remote team members help maintain Group-IB's productivity, security, and integrity, regardless of location.

30 Reporting Channels

If you have any questions about this Code—or believe that it may have been violated—it's important that you speak up.

You have several options for raising concerns or seeking clarification:

- Discuss the issue directly with your manager
- Report your concern via email to: codeofconduct@group-ib.com. Please include the name of the relevant department in the subject line to ensure your message is directed appropriately.

All reports are taken seriously. Group-IB is committed to maintaining a culture of openness, accountability, and integrity—and your voice plays a key role in that.

Fight against cybercrime

GROUP-IB