



# ESR Group Limited

Stock Code: 1821

## Code of Conduct and Business Ethics

### 1. INTRODUCTION

- 1.1 ESR Group Limited and its subsidiaries (collectively, “**ESR**” or the “**Group**”) is firmly committed to conducting business with the highest integrity and in compliance with the letter and spirit of law. The Group is operating in a world where the rules that govern business conduct are more complex and demanding than ever. Violating any rules could have very serious consequences to ESR and personally to those violating the rules.
- 1.2 This Code of Conduct and Business Ethics (the “**Code**”) embodies the fundamental principles covers a wide range of business practices and procedures, and emphasizes and advances the principles of discipline, good conduct, professionalism, loyalty, integrity and cohesiveness that are critical to the success and well-being of ESR. All of ESR’s directors, officers and employees (the “**Employees**”) must conduct themselves accordingly and seek to avoid improper behaviour. The Group also expects that contractors, sub-contractors, consultants, agents, representatives and others performing work or services for or on behalf of ESR will comply with the relevant parts of the Code when performing such work or services.
- 1.3 If a law in your country conflicts with a policy in this Code, you must comply with the local law. However, should the Code being more stringent than the local law, it should be the Code taking the higher priority for compliance purpose. Employees are responsible for understanding the legal and policy requirements that apply to their jobs and to report any suspected violation of law or this Code to the local Compliance Officer or Group Compliance Officer.
- 1.4 All Employees are required to read and sign off the Code of Conduct and Business Ethics Attestation Form on an annual basis at the beginning of each calendar year or upon their joining of the Group in making sure that they understand their on-going obligations. The signing-off should be done electronically for more effective monitoring and record keeping purposes, and please refer to your local or group compliance for how to gain access to the relevant system.

### 2. BUSINESS INTEGRITY AND ETHICS

- 2.1 All Employees must
  - a) at all times perform their duties with honesty, faithfulness and fairness and ensure the avoidance of conflicts of interests or situation of undue influence;
  - b) abide by all applicable laws, rules and regulations and internal policies that apply to the business in all the countries which the Group operates; and
  - c) be committed to principles of good corporate governance which emphasize transparency, accountability and independence.

### **3. CONFLICTS OF INTEREST**

- 3.1 A “conflict of interest” is where personal interest conflicts with the interest of the Group, a situation which could affect a person’s ability to act objectively. A conflict of interest arises in any situation in which an individual is in a position to take advantage of his or her role for personal benefit, including the benefit of his or her family members (including spouse, parents or children) and friends.
- 3.2 Relating to third parties (supplier, contractor, or service provider) that the Group will engage and interact with, conflict of interest could potentially arise if Employees or their family members:
- a) have a direct or indirect ownership interest in these third parties;
  - b) holds a position as director, officer, legal representative or colleague of, or consultant to, these third parties; or
  - c) have a direct or indirect financial interest in these third parties as a lender, guarantor, borrower or otherwise.
- 3.3 A conflict of interest will undermine the values of good faith, fidelity, diligence and integrity in the performance of the duties and obligations as expected by the Group. You must therefore avoid conflicts of interest between your personal dealings and your duties and responsibilities in conducting the Group’s business.
- 3.4 Full disclosure and prior approval is required from department head, compliance and human resources departments for:
- a) any outside employment activity;
  - b) engaging any outside organization in which there is personal interest to undertake any service or work for the Group
  - c) giving an undue advantage to any outside third party dealing with the Group, whether or not that will result in personal gain, benefit or advantage
- 3.5 The granting of approval will be subject to Employees satisfying the Group that such activity will not interfere with or compromise the proper performance of their duties or the fulfilment of their obligations. Any approval granted may be withdrawn at any time at the sole discretion of the Group without the need for assigning any reason thereof. In such an event, the Group will be deemed fully indemnified by the Employees and will not be held liable for any repercussion arising from such decision to withdraw the approval so granted before.
- 3.6 Conflicts of interest and potential conflicts of interest which have been fully disclosed and which are formally permitted by the Group will not constitute violations of this Code.
- 3.7 Please refer to the Group’s **Conflicts of Interest (COI) Policy** for more details.

### **4. CORPORATE OPPORTUNITIES**

- 4.1 Employees are prohibited from taking opportunities that are obtained through the use of corporate property, information or his/her position. Employees may not use corporate property, information or position for personal gains and Employees may not compete with the Group.

## 5. COMPETITION AND FAIR DEALING

- 5.1 All Employees should respect the rights of and deal fairly with the Group's clients, suppliers and competitors. Employees should not take advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other illegal business practices.
- 5.2 To ensure activities and interactions with suppliers, customers, competitors, and government authorities reflect fair and proper business practices and in compliance with the laws and regulations governing competition laws of the country in which the Group operates.
- 5.3 The purpose of business entertainment and gifts is to create sound working relationships, not to gain unfair advantage with clients. No gift or entertainment should be offered, given, provided or accepted by any Group Employee unless it (1) is consistent with customary business practice, (2) is reasonable in value, (3) does not violate any laws, regulations or applicable policies of the other party.
- 5.4 Please refer to the respective travel and entertainment policy and procedures and the Group's "**Anti-Bribery & Anti-Corruption and the Handling of Gifts, Travel and Entertainment Policy**" for details.

## 6. CONFIDENTIALITY

- 6.1 All Employees must maintain the confidentiality of proprietary information entrusted to them by the Group or its clients. Proprietary information includes all non-public information that might be of use to competitors or harmful to the Group or its clients if disclosed. The obligation to preserve proprietary information continues even after employment ends as specifically described in the employment contract.
- 6.2 Upon the termination of employment, any information acquired by an Employee in the course of his/her service with the Group shall remain the property of the Group. The Employee shall return all such information and shall not take any copies of or make use of such information for any purpose whatsoever.

## 7. ANTI-BRIBERY AND CORRUPTION

- 7.1 The Group takes a **zero-tolerance** approach to bribery and corruption and is committed to acting professionally, fairly and with integrity in all its business dealings and relationships wherever it operates and implementing and enforcing effective systems to counter bribery.
- 7.2 All Employees are required to observe the following:
  - a) prohibited from, directly or indirectly, **soliciting, accepting or obtaining or agreeing to accept or attempting to obtain**, from any party for yourself or for any other party, any bribe or gratification as an inducement or a reward for doing or forbearing to do, or for having done or forborne to do, any act in relation to Group's affairs or business, or for showing favour or forbearing to show disfavour to any party in relation to Group's affairs or business;

- b) may not directly or indirectly **offer, promise or give** any bribe as an inducement or a reward for doing or forbearing to do, or for having done or forborne to do, any act in relation to Group's affairs or business, or for showing favour or forbearing to show disfavour to Group in relation to Group's affairs or business, whether in the form of a facilitation payment, kickback, donation, fee or any other form; and
- c) prohibited from, directly or indirectly, making or accepting **facilitation payments** to or from any person for yourself or for any other person subject to this Code. In general, facilitation payment means payments made to secure or expedite the performance by a person executing a routine or administrative duty or function.
- d) **political contribution** is not allowed.

7.3 The Group operates in various countries and from time to time subject to various laws and regulation for conducting business. The below being the jurisdictions with the relevant laws on anti-bribery and corruption that would have an impact to the Group when dealing with both **private** and **public** sectors.

- |                    |                      |                   |
|--------------------|----------------------|-------------------|
| • <b>Australia</b> | • <b>Japan</b>       | • <b>Thailand</b> |
| • <b>China</b>     | • <b>South Korea</b> | • <b>U.S.A.</b>   |
| • <b>India</b>     | • <b>Hong Kong</b>   | • <b>U.K.</b>     |
| • <b>Indonesia</b> | • <b>Singapore</b>   | • <b>Vietnam</b>  |

7.4 All Employees should refer to the Group's "**Anti-Bribery & Anti-Corruption and the Handling of Gifts, Travel & Entertainment Policy**" for further details.

## **8. MONEY LAUNDERING & TERRORIST FINANCING**

8.1 Safeguarding the Group from reputational, operational, and even financial risks by not linking any business and financial transactions in crimes related to money laundering and terrorist financing is a top priority for all Employees.

8.2 In general terms, **money laundering** is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the property can lose its criminal identity and appear legitimate, meaning that criminals can benefit from their crimes without the fear of being caught by tracing their property back to a crime.

8.3 The **financing of terrorism** is the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism. Terrorist financing differs from money laundering in that the source of funds can be legitimate such as charity donation.

8.4 Appropriate counterparty due diligence should be conducted to understand the business and background of the Group's prospective business counterparties and to determine the origin and destination of money, property, and services.

8.5 Taking an indifferent attitude or turning a blind eye to a transaction you know or have reasonable grounds to believe that crime proceeds or terrorist funds are involved may result in a conviction by respective local regulations. Failing to report knowledge or suspicion of crime

proceeds or terrorist property may even be treated as a **criminal offense** in jurisdictions where the Group operates.

- 8.6 Any suspicion of transactions related to the above must be reported to the local Compliance Officer or the Group's Compliance Officer if there is no such local function, and not to be investigated on your own.
- 8.7 All Employees should refer to the Group's "**Anti-Money Laundering & Counter-Terrorist Financing Policy**" for further details.

## **9. THIRD PARTY RISK MANAGEMENT**

- 9.1 Other than our own Employees, we rely on a vast network of third parties to deliver high-quality products or services to our Group, our customers, investors and other stakeholders. Those third parties may include vendors, construction contractors, property managers, property valuers, real estate agents, distributors, consultants, brokers, licensing representatives, lawyers, accountants, and other service providers that the Group has contractual relationship in doing business with them.
- 9.2 Our Group is responsible for performing due diligence on any third-party with whom we engage with by gathering information of them in order to choose the best relationship given the risks, costs and services available. Risk will be assessed by answering the questionnaires using the third-party risk due diligence platform the Group has subscribed or other means as designated by Group Compliance if the third-party risk due diligence platform is not available. No contractual agreement with a new third party can be signed without the third-party risk assessment been performed and approved by Compliance. Any monetary threshold limit set by the local office in the third-party onboarding procedures will require Group Compliance approval. Before the contractual agreement is signed, the department or person responsible in engaging the third-party is required to provide the approval evidence together with the contractual agreement's terms and conditions for Legal department's review and vetting and the approval evidence to finance department for payment arrangement.
- 9.3 The third-party should be made aware by the department or person responsible for the onboarding of such third-party that they understand and read our Code of Conduct & Business Ethics Policy and the Supplier's Code of Conduct Policy published in the corporate webpage.

## **10. INSIDER DEALING**

- 10.1 All Employees with inside information<sup>1</sup> with regard to the Group (if applicable) or another company, such as a customer, supplier, investor, or joint venture partner whose securities, equity or debt, are admitted to trading on a stock exchange or an organized securities market are not allowed to trade in these companies' securities or in financial instruments, the prices of which depend directly or indirectly on these companies' securities.

---

<sup>1</sup> **Inside information** is any specific information which is not public knowledge relating to ESR or such other issuer of insider securities, which, if it became publicly known, would likely have a significant effect on the price of the insider security. Such likelihood exists if a reasonable investor would view the information as likely to have an impact on the price of the security. It would also exist if a reasonable investor would take the information into account in making an investment decision.

- 10.2 All Employees are required to abide by all applicable laws on insider dealing, which generally is when you trade in shares or other securities while in possession of inside information or when you share such information with someone else who then trades in those shares or other securities.
- 10.3 Access to inside information should be administered under a **need-to-know basis**, i.e. when it is appropriate for the type and scope of the task in question. An **Insider List** is maintained by Group Compliance for the approval, monitoring and even possible investigation of Employee dealing in securities when the Group is in possession of inside information during the course of business. This will also include inside information related to ESR Shares.
- 10.4 Employees must not engage in any dealing in an issuer's securities, including ESR shares, if he or she is in the possession inside information about such issuer. If an employee acquires inside information or thinks he or she may have been passed with such information either inadvertently or otherwise, Group or local compliance personnel should be notified immediately for record and approval for monitoring purposes.
- 10.5 Pre-approval is required in the dealing of ESR securities, equity or debt, by submitting an **Employee Trading Approval Form** to Group Compliance or through the designated on-line compliance management platform. In the case of the ESR-REIT shares which is listed in the Singapore Stock Exchange and the ESR Kendall Square REIT listed in the Korea Stock Exchange, it is covered separately by respective local compliance policy to comply with local regulatory requirements for approval and monitoring purposes.
- 10.6 Group Compliance will from time to time circulate the "*Restricted Trading*" info to Employees on listed company(ies) in which the Group may have possession of inside information.
- 10.7 The insider dealing is covered in the Group's **Employee Trading and the Handling of Inside Information** policy and the respective disclosure requirement related to inside information handled in another Group policy named **Disclosure Controls and Procedures**.

## **11. PROTECTION AND USE OF GROUP INFORMATION AND ASSETS**

- 11.1 All Employees must protect the Group's information and assets, which shall be used for legitimate company purposes only.
- 11.2 Authorisation from the senior management is required prior to disclosure to any outside party or use for your own purpose for any confidential or proprietary information about the Group or third parties with which the Group has entered into a confidentiality agreement or has entered into any type of business relationship.
- 11.3 Confidential or proprietary information may include intellectual property such as personal data, customer information, trade secrets, copyrights, patent, business/marketing plans, designs, databases, records, and unpublished financial data and reports. Unauthorized use or distribution of this information is a violation of company policy and subject to disciplinary action.

## **12. CLEAN DESK POLICY**

12.1 The purpose for this Policy is to establish a culture of security and trust for all Employees and their participation and support will greatly protect both paper and electronic documentations that contain sensitive / confidential information about staff, investors, customers and vendors. Promulgation of a clean desk policy may assist in ensuring that both paper and electronic documentations of personal and sensitive/confidential data has the appropriate physical protection.

12.2 The following best practices are expected:

- a) printing of personal or sensitive or confidential data should be minimized as much as possible in reducing the opportunity for hard copy of personal data to be lost or stolen, as well as reduces the task of proper disposing of personal data.
- b) any printers that could be used for printing personal or sensitive/ confidential data should be in a physically controlled environment in which only people who are authorized for access to personal data have unescorted or unsupervised access. This addresses the risk of hard copy of personal data being removed from a printer before the person who printed it has the chance to pick it up.
- c) highly sensitive/confidential or personal data should only be printed on printers in tightly controlled environments, for example in a staff member's personal office or under access right setting. This typically addresses situations in which there is a low volume of printing, but the consequences of loss or disclosure of the personal data is high.
- d) printers or photocopiers that support secure printing, where passcode can be assigned to each print job and the printout would not be printed until the correct code is entered at the printers, should be promoted for printing for use where personal or sensitive data is to be printed.
- e) personal or sensitive/ confidential data printed on hard copies and stored in mass storage device such as portable USB drive should be stored in a locked container, e.g. file cabinet or desk drawer, when not in use.
- f) hard copies of personal or sensitive or confidential data should be properly destroyed, for example by a cross cut shredder, when no longer needed.
- g) always clear your workspace before leaving for longer periods of time, including lunch break.
- h) allocate time in your calendar to clear away your paperwork.
- i) screen lock your computer whenever you are away from your desk and lock away portable computing devices such as laptops or tablets.
- j) tidy your desk, lock your desk and file cabinets, and logoff or shut down the desktop computer at the end of the working day.

- k) passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- l) whiteboards containing sensitive or confidential or personal information should be erased.

### 13. DATA PROTECTION

13.1 A good data protection policy not only helps securing the confidentiality and safe keeping of the data, but also assist the followings:

- a) ensuring regulatory compliance
- b) protecting reputation
- c) preserving customer and Employee trust
- d) safeguarding information infrastructure and asset protection
- e) enhancing information value
- f) reducing risk of data loss or theft

13.2 Particular attention should be paid to those **high risk data**, which is any information that when lost can lead to significant contractual or legal liabilities; serious damage to the Group's image and reputation; or legal, financial, or business losses. Examples of high risk data may include:

- a) **Name and contact information:** name and initial in any combination, home address, home telephone number, email address, mobile telephone number, or date of birth.
- b) **Personal characteristic:** age, gender, marital status, nationality, sexual orientation, racial or ethnic origin, or religious beliefs.
- c) **Personal identifiable information:** government-issued identification number, mother's maiden name, driving license number, passport number, credit history, or criminal history.
- d) **Financial institution data:** credit card or ATM numbers, bank account numbers, PIN numbers, or security codes or access codes and passwords that permit access to financial accounts.
- e) **Employment related information:** salary, bonus, other compensation information, or background check information.

13.3 Many jurisdictions have specific regulations in place in the protection of **personal data** which can be defined as:

*"any data relating directly or indirectly to a natural person, from which it is possible and practical to ascertain the identity of the individual from the said data"*

13.4 In regards to personal data, restriction in cross-border data transfer and the mandatory breach notification to respective regulatory authority are the risks that may expose the Group to legal and compliance risks in which it operates. Advice should be obtained from the human resources or compliance departments if in doubt.

13.5 Personal data protection is underpinned by the below important principles.

- a) be processed fairly and lawfully
- b) be obtained only for specific lawful purposes



- c) be adequate, relevant and not excessive
- d) be accurate and kept up to date
- e) not be held for any longer than necessary
- f) processed in accordance with the rights of data subjects
- g) be protected in appropriate ways
- h) not be transferred cross-border unless it is allowed by laws

13.6 All Employees should protect the Group's data and in compliance with the applicable laws. Please refer to the **Information Security Policy** published by Group I.T..

#### **14. FINANCIAL AND BUSINESS REPORTING**

14.1 It is necessary for the Group to submit financial and/or annual business reports to the relevant governmental agencies in accurate and timely manner.

14.2 The management of ESR expects all Employees to take this responsibility very seriously.

14.3 The Group's policy is to comply with all financial reporting and accounting regulations applicable to each Group company. If any Employees has concerns regarding accounting or auditing matters, he or she should submit those concerns to the Chief Financial Officer ("CFO") or the local Compliance Officer or the Group Compliance Officer if there is no such local function.

#### **15. RECORD-KEEPING AND DISCLOSURES**

15.1 The Group requires accurate and timely recording and reporting of information in order to make responsible business decisions. All business expense accounts must be documented and recorded accurately in a timely manner.

15.2 All of the Group's books, records, accounts and financial statements must be maintained in reasonable detail for statutory and audit trails purposes; must accurately reflect the Group's transactions; and be in compliance with any applicable laws or regulations for disclosure, reporting and record retention purposes.

#### **16. DISCRIMINATION AND HARASSMENT**

16.1 The Group is committed to providing equal opportunity in all aspects of employment and will not tolerate any unlawful discrimination or harassment based on race, colour, religion, sex, age, disability or national origin.

16.2 The values of mutual respect by maintaining a workplace that is free of all forms of harassment, including verbal, physical, visual or sexual must be upheld.

#### **17. WORKPLACE SAFETY AND ENVIRONMENT**

17.1 The Group is committed to providing a safe and healthy workplace for all Employees working at its facilities and minimizing impact of its operations on the environment.

- 17.2 The misuse of impairing substances is strictly prohibited while Employees are conducting work activities within or outside the Group premises as it can not only impair the performance at work, but also can be a threat to health, safety and the environment. Such impairing substances may include, but are not limited to, any legal or illegal drugs, alcoholic beverages, legal psychoactive drugs obtained or used without legal prescription or any such similar substances.
- 17.3 The Group places a high priority on operation according to best business practice standards, with a well-governed development and management platform that incorporates strong consideration to our Environmental, Social and Governance (“**ESG**”) responsibilities. Within the sphere of influence, the Group will undertake initiatives to promote greater environmental responsibility and encourage the development and diffusion of environmentally friendly technologies and processes. Please refer to the Group’s **ESG Policy** for details.

## **18. SOCIAL MEDIA**

- 18.1 Social media is defined by the Group to include online platforms and applications that facilitate activities such as professional or social networking, posting commentary or opinions, and sharing pictures, audio, video, or other content. And social media forums can include blogs, social network (e.g. Facebook, Twitter, YouTube, LinkedIn, Instagram, Tumblr, WeChat, etc.), personal websites, and other media yet to be developed in a dynamic communications field.
- 18.2 The Group respects Employees’ rights to communicate and it is not the Group’s intention to interfere or limit such.
- 18.3 The following principles should be used when communicating in the social media:
- a) Be authentic and transparent
  - b) Be respectful and polite
  - c) Protect confidential and private information
  - d) Follow applicable rules and regulation
  - e) Use good judgement
  - f) Be accountable for your own actions
- 18.4 The following Do’s and Don’ts not meant to be exhaustive

### **Do’s**

- Review the terms of engagement of each platform you wish to participate in
- Engage in social media personally using your own name and not on behalf of the Group
- Remain truthful and accurate at all times
- Mention your affiliation to ESR, if relevant to the topic of conversation
- State that your views are your own using a disclosure statement, unless you are authorized otherwise
- Act online as you would with colleagues or customers

### **Don’ts**

- Use expletives
- Make disrespectful, defamatory or dishonest comments
- Share sensitive information about the Group, customers, suppliers, colleagues, or business partners

- Position yourself as an ESR representative unless you have expressly received the authorization to do so
- Create social media accounts for ESR without the prior consent of the dedicated community manager

## **19. REPORTING ILLEGAL OR UNETHICAL BEHAVIOR**

- 19.1 All Employees should consult and report actual or potential illegal or unethical conduct which could be illegal or violation of the Code to the local Compliance Officer or the Group Compliance Officer if there is no such local function.
- 19.2 Any retaliation against an Employee who raises an issue honestly is strictly prohibited and is a violation of the Code, but it is also a violation to knowingly make a false accusation. Honest reporting does not mean that you have to be right when a concern is raised, but the information that is provided must be accurate.
- 19.3 The Group will keep the whistle-blower's identity confidential, and he or she will be assured of fair treatment, including protection against unfair dismissal, victimisation or unwarranted disciplinary action. However, if an investigation leads to a possible criminal prosecution, it may become necessary for a whistle-blower to provide evidence or be interviewed by the relevant authorities. Please refer to the **Whistleblowing Report Form** and the reporting should be done electronically for more effective monitoring and record keeping purposes. Kindly refer to your local or group compliance for how to gain access to the relevant system. An email group [whistleblowing@esr.com](mailto:whistleblowing@esr.com) is also available for submission and reporting purpose.
- 19.4 A **Whistleblowing Policy** is maintained for public access in our Group's corporate webpage.

## **20. BREACH OF THE CODE AND DISCIPLINARY ACTION**

- 20.1 Employees who violate the principles in this Code will lead to disciplinary action, which could include summary dismissal. It should also note that the violations of this Code may also be subject to local laws and regulations for possible criminal offence and prosecution.

Updated on 13 July 2021.

## ESR Group Limited

股份代號：1821

# 行爲準則和商業道德規範

## 1. 引言

- 1.1 ESR Group Limited 及其子公司（統稱「**ESR**」或「**集團**」）堅定地致力於按照最高標準的誠信以及法律的字義與精神開展業務。集團在規範商業行爲的規則比以往更加複雜和苛刻的世界中營運。違反任何規則可能會給 ESR 以及違反規則的個人帶來非常嚴重的後果。
- 1.2 本《行爲準則和商業道德規範》（「**準則**」）包含涵蓋廣泛的商業慣例和規程的基本原則，強調和信奉對 ESR 成功和康樂關鍵的紀律、品行端正、敬業、忠誠、正直和凝聚原則。所有 ESR 董事、管理人員和員工（「**員工**」）必須相應行事，設法避免不當行爲。集團還期望承包商、分包商、顧問、代理商、代表以及爲 ESR 或代表 ESR 工作或服務的其他人在工作或服務時遵守準則的相關規定。
- 1.3 如果您所在國家/地區的法律與準則中的政策衝突，您必須遵守當地法律。但若準則比當地法律更嚴格，則在合規方面準則具有更高的優先考慮。員工有責任了解適用於其工作的法律和政策要求，並向當地合規官或集團合規官報告任何涉嫌違反法律或準則的行爲。
- 1.4 全體員工須在每個日曆年年初或加入集團時閱讀並簽署《行爲準則和商業道德規範證明表》，確保其理解其持續義務。爲有效地監督和保留記錄，應以電子方式完成簽發，請參閱您當地或集團的合規規定，了解如何訪問相關系統。

## 2. 商業誠信與道德規範

### 2.1 全體員工必須

- a) 始終誠實、忠誠和公平地履行職責，並確保避免利益衝突或不當影響的情況；
- b) 遵守適用於所有集團營運所在國家/地區業務的所有適用的法律法規、規章條例和內部政策；及
- c) 踐行強調透明、問責和獨立性的良好公司治理原則。

### 3. 利益衝突

- 3.1 「利益衝突」是指個人利益與集團利益相衝突的情況，這可能影響人們客觀行事的能力。在個人能够利用其職位謀取私人利益的任何情況下均將產生利益衝突，其中包括其家人（包括配偶、父母或子女）和朋友的利益。
- 3.2 就與集團往來和互動的第三方（供應商、承包商或服務供應商）而言，如果員工或其家人有下列情形，則可能形成利益衝突：
- a) 在這些第三方中擁有直接或間接的擁有者權益；
  - b) 擔任這些第三方的董事、管理人員、法定代表人或顧問，或者為其工作；或
  - c) 以貸款人、擔保人、借款人或其他身份在這些第三方擁有直接或間接的經濟利益。
- 3.3 在履行集團期望的職責和義務時，利益衝突將破壞誠信、忠誠、勤勉和正直的價值觀。因此，您必須避免您的個人交易與您在開展集團業務時的職責和責任之間的利益衝突。
- 3.4 下列行為須要向合規與人力資源部門的部門主管全面披露和獲取事先批准：
- a) 外部工作活動；
  - b) 聘請任何有個人利益的外部組織為集團提供任何服務或工作；
  - c) 向與集團往來的外部第三方提供不正當的利益（不論是否導致個人利益）。
- 3.5 授予批准的前提是員工使集團確於信相關活動不會干擾或損害其適當履行職責或義務。集團可依單方酌情權隨時收回授予的批准，毋須指明任何理由。在這種情況下，將視為員工為集團提供充分的賠償，並且集團概不承擔決定收回先前授予的批准產生的影響。
- 3.6 已充分披露且由集團正式准許的利益衝突和潛在的利益衝突不構成對準則的違反。
- 3.7 有關基金和資產管理職能，請參閱《利益衝突政策》。

### 4. 公司機會

- 4.1 禁止員工利用通過使用公司財產、信息或其職位獲得的機會。員工不得將公司財產、信息或職位用於私人利益，不得與集團競爭。

### 5. 競爭和公平交易

- 5.1 全體員工均應尊重集團的客戶、供應商與競爭對手的權利並與之公平交易。員工不得通過操縱、隱瞞、濫用特權信息、歪曲重要事實或者任何其他非法商業行為利用他人。

- 5.2 確保與供應商、客戶、競爭對手和政府機構的活動和互動反映公平和正當的商業慣例，並符合集團營運所在國家/地區競爭法所適用的法律和法規。
- 5.3 業務招待和禮品的目的是建立良好的工作關係，而不是從客戶獲得不正當優勢。禁止集團員工提議、贈予、提供或者收受禮品或業務招待，除非其：**(1)** 符合正常的商業慣例；**(2)** 其價值合理；**(3)** 不違反另一方的法律法規或相應政策。
- 5.4 請參閱相應的差旅與招待的政策和程序以及集團的《**反賄賂和反腐敗以及禮品、差旅和招待的應對政策**》了解詳情。

## 6. 保密

- 6.1 全體員工必須保持集團或其客戶託付的專有信息的機密性。專有信息包括在披露後可能對競爭對手有用或者損害集團或其客戶的所有非公開信息。僱傭合同中明確規定，保護專有信息的義務在終止受僱後仍然有效。
- 6.2 在終止受僱後，員工在為集團服務過程中獲取的信息應仍為集團財產。員工應歸還所有此類信息，不得出於任何目的加以複製或使用。

## 7. 反賄賂和反腐敗

- 7.1 集團對賄賂和腐敗採取**零容忍**態度，致力於在其所有業務往來和關係中以專業、公平和誠信的方式行事並實施和執行有效的反賄賂制度。
- 7.2 全體員工須遵守以下規定：
- a) 禁止直接或間接為自己或他人而向/從任何其他人**索取、收受或獲取，或者同意收受或試圖獲取**賄賂或酬金作為相關行為或不作為、已完成的相關作為或不作為、有關集團事務或業務的行為或者表示支持或不表示反對涉及集團事務或業務的任何人的誘因或獎勵；
  - b) 不得直接或間接**提議、承諾或提供**任何賄賂（不論是採用疏通費、回扣、捐贈、費用或其他形式）作為相關行為或不作為、已完成的相關作為或不作為、有關集團事務或業務的行為或者表示支持或不表示反對涉及集團事務或業務的任何人的誘因或獎勵；及
  - c) 禁止直接或間接為自己或受本準則約束的他人向/從任何人提供或收受**疏通費**。一般而言，疏通費是指為確保或加快承擔日常或行政職責或職能的人履職支付的款項。

7.3 集團在多個國家經營業務，營運業務時亦不時受各種法律及規例的約束。應對**私營**及**公共**部門時，若干司法管轄區擁有對本集團產生影響的反賄賂及反貪污相關法律，該等司法管轄區載列如下：

- 澳洲
- 中國
- 印度
- 印尼
- 日本
- 韓國
- 香港
- 新加坡
- 泰國
- 美國
- 英國
- 越南

7.4 全體員工應參閱《反賄賂和反腐敗以及禮品、差旅和招待應對政策》了解更多詳情。

## 8. 洗錢和恐怖分子資金籌集

8.1 切斷洗錢和恐怖分子資金籌集犯罪中的任何商業和金融交易聯繫，保護集團免受聲譽、營運甚至財務風險的影響是全體員工的首要任務。

8.2 一般而言，「**洗錢**」是指犯罪分子企圖隱瞞犯罪活動所得的真正來源和所有權的過程。如果洗錢成功，相關財產可以擺脫犯罪身份並顯得合法，這意味著犯罪分子可以犯罪中受益，而不必害怕因為財產被查出為犯罪所得而被抓獲。

8.3 **恐怖主義資金籌集**是指以任何形式為恐怖主義或者煽動、計劃或從事恐怖主義的人提供經濟支持。恐怖分子資金籌集與洗錢有所不同，這表現在其資金來源可以是合法的（例如慈善捐贈）。

8.4 為了解集團潛在業務對手方的業務和背景，確定資金、財產和服務的來源和目的地，應開展相應的對手方盡職調查。

8.5 對您知悉或有合理理由認為涉及犯罪所得或恐怖主義資金的交易採取漠不關心的態度或視而不見可能導致您在相應的地方規定下被定罪。未能報告對犯罪所得或恐怖分子財產的了解或懷疑在集團營運所在司法管轄區甚至可能被視為**刑事犯罪**。

8.6 必須向當地合規官或者（如無當地合規官）集團合規官報告對上述相關交易的懷疑，禁止自行調查。

8.7 所有員工應參閱本集團之《反洗錢及反恐怖分子資金籌集政策》，以了解更多詳情。

## 9. 第三方風險管理

- 9.1 除集團員工外，我們亦依靠龐大的第三方網絡為集團、客戶、投資者及其他持份者提供優質產品或服務。該等第三方可能包括供應商、承建商、物業經理、物業估值師、房地產代理、分銷商、顧問、經紀、授權代表、律師、會計師及因與集團有業務往來而有合約關係的其他服務供應商。
- 9.2 集團負責對有業務往來的任何第三方進行盡職審查，收集彼等資料，以便在考慮到風險、成本及可用服務的情況下選擇最佳合作方。倘並無可用的第三方風險盡職審查平台，集團將使用已認購的第三方風險盡職審查平台或集團合規部指定的其他方式，以回答問卷的形式評估風險。倘未經進行第三方風險評估且未經合規部批准，不得與新的第三方簽訂合約協議。當地辦事處在第三方入門程序中設定的任何金錢門檻，均須獲集團合規部批准。簽訂合約協議前，委聘第三方之部門或負責人員須提供批准證明及合約協議之條款及條件，供法務部審閱及審查，並向財務部提交批准證明以安排付款。
- 9.3 負責第三方入職的部門或負責人員應讓該第三方了解並閱讀我司網頁上發佈的《行為準則和商業道德規範》以及《供應商行為準則》。

## 10. 內幕交易

- 10.1 掌握有關集團（如適用）或其他企業（例如證券、股權或債務在股票交易所或有序證券市場交易的客戶、供應商、投資人或聯營夥伴）內幕消息<sup>1</sup>的全體員工不得買賣價格直接或間接取決於這些企業證券的企業證券或金融工具。
- 10.2 全體員工須遵守關於內幕交易的所有適用法律，這通常是指您在掌握內幕消息期間買賣股份或其他證券，或者您與他人分享內幕消息，然後由其買賣這些股份或其他證券。
- 10.3 內幕消息的訪問權限應以「**按需知密**」（即與相關任務的類型和範圍相稱）的方式管理。當集團在經營過程中擁有內幕消息時，集團合規部負責**內幕人員名單**的維護以及對員工證券交易的批准和監督，甚至還有潛在的調查。這同樣包括與 ESR 股份相關的內幕消息。

---

<sup>1</sup> 內幕消息是與ESR或內幕證券的發行人相關但並非公眾獲悉的具體信息，而如果公眾獲悉該等具體信息，將可能對內幕證券的價格構成重大影響。該可能性在於若一名合理的投資者認為該等信息可能對證券的價格有所影響，或一名合理的投資者會以該等信息作為投資決定的考慮。



- 10.4 如果員工掌握發行人的相關內幕消息，其不得參與交易該發行人證券（包括 ESR 股份）的任何交易。如果員工取得內部消息或者認為其可能無意中或另行收到此類信息，則其應立即通知集團或當地合規人員，以為監督目的進行記錄和批准。
- 10.5 在買賣ESR證券（股票或債務）之前，須向集團合規部或透過指定線上合規管理平台提交《員工交易審批表》。就於新加坡證券交易所上市的ESR-REIT股份及在韓國證券交易所上市的ESR Kendall Square REIT而言，該等股份分別受各自的當地合規政策所涵蓋，以遵守當地的審批和監管要求。
- 10.6 集團合規部將不時向員工分發關於集團可能掌握內幕消息的上市公司的《限制交易信息》。
- 10.7 內幕交易由集團《員工交易和內幕信息處理》政策規定，與處理內幕消息相關的相應披露要求由《披露控制和程序》集團政策規定。

## 11. 保護和使用集團信息與資產

- 11.1 全體員工必須保護集團的信息和資產，並只可將其用於正當的公司目的。
- 11.2 在向外部人士披露或為個人目的使用關於集團或者與集團訂立保密協議或建立任何類型的業務關係的第三方的機密或專有信息前，須獲得高級管理層授權。
- 11.3 機密或專有信息可能包括知識產權（例如個人數據、客戶信息、行業秘密、版權、專利、商業/營銷計劃、設計、數據庫、記錄）以及未發佈的財務數據和報告。未經授權使用或分發此類信息將違反公司政策並面臨紀律處分。

## 12. 桌面整潔政策

- 12.1 該政策旨在為全體員工建立安全和信任的文化。員工的參與和支持將極大地保護包含關於員工、投資者、客戶和供應商的敏感/機密信息的紙質和電子文檔。頒佈桌面整潔政策可能有助於確保個人和敏感/機密數據的紙質和電子文件獲得適當的實體防護。
- 12.2 應遵循下列最佳做法：
- a) 應盡可能減少打印個人、敏感或機密數據，以減少個人數據的硬拷貝丟失或被盜的機會，並減少妥善處理個人數據的任務。
  - b) 可用於打印個人或敏感/機密數據的打印機應放置有實體控制措施的環境中，只有經授權訪問個人數據的人士可以進行無陪同或無監督的訪問。這解決了他人打印人

之前從打印機上取走個人數據硬拷貝的風險。

- c) 高度敏感/機密或個人數據只可在位於有嚴格控制措施的環境中的打印機上打印，例如在工作人員的個人辦公室或存在訪問權限設置的情況。這通常解決了打印量低但丟失或泄露個人數據的後果很嚴重的情況。
- d) 在需要打印個人或敏感數據時，應推廣使用支持安全打印（可為每次打印任務分配密碼，並且在向打印機中輸入正確密碼前無法打印資料）的打印機或影印機。
- e) 不使用時，打印在硬拷貝上並存儲在大容量存儲設備（例如便携式 USB 驅動器）中的個人或敏感/機密數據應存放在上鎖的空間中，例如文件櫃或書桌抽屜。
- f) 不再需要時，應妥善銷毀個人、敏感或機密數據的硬拷貝，例如使用十字粉碎機銷毀。
- g) 在離開較長時間（包括午餐休息）之前，請務必清理工作區。
- h) 在您的日程中安排整理文件的時間。
- i) 當您離開辦公桌時，鎖定計算機屏幕並鎖住便携式電腦設備（例如筆記本電腦或平板電腦）。
- j) 整理桌面，將辦公桌和文件櫃上鎖，並在工作日結束時注銷或關閉桌上型電腦。
- k) 不得在電腦上下張貼的便箋上保存密碼，也不得保存在可以訪問的位置。
- l) 應擦除白板上的敏感、機密或個人信息。

### 13. 數據保護

13.1 良好的數據保護政策不僅有助於確保數據的機密性和安全保管，還有助於：

- a) 確保監管合規
- b) 保護聲譽
- c) 保持客戶和員工信任
- d) 保護信息基礎設施和資產
- e) 提升信息價值
- f) 降低數據丟失或被盜的風險

13.2 應特別注意那些**高風險數據**，此類數據在丟失後能夠導致重大的合同或法律責任，嚴重影響集團形象和聲譽，或者法律、經濟或業務方面的損失。高風險數據的示例可能包括：

- a) **姓名和聯繫信息**：姓名和首字母的任意組合、家庭住址、家庭電話號碼、電子郵件地址、手機號碼或出生日期。
- b) **個人特徵**：年齡、性別、婚姻狀況、國籍、性取向、種族或民族血統或者宗教信仰。

- c) **個人身份信息**：政府頒發的身份證號碼、母親婚前姓名、駕駛執照號碼、護照號碼、信用記錄或犯罪記錄。
- d) **金融機構數據**：能夠用於查閱財務賬戶的信用卡或ATM號碼、銀行賬號、個人識別碼、安全碼、訪問代碼和密碼。
- e) **工作相關信息**：工資、獎金、其他酬金信息或者背景調查信息。

13.3 許多司法管轄區有保護**個人數據**的具體規定，這是指：

*“直接或涉及自然人的，可能據此查明該自然人身份且查明可行的數據”*

13.4 就個人數據而言，跨境數據轉移的限制以及向各監管機構發送強制性違規通知是可能使集團面臨經營方面的法律與合規風險。如有疑問，應從人力資源部門或合規部門獲取建議。

13.5 個人數據保護由以下重要原則為基礎。

- a) 公平合法地處理
- b) 只可出於特定的合法目的獲取
- c) 足夠、相關且不過度
- d) 準確、保持更新
- e) 不超過必要時間保存
- f) 按照數據主體的權利處理
- g) 以適當方式保護
- h) (除法律許可外) 禁止跨境轉移

13.6 全體員工均應保護集團的數據並遵守適用法律。請參閱集團信息科技部發佈的《**信息安全政策**》。

## 14. 財務和業務報告

14.1 集團有必要準確及時地向相關政府機構提交財務和/或年度業務報告。

14.2 ESR 管理層希望全體員工高度重視這項責任。

14.3 遵守適用於各集團公司的所有財務報告和會計法規是集團的政策。如果任何員工對會計或審計事項有疑慮，其應將相關疑慮提交給首席財務官、當地合規官或（如無當地合規官）集團合規官。

## 15. 記錄保存和披露

- 15.1 集團要求準確及時地記錄和報告信息，以便做出負責任的商業決策。必須及時準確地記載和記錄所有業務費用帳目。
- 15.2 集團的所有帳簿、記錄、帳目和財務報表必須根據法定和審計線索目的以合理的詳情維護，必須準確反映集團的交易，並符合關於披露、報告和記錄保留目的的任何適用法律法規。

## 16. 歧視與騷擾

- 16.1 集團致力於在勞動的各個方面提供平等機會，不容忍任何基於種族、膚色、宗教、性別、年齡、殘疾或國籍的非法歧視或騷擾。
- 16.2 必須通過維護無任何形式（包括口頭、肢體、視覺或性形式）騷擾的工作場所來維護互相尊重的價值觀。

## 17. 工作場所安全與環境

- 17.1 集團致力為在其設施工作的全體員工提供安全健康的工作環境，儘量減少集團營運對環境的影響。
- 17.2 嚴禁員工在集團內部或外部工作時濫用有害物質，因為這不僅影響工作表現，還可能威脅健康、安全和環境。這些有害物質可包括但不限於任何合法或非法藥物、酒精飲料、在沒有合法處方情況下取得或使用的合法精神類藥物或者任何類似的物質。
- 17.3 集團對根據最佳商業慣例標準營運高度重視，並具有充分考慮了我們環境、社會及管治（「ESG」）責任的良好規範的發展與管理平台。集團將在影響力的範圍內採取措施推進更大的環境責任，並建議開發和推廣環保技術與工藝。請參閱集團ESG政策了解詳情。

## 18. 社交媒體

- 18.1 集團對社交媒體的定義包括方便專業或社會交往、發佈評論或意見以及分享圖片、音頻、視頻或其他內容等活動的在線平台和應用程式。社交媒體論壇可以包括博客、社交網絡（例如Facebook、Twitter、YouTube、LinkedIn、Instagram、Tumblr及微信等）、個人網站以及動態通信領域有待開發的其他媒體。
- 18.2 集團尊重員工的通信權利，無意加以干預或限制。

18.3 在社交媒體上交流時，應遵循以下原則：

- a) 保持真實和透明
- b) 保持尊重和禮貌
- c) 保護機密和私人信息
- d) 遵守相應的規則和規定
- e) 善用判斷力
- f) 對自己的行為負責

18.4 下列的可以做和不可以做事項並非窮盡列舉。

#### 可以做

- 查看您有意參與的每個平台的參與條款
- 以個人方式並使用您自己的姓名而非代表集團參與社交媒體
- 始終保持真實和準確
- （如與對話主題相關）請提及您與 ESR 的關係
- 除非您另獲授權，否則請使用披露聲明表明您的觀點是自己的觀點
- 網上的行為方式同與同事或客戶的往來方式

#### 不可以做

- 咒罵
- 發表缺乏尊重、誹謗或不誠實的評論
- 分享關於集團、客戶、供應商、同事或業務合作夥伴的敏感信息
- 將自己定位為 ESR 代表（明確獲得相應授權除外）
- 未經專職社區經理事先同意，為 ESR 創建社交媒體賬戶

### 19. 舉報非法行為或不道德行為

19.1 全體員工應向當地合規官或（如無當地合規官）集團合規官諮詢和舉報實際或潛在的非法行為或者可能違法或違反準則的不道德行為。

19.2 嚴禁報復誠實提出問題的員工，報復是違反準則的行為，但故意虛假指控也是違規行為。誠實舉報不表示您在提出問題時必須正確，但提供的信息必須準確。

19.3 集團將對舉報人的身份保密，確保其獲得公平待遇，包括防止不正當解僱、受害或無根據的紀律處分。但若調查可能導致刑事起訴，則舉報人可能需要提供證據或者接受有關當局的訪談。請參閱舉報表。為有效地監督和保存記錄，應通過電子方式舉報。請參閱您當地或集團合規制度，了解如何登錄相關系統。還可使用電子郵件組 [whistleblowing@esr.com](mailto:whistleblowing@esr.com) 提交資料和舉報。

19.4 集團公司網頁上有舉報政策可供公眾使用。

## 20. 違反準則和紀律處分

20.1 違反準則原則的員工將受到紀律處分，其中可能包括立即解僱。還應注意，違反準則的行為也可能在當地法律法規下被視為犯罪並被起訴。

2021年7月13日更新



## ESR Group Limited

股份代号: 1821

# 行为准则和商业道德规范政策

## 1. 引言

- 1.1 ESR Group Limited 及其子公司（统称“ESR”或“集团”）坚定地致力于按照最高标准的诚信以及法律的字义与精神开展业务。集团在规范商业行为的规则比以往更加复杂和苛刻的世界中运营。违反任何规则可能会给 ESR 以及违反规则的规则的个人带来非常严重的后果。
- 1.2 本《行为准则和商业道德规范》（“准则”）包含涵盖广泛的商业惯例和规程的基本原则，强调和信奉对 ESR 成功和康乐关键的纪律、品行端正、敬业、忠诚、正直和凝聚原则。所有 ESR 董事、管理人员和员工（“员工”）必须相应行事，设法避免不当行为。集团还期望承包商、分包商、顾问、代理商、代表以及为 ESR 或代表 ESR 工作或服务的其他人在工作或提供服务时遵守准则的相关规定。
- 1.3 如果您所在国家/地区的法律与准则中的政策冲突，您必须遵守当地法律。但若准则比当地法律更严格，则在合规方面准则具有更高的优先考虑。员工有责任了解适用于其工作的法律和政策要求，并向当地合规官或集团合规官报告任何涉嫌违反法律或准则的行为。
- 1.4 全体员工须在每个日历年年初或加入集团时阅读并签署《行为准则和商业道德规范证明表》，确保其理解其持续义务。为有效地监督和保留记录，应以电子方式完成签发，请参阅您当地或集团的合规规定，了解如何访问相关系统。

## 2. 商业诚信与道德规范

### 2.1 全体员工必须

- a) 始终诚实、忠诚和公平地履行职责，并确保避免利益冲突或不当影响的情况；
- b) 遵守适用于所有集团运营所在国家/地区业务的所有适用的法律法规、规章条例和内部政策；及
- c) 践行强调透明、问责和独立性的良好公司治理原则。

### 3. 利益冲突

- 3.1 “利益冲突”是指个人利益与集团利益相冲突的情况，这可能影响人们客观行事的能力。在个人能够利用其职位谋取私人利益的任何情况下均将产生利益冲突，其中包括其家人（包括配偶、父母或子女）和朋友的利益。
- 3.2 就与集团往来和互动的第三方（供应商、承包商或服务提供商）而言，如果员工或其家人有下列情形，则可能形成利益冲突：
- a) 在这些第三方中拥有直接或间接的拥有者权益；
  - b) 担任这些第三方的董事、管理人员、法定代表人或顾问，或者为其工作；或
  - c) 以贷款人、担保人、借款人或其他身份在这些第三方拥有直接或间接的经济利益。
- 3.3 在履行集团期望的职责和义务时，利益冲突将破坏诚信、忠诚、勤勉和正直的价值观。因此，您必须避免您的个人交易与您在开展集团业务时的职责和责任之间的利益冲突。
- 3.4 下列行为须要合规与人力资源部门的部门主管全面披露和事先批准：
- a) 外部工作活动；
  - b) 聘请任何有个人利益的外部组织为集团提供任何服务或工作；
  - c) 向与集团往来的外部第三方提供不正当的利益（不论是否导致个人利益）。
- 3.5 授予批准的前提是员工使集团确信相关活动不会干扰或损害其适当履行职责或义务。集团可依单方酌情权随时收回授予的批准，毋须指明任何理由。在这种情况下，将视为员工为集团提供充分的赔偿，并且集团概不承担决定收回先前授予的批准产生的影响。
- 3.6 已充分披露且由集团正式准许的利益冲突和潜在的利益冲突不构成对准则的违反。
- 3.7 有关基金和资产管理职能，请参阅《利益冲突政策》。

### 4. 公司机会

- 4.1 禁止员工利用通过使用公司财产、信息或其职位获得的机会。员工不得将公司财产、信息或职位用于私人利益，不得与集团竞争。



## 5. 竞争和公平交易

- 5.1 全体员工均应尊重集团的客户、供应商与竞争对手的权利并与之公平交易。员工不得通过操纵、隐瞒、滥用特权信息、歪曲重要事实或者任何其他非法商业行为利用他人。
- 5.2 确保与供应商、客户、竞争对手和政府机构的活动和互动反映公平和正当的商业惯例，并符合集团运营所在国家/地区竞争法所适用的法律和法规。
- 5.3 业务招待和礼品的目的是建立良好的工作关系，而不是从客户获得不正当优势。禁止集团员工提议、赠与、提供或者收受礼品或业务招待，除非其：**(1)** 符合正常的商业惯例；**(2)** 其价值合理；**(3)** 不违反另一方的法律法规或相应政策。
- 5.4 请参阅相应的差旅与招待的政策和程序以及集团的《**反贿赂和反腐败以及礼品、差旅和招待的应对政策**》了解详情。

## 6. 保密

- 6.1 全体员工必须保持集团或其客户托付的专有信息的机密性。专有信息包括在披露后可能对竞争对手有用或者损害集团或其客户的所有非公开信息。劳动合同中明确规定，保护专有信息的义务在劳动关系终止后仍然有效。
- 6.2 在劳动关系终止后，员工在为集团服务过程中获取的信息应仍为集团财产。员工应归还所有此类信息，不得出于任何目的加以复制或使用的。

## 7. 反贿赂和反腐败

- 7.1 集团对贿赂和腐败采取**零容忍**态度，致力于在其所有业务往来和关系中以专业、公平和诚信的方式行事并实施和执行有效的反贿赂制度。
- 7.2 全体员工须遵守以下规定：
  - a) 禁止直接或间接为自己或他人而向/从任何其他人**索取、收受或获取，或者同意收受或试图获取**贿赂或酬金作为相关行为或不作为、已完成的相关作为或不作为、有关集团事务或业务的行为或者表示支持或不表示反对涉及集团事务或业务的任何人的诱因或奖励；
  - b) 不得直接或间接**提议、承诺或提供**任何贿赂（不论是采用疏通费、回扣、捐赠、费用或其他形式）作为相关行为或不作为、已完成的相关作为或不作为、有关集

团事务或业务的行为或者表示支持或不表示反对涉及集团事务或业务的任何人的诱因或奖励；及

- c) 禁止直接或间接为自己或受本准则约束的他人向/从任何人提供或收受**疏通费**。一般而言，疏通费是指为确保或加快承担日常或行政职责或职能的人履职支付的款项。

7.3 集团在不同的国家运营，开展业务过程中应不时遵守各种法律法规。以下是将对集团与私人 and 公共部门往来造成影响的关于反贿赂和反腐败的相关法律。

- |         |       |      |
|---------|-------|------|
| • 澳大利亚  | • 日本  | • 泰国 |
| • 中国    | • 韩国  | • 美国 |
| • 印度    | • 香港  | • 英国 |
| • 印度尼西亚 | • 新加坡 | • 越南 |

7.4 全体员工应参阅《反贿赂和反腐败以及礼品、差旅和招待应对政策》了解更多详情。

## 8. 洗钱和恐怖分子资金筹集

8.1 切断洗钱和恐怖分子资金筹集犯罪中的任何商业和金融交易联系，保护集团免受声誉、运营甚至财务风险的影响是全体员工的首要任务。

8.2 一般而言，“**洗钱**”是指犯罪分子企图隐瞒犯罪活动所得的真正来源和所有权的过程。如果洗钱成功，相关财产可以摆脱犯罪身份并显得合法，这意味着犯罪分子可以在犯罪中受益，而不必害怕因为财产被查出为犯罪所得而被抓获。

8.3 “**恐怖主义资金筹集资助**”是指以任何形式为恐怖主义或者煽动、计划或从事恐怖主义的人提供经济支持。恐怖分子资金筹集与洗钱有所不同，这表现在其资金来源可以是合法的（例如慈善捐赠）。

8.4 为了解集团潜在业务对手方的业务和背景，确定资金、财产和服务的来源和目的地，应开展相应的对手方尽职调查。

8.5 对您知悉或有合理理由认为涉及犯罪所得或恐怖主义资金的交易采取漠不关心的态度或视而不见可能导致您在相应的地方规定下被定罪。未能报告对犯罪所得或恐怖分子财产的了解或怀疑在集团运营所在司法管辖区甚至可能被视为**刑事犯罪**。

8.6 必须向当地合规官或者（如无当地合规官）集团合规官报告对上述相关交易的怀疑，禁止自行调查。

8.7 所有员工应查阅集团的《反洗钱和打击恐怖主义融资政策》，了解更多详情。

## 9. 第三方风险管理

9.1 除集团员工外，我们还依靠庞大的第三方网络向集团、客户、投资者和其他利益相关方提供高质量的产品或服务。这些第三方可能包括：供应商、建筑承包商、物业经理、物业估价师、房地产代理商、分销商、顾问、经纪人、许可代表、律师、会计师以及集团在与之进行业务往来时与之有合同关系的其他服务提供商。

9.2 我们的集团负责收集我们聘用的任何第三方的信息，对其进行尽职调查，以便根据风险、成本和服务选择最佳关系。将使用集团订阅的第三方风险尽职调查平台，或者，如果没有订阅第三方风险尽职调查平台，则采用集团合规部指定的其他方式回答调查问卷来评估风险。只有在已进行第三方风险评估且评估得到合规部批准的情况下，才能与新的第三方签署合同协议。当地办事处在第三方聘用程序中设定的任何金额门槛限额都需要得到集团合规部的批准。在签署合同协议之前，负责聘用第三方的部门或人员需要提供获批证明以及合同协议的条款和条件，供法务部审查，并向财务部提供获批证明，以便安排付款。

9.3 负责此类第三方聘用的部门或人员应告知此类第三方他们应理解并阅读我们公司网页上发布的《行为准则和商业道德规范政策》以及《供应商行为准则》。

## 10. 内幕交易

10.1 掌握有关集团（如适用）或其他企业（例如证券、股权或债务在股票交易所或有序证券市场交易的客户、供应商、投资人或联营伙伴）内幕信息<sup>1</sup>的全体员工不得买卖价格直接或间接取决于这些企业证券的企业证券或金融工具。

10.2 全体员工须遵守关于内幕交易的所有适用法律，这通常是指您在掌握内幕信息期间买卖股份或其他证券，或者您与他人分享内幕信息，然后由其买卖这些股份或其他证券。

10.3 内幕信息的访问权限应以“**按需知密**”（即与相关任务的类型和范围相称）的方式管理。当集团在经营过程中拥有内幕消息时，集团合规部负责**内幕人员名单**的维护以及对员工证券交易的批准和监督，甚至还有潜在的调查。这同样包括与**ESR**股份相关的内幕信

---

<sup>1</sup>内幕信息是与ESR或内幕证券的发行人相关但并非公众获悉的具体信息，而如果公众获悉该等具体信息，将可能对内幕证券的价格构成重大影响。该可能性在于若一名合理的投资者认为该等信息可能对证券的价格有所影响，或一名合理的投资者会以该等信息作为投资决定的考虑。

息。

- 10.4 如果员工掌握发行人的相关内幕信息，其不得参与交易该发行人证券（包括 ESR 股份）的任何交易。如果员工取得内部信息或者认为其可能无意中或另行收到此类信息，则其应立即通知集团或当地合规人员，以为监督目的进行记录和批准。
- 10.5 在交易 ESR 的证券（股票或债务）之前，需要事先得到批准，方式是向集团合规部提交或通过指定的在线合规管理平台提《员工交易审批表》。对于在新加坡证券交易所上市的 ESR-REIT 股票以及在韩国证券交易所上市的 ESR Kendall Square REIT，它们分别受各自当地的合规政策管辖，须分别遵守当地的审批和监督要求。
- 10.6 集团合规部将不时向员工分发关于集团可能掌握内幕消息的上市公司的《限制交易信息》。
- 10.7 内幕交易由集团《员工交易和内幕信息处理》政策规定，与处理内幕信息相关的相应披露要求由《披露控制和程序》集团政策规定。

## 11. 保护和使用权集团信息与资产

- 11.1 全体员工必须保护集团的信息和资产，并只可将其用于正当的公司目的。
- 11.2 在向外部人士披露或为个人目的使用关于集团或者与集团订立保密协议或建立任何类型的业务关系的第三方的机密或专有信息前，须获得高级管理层授权。
- 11.3 机密或专有信息可能包括知识产权（例如个人数据、客户信息、行业秘密、版权、专利、商业/营销计划、设计、数据库、记录）以及未发布的财务数据和报告。未经授权使用或分发此类信息将违反公司政策并面临纪律处分。

## 12. 桌面整洁政策

- 12.1 该政策旨在为全体员工建立安全和信任的文化。员工的参与和支持将极大地保护包含关于员工、投资者、客户和供应商的敏感/机密信息的纸质和电子文档。颁布桌面整洁政策可能有助于确保个人和敏感/机密数据的纸质和电子文件获得适当的实体防护。
- 12.2 应遵循下列最佳做法：
  - a) 尽可能减少打印个人、敏感或机密数据，以减少个人数据的硬拷贝丢失或被盗

的机会，并减少妥善处理个人数据的任务。

- b) 可用于打印个人或敏感/机密数据的打印机应放置有实体控制措施的环境中，只有经授权访问个人数据的人士可以进行无陪同或无监督的访问。这解决了他人打印之前从打印机上取走个人数据硬拷贝的风险。
- c) 高度敏感/机密或个人数据只可在位于有严格控制措施的环境中的打印机上打印，例如在工作人员的个人办公室或存在访问权限设置的情况。这通常解决了打印量低但丢失或泄露个人数据的后果很严重的情况。
- d) 在需要打印个人或敏感数据时，应推广使用支持安全打印（可为每次打印任务分配密码，并且在向打印机中输入正确密码前无法打印资料）的打印机或复印机。
- e) 不使用时，打印在硬拷贝上并存储在大容量存储设备（例如便携式 USB 驱动器）中的个人或敏感/机密数据应存放在上锁的空间中，例如文件柜或书桌抽屉。
- f) 不再需要时，应妥善销毁个人、敏感或机密数据的硬拷贝，例如用十字粉碎机销毁。
- g) 在离开较长时间（包括午餐休息）之前，请务必清理工作区。
- h) 在您的日程中安排整理文件的时间。
- i) 当您离开办公桌时锁定计算机屏幕并锁住便携式计算设备（例如笔记本电脑或平板电脑）。
- j) 整理桌面，将办公桌和文件柜上锁，并在工作日结束时注销或关闭台式计算机。
- k) 不得在计算机上下张贴的便签上保存密码，也不得保存在可以访问的位置。
- l) 应擦除白板上的敏感、机密或个人信息。

## 13. 数据保护

13.1 良好的数据保护政策不仅有助于确保数据的机密性和安全保管，还有助于：

- a) 确保监管合规
- b) 保护声誉
- c) 保持客户和员工信任
- d) 保护信息基础设施和资产
- e) 提升信息价值
- f) 降低数据丢失或被盗的风险

13.2 应特别注意那些**高风险数据**，此类数据在丢失后能够导致重大的合同或法律责任，严重影响集团形象和声誉，或者法律、经济或业务方面的损失。高风险数据的示例可能包括：

- a) **姓名和联系信息**：姓名和首字母的任意组合、家庭住址、家庭电话号码、电子邮件地址、手机号码或出生日期。
- b) **个人特征**：年龄、性别、婚姻状况、国籍、性取向、种族或民族血统或者宗教信仰。
- c) **个人身份信息**：政府颁发的身份证号码、母亲婚前姓名、驾驶执照号码、护照号码、信用记录或犯罪记录。
- d) **金融机构数据**：能够用于访问财务账户的信用卡或 ATM 号码、银行账号、个人识别码、安全码、访问代码和密码。
- e) **工作相关信息**：工资、奖金、其他酬金信息或者背景调查信息。

13.3 许多司法管辖区有保护**个人数据**的具体规定，这是指：

*“直接或涉及自然人的，可能据此查明该自然人身份且查明可行的数据”*

13.4 就个人数据而言，跨境数据转移的限制以及向各监管机构发送强制性违规通知是可能使集团面临经营方面的法律与合规风险。如有疑问，应从人力资源部门或合规部门获取建议。

13.5 个人数据保护由以下重要原则为基础。

- a) 公平合法地处理
- b) 只可出于特定的合法目的获取
- c) 足够、相关且不过度
- d) 准确、保持更新
- e) 不超过必要时间保存
- f) 按照数据主体的权利处理
- g) 以适当方式保护
- h) （除法律许可外）禁止跨境转移

13.6 全体员工均应保护集团的数据并遵守适用法律。请参阅集团信息科技部发布的《信息安全政策》。

## 14. 财务和业务报告

14.1 集团有必要准确及时地向相关政府机构提交财务和/或年度业务报告。

14.2 ESR 管理层希望全体员工高度重视这项责任。

14.3 遵守适用于各集团公司的所有财务报告和会计法规是集团的政策。如果任何员工对会计或审计事项有疑虑，其应将相关疑虑提交给首席财务官、当地合规官或（如无当地合规官）集团合规官。

## 15. 记录保存和披露

15.1 集团要求准确及时地记录和报告信息，以便做出负责任商业决策。必须及时准确地记载和记录所有业务费用账目。

15.2 集团的所有账簿、记录、账目和财务报表必须根据法定和审计线索目的以合理的详情维护，必须准确反映集团的交易，并符合关于披露、报告和记录保留目的的任何适用法律法规。

## 16. 歧视与骚扰

16.1 集团致力于在劳动的各个方面提供平等机会，不容忍任何基于种族、肤色、宗教、性别、年龄、残疾或国籍的非法歧视或骚扰。

16.2 必须通过维护无任何形式（包括口头、肢体、视觉或性形式）骚扰的工作场所来维护互相尊重的价值观。

## 17. 工作场所安全与环境

17.1 集团致力为在其设施工作的全体员工提供安全健康的工作环境，尽量减少集团运营对环境的影响。

17.2 严禁员工在集团内部或外部工作时滥用有害物质，因为这不仅影响工作表现，还可能威胁健康、安全与环境。这些有害物质可包括但不限于任何合法或非法药物、酒精饮料、在没有合法处方情况下取得或使用的合法精神类药物或者任何类似的物质。

17.3 集团对根据最佳商业惯例标准运营高度重视，并具有充分考虑了我们环境、社会及管治（“ESG”）责任的良好规范的发展与管理平台。集团将在影响力的范围内采取措施推进更大的环境责任，并建议开发和推广环保技术与工艺。请参阅集团ESG政策了解详情。

## 18. 社交媒体

18.1 集团对社交媒体的定义包括方便专业或社会交往、发布评论或意见以及分享图片、音频、视频或其他内容等活动的在线平台和应用程序。社交媒体论坛可以包括博客、社交网络

(例如 Facebook、Twitter、YouTube、LinkedIn、Instagram、Tumblr、微信等)、个人网站以及动态通信领域有待开发的其他媒体。

18.2 集团尊重员工的通信权利，无意加以干预或限制。

18.3 在社交媒体上交流时，应遵循以下原则：

- a) 保持真实和透明
- b) 保持尊重和礼貌
- c) 保护机密和私人信息
- d) 遵守相应的规则和规定
- e) 善用判断力
- f) 对自己的行为负责

18.4 下列的可以做和不可以做事项并非穷尽列举。

#### 可以做

- 查看您有意参与的每个平台的参与条款
- 以个人方式并使用您自己的姓名而非代表集团参与社交媒体
- 始终保持真实和准确
- (如与对话主题相关) 请提及您与 ESR 的关系
- 除非您另获授权，否则请使用披露声明表明您的观点是自己的观点
- 网上的行为方式同与同事或客户的往来方式

#### 不可以做

- 咒骂
- 发表缺乏尊重、诽谤或不诚实的评论
- 分享关于集团、客户、供应商、同事或业务合作伙伴的敏感信息
- 将自己定位为 ESR 代表 (明确获得相应授权除外)
- 未经专职社区经理事先同意，为 ESR 创建社交媒体账户

### **19. 举报非法行为或不道德行为**

19.1 全体员工应向当地合规官或 (如无当地合规官) 集团合规官咨询和举报实际或潜在的非法行为或者可能违法或违反准则的不道德行为。

19.2 严禁报复诚实提出问题的员工，报复是违反准则的行为，但故意虚假指控也是违规行为。诚实举报不表示您在提出问题时必须正确，但提供的信息必须准确。

19.3 集团将对举报人的身份保密，确保其获得公平待遇，包括防止不正当解雇、受害或无



根据的纪律处分。但若调查可能导致刑事起诉，则举报人可能需要提供证据或者接受有关当局的访谈。请参阅**举报表**。为有效地监督和保存记录，应通过电子方式举报。请参阅您当地或集团合规制度，了解如何登录相关系统。还可使用电子邮件组 [whistleblowing@esr.com](mailto:whistleblowing@esr.com) 提交资料和举报。

19.4 集团公司网页上有**举报政策**可供公众使用。

## 20. 违反准则和纪律处分

20.1 违反准则原则的员工将受到纪律处分，其中可能包括立即解雇。还应注意，违反准则的行为也可能在当地法律法规下被视为犯罪并被起诉。

2021年7月13日更新



## ESR Group Limited

証券コード：1821

### 行動倫理規範

#### 1. はじめに

- 1.1 ESR Group Limitedとその子会社（以下、総称して「**ESR**」または「**当グループ**」）は、最高の誠実さをもって、法令の文言と主旨に準拠して、真摯に事業の遂行に取り組んでいます。当グループが携わっている業界では、事業活動に適用される規則が以前よりも複雑化しており、要求が厳しくなっています。いずれかの規則に違反した場合には、ESRと違反者は極めて厳格な処分を受ける可能性があります。
- 1.2 この行動倫理規範（以下、「**本規範**」）は、様々な事業活動と手順に適用される基本原則を定めるとともに、ESRの成功と状態を測る基準となる規律、適切な行動、プロフェッショナリズム、忠誠、誠実さ、および結束の原則に着目し、これを発展させるものです。ESRのすべての取締役、役員、および従業員（以下、「**従業員**」）は、本規範に従って行動し、不適切な行動の回避に努めなければなりません。当グループはまた、業務やサービスをESRに提供したり、ESRに代わって業務やサービスを実施したりする請負業者、下請業者、顧問、代理業者、代行者などに対しても、業務やサービスの実施において本規範の関連部分を遵守するように求めています。
- 1.3 所在国の法令と本規範の方針が矛盾する場合は、地域の法令を遵守しなければなりません。ただし、本規範が現地法よりも厳格な場合は、コンプライアンスのために本規範を優先する必要があります。従業員は、自身の職務に適用される法的要件と方針上の要件を理解する責任を負うとともに、法令や本規範の違反が疑われる場合には、それを地域コンプライアンス担当者かグループコンプライアンス担当者に報告する責任を負います。
- 1.4 どの従業員も、当グループへの入社時、また年に一度、各暦年の初めに、自身が負っている義務を理解していることの確認として、行動倫理規範確認書を読み、これに署名することが求められます。この署名は、監視と記録保持を効率化するため、電子署名で行う必要があります。関連システムへのアクセス方法については、地域かグループのコンプライアンス担当者に問い合わせてください。

#### 2. 業務における誠実さと倫理

- 2.1 どの従業員も、以下を行うことが義務付けられています。
  - a) 常に、正直、実直、かつ公正に職務を遂行し、利益相反や不当威圧となる状況を避けなければなりません。
  - b) すべての適用法、規則、および規制、さらには当グループの事業展開国での業務に適用される内部方針を遵守しなければなりません。

- c) 透明性、説明責任、および独立を強調する適切な企業統治の原則を遵守しなくてはなりません。

### 3. 利益相反

- 3.1 「利益相反」とは、個人の利益が当グループの利益と一致せず、個人の客観的に行動する能力に影響を与える可能性がある状況を指します。利益相反は、個人が職務上の立場を利用して個人的な利益（配偶者、親、子といった家族や友人の利益を含む）を得られる状況で発生します。
- 3.2 当グループの委託先や取引相手となる第三者（サプライヤー、契約業者、サービス業者）に関して、従業員やその家族が次に該当する場合、利益相反が発生する可能性があります。
  - a) 第三者の直接的または間接的な持分権を保有している場合。
  - b) 第三者の取締役、役員、法定代理人、従業員、または顧問を務めている場合。
  - c) 貸借関係や保証・被保証関係など、第三者との間に直接的または間接的な金銭的利害関係がある場合。
- 3.3 利益相反は、当グループが求める職務遂行や義務履行における公正さ、忠誠、尽力、および誠実さを根底から揺るがすものです。したがって、従業員は、個人的な活動と当グループの事業活動における職務や責務との間に利益相反が生じないようにしなければなりません。
- 3.4 次に該当する場合は、部門責任者、コンプライアンス部門、および人事部門に届け出て、事前に承認を得なければなりません。
  - a) 副業を行う場合
  - b) 当グループへのサービスや業務の提供を、個人的な利害関係のある外部組織に委託する場合
  - c) 個人的な利得、利益、または便宜が生じるか否かにかかわらず、当グループと取引関係にある第三者に対し、必要以上の便宜を提供する場合
- 3.5 承認を得るには、当グループに対し、活動が適切な職務遂行や義務履行を妨げたり損なったりするものではないことを十分に説明しなければなりません。当グループは、理由を挙げることなく、以前に行った承認を独自の裁量でいつでも撤回することができます。その場合、当グループは、従業員から全面的に免責されたものとみなされ、以前に与えた承認を撤回するとの決定によるいかなる影響についても責任を負いません。
- 3.6 利益相反や潜在的利益相反を不備なく開示し、当グループが正式に容認した場合、その利益相反は本規範の違反とはみなされません。
- 3.7 詳細については、当グループの利益相反（COI）に関する方針を参照してください。

### 4. 会社の機会

- 4.1 従業員は、会社の資産、情報、または職務上の地位を通じて得た機会を利用することを禁止されています。従業員は、個人的利益のために会社の資産、情報、または職務上の地位を利用してはならず、また当グループと競争してはなりません。

## 5. 競争と公正取引

- 5.1 どの従業員も、当グループの顧客、サプライヤー、および競合他社の権利を尊重し、これらの者と公正に取引する必要があります。従業員は、部外秘情報の不正操作、隠蔽、濫用や、重要事実の不実表示といった違法なビジネス手法を用いて他者を利用してはなりません。
- 5.2 サプライヤー、顧客、競合他社、および政府当局との活動や取引が、公正かつ適切なビジネス手法を実践し、当グループの事業展開国の競争法に適用される法令と規制を遵守することを保証します。
- 5.3 業務上の接待や贈答品の授受は、良好な協業関係の構築を目的として行い、顧客との間で不当な便宜を獲得することを目的として行ってはなりません。当グループの従業員は、(1) 商慣習に沿っている場合、(2) 価値が妥当である場合、かつ (3) あらゆる法令や規制、さらには相手方の適用方針に反しない場合を除き、贈答品や接待の申し出、授与、提供、または受諾を行ってはなりません。
- 5.4 詳細については、各地域の出張や接待に関する方針や手順、および当グループの「**贈収賄防止および腐敗行為防止ならびに贈答品、出張および接待の取扱いに関する方針**」を参照してください。

## 6. 秘密保持

- 6.1 どの従業員も、当グループや顧客から預かった専有情報を秘密にしなければなりません。専有情報には、競合他社にとって有用となり得る非公開情報や、開示された場合に当グループや顧客が損害を被る可能性のある非公開情報などが該当します。専有情報を保護する義務は、雇用契約書に明記されている雇用期間の終了後も存続します。
- 6.2 雇用期間が終了しても、退職者が当グループでの業務や当グループとの協業で得た情報の所有権は当グループに帰属するものとします。退職者はこのような情報をすべて返却するものとし、目的の如何にかかわらず、コピーを作成したり情報を使用したりしてはなりません。

## 7. 贈収賄防止と腐敗行為防止

- 7.1 当グループは、贈収賄と腐敗行為に対して**ゼロトレランス**方式を採用しており、事業展開国のすべての商取引やビジネス関係において職業人らしい、公正かつ誠実な行動に努めるとともに、贈収賄への効果的な対策の導入と実施に取り組んでいます。
- 7.2 どの従業員も、以下を遵守することが求められます。
  - a) 当グループの業務や事業に関する今後や過去における行為の実施や不実施の働きかけやこれらに対する見返りとして、また当グループの業務や事業に関して何者かに対する支持を表明したり不支持の表明を控えたりすることの働きかけやこれらに対する見返りとして、自身や他者のために、何者かとの間で、直接的または間接的に賄賂や便宜の**勧誘、受領や獲得、または受領の同意や獲得の試み**を行うことが禁止されます。

- b) ファシリテーションペイメント、キックバック、寄付、手数料、その他形式の如何を問わず、当グループの業務や事業に関する今後や過去における行為の実施や不実施の働きかけやこれらに対する見返りとして、また当グループの業務や事業に関して当グループに対する支持を表明したり不支持の表明を控えたりすることの働きかけやこれらに対する見返りとして、直接的にも間接的にも、賄賂の**申し出、約束、または提供**を行ってはなりません。
- c) 自身やその他の本規範の適用対象者のために、何者かとの間で、直接的または間接的に**ファシリテーションペイメント**の支払いや承諾を行うことは禁止されています。一般に、ファシリテーションペイメントとは、日常や行政上の職務や事務の担当者による業務遂行の確保や期間短縮を目的として行われる支払いを意味します。
- d) **政治献金**は許可されていません。

7.3 当グループは様々な国で事業を行っており、場合によって、事業活動には様々な法令や規制が適用されます。次の法域では、**民間部門**や**公的部門**との取引において当グループに適用され得る贈収賄および腐敗行為防止に関する関連法を備えています。

- |           |          |        |
|-----------|----------|--------|
| • オーストラリア | • 日本     | • タイ   |
| • 中国      | • 韓国     | • 米国   |
| • インド     | • 香港     | • 英国   |
| • インドネシア  | • シンガポール | • ベトナム |

7.4 詳細については、当グループの「**贈収賄防止および腐敗行為防止ならびに贈答品、出張および接待の取扱いに関する方針**」を参照してください。

## 8. マネーロンダリングとテロ資金供与

- 8.1 どの従業員も、商取引や金融取引をマネーロンダリングやテロ資金供与に関する犯罪に関与させないことにより、社会的評価上のリスク、営業上のリスク、さらには財務上のリスクから当グループを保護することを最優先にすべきです。
- 8.2 一般に、**マネーロンダリング**とは、犯罪者が犯罪行為で得た収益の本当の出所や所有者を隠蔽しようとする手法を指します。これに成功した場合、資産から犯罪の痕跡が失われ、適法な資金に見せかけることができます。すなわち、犯罪者は、資産から犯罪行為を突き止められて逮捕される恐れなく、犯罪から収益を得ることができます。
- 8.3 **テロ資金供与**とは、形式の如何にかかわらず、テロリズムへの金銭的支援を行ったり、テロリズムの助長、計画、または参加を行っている者への金銭的支援を行ったりすることを指します。テロ資金供与がマネーロンダリングと異なるのは、慈善寄付など、資金源が適法である場合があることです。
- 8.4 当グループの取引先候補の事業と背景を理解し、資金、資産、およびサービスの出所や行き先を明確にするため、取引相手に対する適切なデューデリジェンスを実施する必要があります。
- 8.5 犯罪からの収益やテロ資金が関わっていることを知っている場合や、それを疑う合理的な根拠がある場合に、無関心な態度をとったり、見て見ぬふりをしたりすると、各地域の規制によって罰せられる可能性があります。当グループが事業を展開している法域で

は、犯罪収益やテロ資産の認識やその疑いを報告しないことは、**犯罪行為**とみなされる可能性があります。

- 8.6 上記に関する取引が疑われる場合は、地域コンプライアンス担当者かグループコンプライアンス担当者（地域に該当部門がない場合）に報告しなければならず、独自に調査を行ってはなりません。
- 8.7 詳細については、当グループの「**マネーロンダリング防止およびテロ資金供与防止に関する方針**」を参照してください。

## 9. 第三者リスク管理

- 9.1 当グループでは、高品質の製品やサービスを当グループ、顧客、投資家、およびその他の利害関係者に提供するため、従業員以外にも、幅広い第三者ネットワークに依拠しています。こうした第三者には、ベンダー、建設請負業者、資産管理者、資産評価人、不動産仲介業者、流通業者、顧問、ブローカー、正規代理店、弁護士、会計士、当グループと取引上の契約関係にあるその他のサービス業者などが該当します。
- 9.2 当グループは、リスク、コスト、および利用可能なサービスを考慮して最善の関係構築を実現するため、関与するすべての第三者の情報を収集してデューデリジェンスを実施する責任を負っています。リスク評価は、当グループが登録している第三者リスクのデューデリジェンスプラットフォームを用いた質問票への回答や、グループコンプライアンス部門が策定したその他の方法（第三者リスクのデューデリジェンスプラットフォームが利用できない場合）を使用して行います。第三者リスク評価を実施し、コンプライアンス部門からその承認を得ない限り、新たな第三者との契約上の合意に署名することはできません。現地オフィスが第三者のオンボーディング手順において金銭的な制限を設ける場合には、グループコンプライアンス部門の承認を得なければなりません。第三者との契約を担当する部門や個人は、契約上の合意に署名する前に、その合意条件とともに承認を得るための根拠を提出して法務部の審査と調査を受けなければならず、また支払いの取決めについて承認を得るための根拠を財務部門に提出しなければなりません。
- 9.3 第三者のオンボーディングを担当する部門や個人は、企業ウェブページに掲載されている行動倫理規範の方針とサプライヤー行動規範の方針を了解し、これを読むよう、第三者に伝える必要があります。

## 10. インサイダー取引

- 10.1 当グループに関する内部情報<sup>1</sup>（該当する場合）を保有している場合や、それ以外の企業（顧客、サプライヤー、投資家、合併事業の相手など）のうち証券取引所や制度証券市場でその証券、株式、または債券の取引が認められている企業に関する内部情報を保有している従業員は、そのような企業の証券や金融商品（価格が企業の証券に直接的または間接的に依存するもの）の取引が禁止されます。

---

<sup>1</sup> **内部情報**とは、ESRやそれ以外のインサイダー証券発行者に関する公知でない特定の情報で、公に知られた場合にそのインサイダー証券の価格が著しい影響を受ける可能性があるものを指します。一般的な投資家が証券の価格に影響を与える可能性があるともみならず場合、その情報は内部情報に該当する可能性があります。また、一般的な投資家が投資判断において考慮に入れると思われる場合、その情報も内部情報に該当する可能性があります。

- 10.2 どの従業員も、一般に、内部情報を保有しながら株式やその他の証券を取引する場合や、情報の受領後にその株式やその他の証券を取引すると思われる他者に内部情報を提供する場合、インサイダー取引に関するすべての適用法を遵守しなければなりません。
- 10.3 内部情報への接触は、**知る必要に基づいて**（つまり作業の種類や範囲に適しているかどうかによって）管理される必要があります。当グループが事業の過程で内部情報を保有する場合、証券を取引する従業員の承認、監視、さらには調査を行うため、グループコンプライアンス部門が**インサイダーリスト**を維持管理します。これには、ESR株式に関する内部情報も含まれます。
- 10.4 従業員は、証券発行者に関する内部情報を保有している場合、その発行者の証券（ESR株式を含む）を取引してはなりません。内部情報を入手した場合や、不注意等で内部情報が漏洩したと思われる場合には、監視のために記録や承認を行えるよう、グループか地域のコンプライアンス担当者に直ちに報告する必要があります。
- 10.5 ESRの証券、株式、または債券を取引する場合は、**従業員取引承認書**をグループコンプライアンス部門に提出するか、または所定のオンラインコンプライアンス管理プラットフォームを通じて、事前に承認を求める必要があります。ESR-REIT株式（シンガポール証券取引所上場）とESR Kendall Square REIT株式（韓国証券取引所上場）については、承認や監視に関する現地の規制要件に準拠するため、固有の地域コンプライアンス方針が別途適用されます。
- 10.6 グループコンプライアンス部門は、当グループが内部情報を保有している上場企業に関する「**制限取引**」情報を従業員に随時通知します。
- 10.7 インサイダー取引については、当グループの**従業員取引および内部情報の取扱い**に関する方針で定められており、また**開示統制および手順**という別のグループ方針で取り上げられる内部情報に関する個々の開示要件で定められています。

## 11. グループ情報と資産の保護と使用

- 11.1 どの従業員も、当グループの情報と資産を保護しなければならず、正当な会社の目的でのみ、これを使用しなければなりません。
- 11.2 当グループや当グループが秘密保持契約を締結していたり何らかの取引関係を結んでいたりする第三者に関する秘密情報や専有情報を社外の者に開示する場合や個人的な目的でこれを使用する場合は、上級管理者から事前に承認を得なければなりません。
- 11.3 秘密情報や専有情報には、個人データ、顧客情報、企業秘密、著作権、特許、事業計画やマーケティング計画、意匠、データベース、記録、未発表の財務データや財務報告書などの知的財産が含まれます。こうした情報の不正使用や頒布を行った場合は、会社方針の違反となり、懲戒処分の対象となります。

## 12. クリーンデスクポリシー

- 12.1 この方針は、全従業員にとって安全で信頼できる文化の確立を目的としており、全従業員が参加し、これに協力することで、職員、投資家、顧客、およびベンダーに関する機微情報や秘密情報が記載されている紙文書や電子文書を確実に保護することができま

す。クリーンデスクポリシーを周知することで、個人の紙文書と電子文書、さらには機微データと秘密データに対する適切な物理的保護の実現を促進することができます。

## 12.2 以下のベストプラクティスの実施が求められます。

- a) 個人データ、機微データ、または秘密データの印刷は、個人データが記載されたハードコピーの紛失や盗難を防止するため、さらには個人データを適切に廃棄処分する作業負担を減らすため、できるだけ最小限に抑える必要があります。
- b) 個人データ、機微データ、秘密データの印刷にあたっては、個人データへのアクセス権を付与されている者のみが付添人や監督者なしでアクセスできるようにするための物理的な制御下に置かれたプリンターを使用する必要があります。こうすることで、印刷者が個人データを含んだハードコピーをプリンターから取り出す前に他者に奪われるというリスクに対処することができます。
- c) 高度な機微性や秘密性を有するデータや個人データの場合は、職員の個人オフィスのプリンターやアクセス権の設定が施されたプリンターなど、厳重な制御下に置かれたプリンターでのみ印刷を行う必要があります。これは、通常、印刷量は少ないものの、その個人データを紛失したり開示されたりした場合の影響が甚大である場合の状況に対処する方法です。
- d) 個人データや機微データの印刷には、印刷ジョブごとにパスコードが発行され、プリンターに適切なコードを入力しない限り印刷を実行できない、安全な印刷をサポートするプリンターやコピー機の使用を奨励すべきです。
- e) 個人データ、機微データ、または秘密データが紙媒体に印刷されている場合や大容量記憶装置（ポータブルUSBドライブなど）に保存されている場合、そのハードコピーや大容量記憶装置を使用しないときは、施錠された収納場所（ファイルキャビネットやデスクの引き出しなど）に保管しておく必要があります。
- f) 個人データ、機微データ、または秘密データのハードコピーが不要になったときは、クロスカットシュレッダーなどを用いて適切に廃棄する必要があります。
- g) 昼休みなど長時間にわたって作業場所を離れるときは、必ず、作業場所の片付けを行ってください。
- h) 予定の中に書類を整理する時間を設けてください。
- i) デスクを離れるときは常にコンピューターのスクリーンをロックし、ノートパソコンやタブレットなどの携帯型コンピューターデバイスをロックしてください。
- j) 就業時間の終了時には、デスクを整理し、デスクとファイルキャビネットを施錠し、さらにデスクトップコンピューターのログオフかシャットダウンを行ってください。
- k) パスワードを付箋に書いてコンピューターの上や下に貼ったり、目に触れる場所にパスワードを書き留めたりしないでください。
- l) 機微情報、秘密情報、個人情報ホワイトボードに書いた場合は、それを消す必要があります。



## 13. データ保護

13.1 適切なデータ保護方針を用いることで、データの秘密性を保護し、データを安全に保管するだけでなく、次のような利点があります。

- a) 規制遵守の徹底
- b) 社会的評価の保護
- c) 顧客や従業員からの信頼の保護
- d) 情報インフラや情報資産の保護
- e) 情報価値の向上
- f) データの紛失や盗難のリスク軽減

13.2 **高リスクデータ**（紛失した場合に厳しい契約責任や法的責任、当グループの印象や社会的評価の深刻な毀損、または法律上、財務上、もしくは商業上の損失が生じる可能性のあるデータ）に対しては、特別な注意を払う必要があります。一例として、高リスクデータには次のようなものがあります。

- a) **氏名や連絡先情報**：氏名やイニシャルの組み合わせ、自宅の住所、自宅の電話番号、電子メールアドレス、携帯電話番号、生年月日など。
- b) **個人的特性**：年齢、性別、結婚歴、国籍、性的指向、人種や民族出自、宗教的信条など。
- c) **個人識別情報**：政府発行のID番号、母親の旧姓、運転免許証番号、パスポート番号、信用情報、犯罪歴など。
- d) **金融機関データ**：クレジットカード番号やATM番号、銀行口座番号、暗証番号、金融口座を利用するためのセキュリティコードやアクセスコードおよびパスワードなど。
- e) **従業員関連情報**：給与、賞与、その他の報酬情報、身元調査情報など。

13.3 多くの法域では、**個人データ**の保護に関する個別の規制が設けられています。個人データは、以下のように定義することができます。

*「自然人に直接的または間接的に関連するデータであって、個人を特定したり個人の特定に用いたりできるもの」*

13.4 個人データに関しては、データの越境移転の制限や各規制当局への違反の通知義務により、当グループが事業において法的リスクやコンプライアンス上のリスクに晒される可能性があります。不明点がある場合は、人事部門やコンプライアンス部門に相談してください。

13.5 個人データの保護については、以下の主要原則が基盤となります。

- a) 公正かつ合法的に処理すること
- b) 明確で合法的な目的でのみ取得すること
- c) 適度で関連があり、過度でないこと
- d) 正確であり、最新の状態を維持すること
- e) 必要な期間を超えて所持しないこと
- f) データ主体の権利に応じて処理すること

- g) 適切な方法で保護すること
- h) 法令で容認されていない限り、越境移転を行わないこと

13.6 どの従業員も、当グループのデータを保護し、適用法を遵守しなければなりません。当グループのI.T.部門が発行している**情報セキュリティに関する方針**を参照してください。

## 14. 財務報告と営業報告

14.1 当グループは、財務報告書または年次営業報告書（または、その両方）を適切な行政機関に不備なく適時に提出する必要があります。

14.2 ESR経営陣は、全従業員がこの責任を極めて真摯に捉えるように求めています。

14.3 当グループでは、各グループ企業に適用される財務報告や会計に関する規制をすべて遵守することを方針としています。会計や監査に関する事柄について懸念のある従業員は、最高財務責任者（以下「CFO」）または地域コンプライアンス担当者かグループコンプライアンス担当者（地域に該当部門がない場合）にその懸念を報告する必要があります。

## 15. 記録保持と開示

15.1 当グループは、責任のある業務上の意思決定を行うため、情報の記録と報告を正確かつ適時に行う義務を負っています。すべての必要経費の勘定を正確かつ適時に文書化し、これを記録しなければなりません。

15.2 当グループのすべての帳簿、記録、取引明細書、および財務報告書は、法定要件や監査証跡のために十分に詳しく残し、当グループの取引を正確に反映し、さらに開示、報告、および記録保持を趣旨とする適用法や規制に準拠したものでなければなりません。

## 16. 差別と嫌がらせ

16.1 当グループは、雇用のあらゆる面で機会均等に取り組み、人種、肌の色、宗教、性別、年齢、障害、または民族的出自による不当な差別や嫌がらせを許しません。

16.2 口頭、身体的、視覚的、または性的な嫌がらせなど、いかなる形態の嫌がらせもない職場を維持することにより、相互尊重という価値観を大切にしていかなければなりません。

## 17. 職場の安全と環境

17.1 当グループは、当グループの施設で働く全従業員にとって安全かつ健全な職場の提供に取り組むとともに、事業による環境への影響を最小限に抑える取り組みを行っています。

17.2 業務のパフォーマンスが損なわれるだけでなく、安全衛生や環境が脅かされる可能性があるため、当グループの施設内外での業務中に有害物質を乱用することは厳格に禁止されています。この有害物質には、合法または違法の薬物、アルコール飲料、正式な処方箋なく入手または使用される合法の向精神薬、これらに類似する物質などがあります。

- 17.3 当グループでは、環境、社会、およびガバナンス（「ESG」）に関する責任を十分に考慮し、適切な統制下にある開発および管理プラットフォームを用いた、業務に関するベストプラクティスに準拠した事業活動を最優先しています。当グループは、影響を与える領域において、環境への責任を高め、環境に配慮した技術とプロセスの開発と普及を奨励するイニシアチブに取り組みます。詳細については、当グループのESG方針を参照してください。

## 18. ソーシャルメディア

- 18.1 当グループの定義において、ソーシャルメディアには、プロフェッショナルネットワーキングやソーシャルネットワーキング、コメントや意見の投稿、写真、音声、動画などのコンテンツの共有といった活動を容易にするオンラインプラットフォームやアプリケーションなどが該当します。さらに、ソーシャルメディアフォーラムには、ブログ、ソーシャルネットワーク（Facebook、Twitter、YouTube、LinkedIn、Instagram、Tumblr、WeChatなど）、個人のウェブサイト、変化するコミュニケーション分野で今後開発されるその他のメディアなどが含まれます。
- 18.2 当グループはコミュニケーションを行う従業員の権利を尊重しており、そうした権利を妨害したり制限したりすることを意図していません。
- 18.3 ソーシャルメディアでのコミュニケーションにあたっては、以下の原則を守る必要があります。
- 自らを偽らず、透明性を保つこと
  - 敬意を払い、礼儀正しくすること
  - 秘密情報や個人情報を保護すること
  - 適用される規則や規制に従うこと
  - 分別を発揮すること
  - 自身の行動に責任を負うこと
- 18.4 以下の推奨事項と禁止事項は、すべてを網羅したものではありません。

### 推奨事項

- 参加を希望する各プラットフォームの利用規約を確認すること
- 自身の名前を使用して、当グループの代理ではなく、個人としてソーシャルメディアを利用すること
- 正直さと正確さを常に保つこと
- ESRに関連する話題では、自身とESRの関係を伝えること
- 特別な許可を得ない限り、情報開示声明によって自身の見解が個人的なものであることを明言すること
- オンラインでも、同僚や顧客と接するときのように振る舞うこと

### 禁止事項

- 罵り言葉を使用すること
- 失礼なコメント、中傷的なコメント、または不誠実なコメントをすること
- 当グループ、顧客、サプライヤー、従業員、またはビジネスパートナーに関する機微情報を共有すること
- ESRの代行者として振る舞うこと（明示的に許可を得ている場合を除く）
- 所定のコミュニティ管理者から事前に承諾を得ることなく、ESRのソーシャルメディアアカウントを作成すること

## 19. 違法行為や非倫理的行為の報告

- 19.1 どの従業員も、法令違反や本規範の違反となり得る違法行為や非倫理的行為がある場合やその可能性がある場合、地域コンプライアンス担当者かグループコンプライアンス担当者（地域に該当部門がない場合）に相談し、これを報告する必要があります。
- 19.2 正直に問題を報告した従業員への報復は厳格に禁止され、そのような報復行為は本規範の違反となります。ただし、故意に虚偽の告発を行うことも違反行為となります。正直な報告とは、懸念の報告時に誤りがあってはならないという意味ではありませんが、提供される情報は正確なものである必要があります。
- 19.3 当グループでは内部告発者の身元を秘密にし、不当解雇、迫害、不当な懲戒処分からの保護など、内部告発者を公正に扱うことを保証します。ただし、調査により刑事訴追の可能性が生じたときは、内部告発者による証拠の提出や関連当局との面談が必要になる場合があります。**内部告発報告書**を参照してください。また、監視と記録保持を効率化するため、報告は電子的手段で行う必要があります。関連システムへのアクセス方法については、地域やグループのコンプライアンス担当者に問い合わせてください。提出や報告には、電子メールグループの[whistleblowing@esr.com](mailto:whistleblowing@esr.com)も利用できます。
- 19.4 **内部告発に関する方針**が定められており、当グループの企業ウェブページで公開されています。

## 20. 本規範の違反と懲戒処分

- 20.1 本規範の原則に違反した従業員には、即時解雇を含む懲戒処分が課される可能性があります。また、本規範に違反した場合は、現地法や規制により、刑事犯罪に問われたり刑事訴追されたりする可能性があることに注意してください。

2021年7月13日に更新”

## ESR Group Limited

증권코드: 1821

### 행동 및 기업윤리 강령

#### 1. 소개

- 1.1 ESR Group Limited와 그 자회사들(총칭하여 이하 “**ESR**” 또는 “**그룹**”)은 높은 수준의 청렴성으로 법률의 규정 및 정신에 입각하여 사업을 영위하기 위해 최선을 다합니다. 그룹은 비즈니스 행동이 그 어느 때보다 복잡하고 까다로운 규칙의 적용을 받는 환경에서 사업을 운영하고 있습니다. 규칙 위반 시에는 매우 심각한 결과가 ESR과 위반 당사자 개인에게 초래될 수 있습니다.
- 1.2 본 행동 및 기업윤리 강령(이하 “**강령**”)은 광범위한 사업 관행과 절차들을 포괄하는 기본 원칙을 구체적으로 제시하는 한편, ESR의 성공과 안녕에 중요한 규율, 모범적 행동, 전문성, 충성심, 청렴성 및 화합의 원칙을 강조하고 촉진합니다. ESR에 소속된 모든 이사, 임원 및 직원(이하 “**임직원**”)은 이에 따라 행동하고 부적절한 행동을 피하고자 노력해야 합니다. 또한 그룹은 ESR을 위해 또는 이를 대신하여 업무나 서비스를 수행하는 계약자, 하청업자, 컨설턴트, 중개인, 대리인 및 기타 사람들이 그러한 업무나 서비스를 수행함에 있어 강령의 관련 규정을 준수할 것으로 기대합니다.
- 1.3 해당 국가의 법률이 본 강령상의 정책과 상충하는 경우에는 현지 법률을 준수해야 합니다. 그러나, 강령의 조항이 현지 법률보다 더 엄격할 경우, 규정준수 목적을 위해 강령이 더 높은 우선순위를 가집니다. 임직원은 본인의 업무에 적용되는 법률 및 정책 요건을 이해해야 하고, 법률 또는 본 강령의 위반 의심 사례를 현지 준법감시인 또는 그룹 준법감시인에게 보고해야 할 책임이 있습니다.
- 1.4 모든 임직원은 행동 및 기업윤리 강령 선서 양식을 읽어보고 이에 서명해야 하며, 이는 매년 초마다 연례적으로, 또는 본인의 의무가 지속됨을 이해했다는 전제 하에 그룹 입사 시점에 수행되어야 합니다. 서명은 보다 효과적인 모니터링 및 기록 보관을 위해 전자 방식으로 이루어지며, 관련 시스템에 액세스하는 방법은 현지 또는 그룹 규정준수 부서에 문의하시기 바랍니다.

#### 2. 비즈니스 청렴성 및 윤리

- 2.1 모든 임직원은 다음을 준수해야 합니다.
  - a) 맡은 바 직무를 항상 정직하고 성실하며 공정하게 수행하고, 이해 상충 또는 부당한 영향력이 행사되는 상황에 개입하는 것을 피합니다.
  - b) 그룹의 사업장이 있는 모든 국가에서 사업 활동에 적용되는 모든 해당 법률, 규칙, 규정, 내부 정책을 준수합니다.
  - c) 투명성, 책임성 및 독립성을 강조하는 바람직한 기업 거버넌스 원칙에 충실합니다.

### 3. 이해 상충

- 3.1 '이해 상충'이란 개인적 이해가 그룹의 이해와 충돌하는 경우로서, 개인의 객관적 행동 능력에 영향을 미칠 수 있는 상황을 의미합니다. 이해 상충은 자신의 가족 구성원(배우자, 부모 또는 자녀 포함) 및 친구의 이익을 비롯한 개인적 이익을 위해 본인의 직위를 이용할 수 있는 모든 상황에서 발생합니다.
- 3.2 그룹이 관여 및 교류하는 제3자(공급업체, 계약업체 또는 서비스 제공업체)와 관련하여, 임직원 또는 그 가족 구성원이 다음에 해당할 때 이해 상충이 발생할 수 있습니다.
- a) 이러한 제3자에 대한 직간접적인 소유지분이 있는 경우,
  - b) 이러한 제3자의 이사, 임원, 법률 대리인 또는 직원으로서, 또는 컨설턴트로서의 지위를 가진 경우, 또는
  - c) 이러한 제3자에 대한 대출자, 보증인, 차용인 등으로서 직간접적인 재정적 이해관계가 있는 경우 등.
- 3.3 이해 상충은 그룹이 기대하는 의무와 직무를 이행함에 있어 신의성실, 충실성, 성실성 및 청렴성의 가치를 훼손합니다. 따라서 그룹의 업무를 수행할 때는 본인의 직무 및 책임과 개인적인 거래 사이에서의 이해 충돌 상황을 피해야 합니다.
- 3.4 다음에 해당 시, 완전한 공개와 함께 부서장, 규정준수 및 인사 부서의 사전 승인이 필요합니다.
- a) 여하한 외부 취업 활동
  - b) 그룹의 서비스 또는 업무를 수행하기 위해 개인적 이해관계가 있는 외부 조직을 고용하는 행위
  - c) 개인적 이득, 혜택 또는 이익으로 이어지는지 여부에 관계없이, 그룹과 거래 관계에 있는 외부의 제3자에게 부당한 이익을 제공하는 행위
- 3.5 승인은 그러한 활동이 맡은 바 직무의 적절한 수행 또는 의무의 이행을 방해하거나 저해하지 않을 것임을 그룹이 만족할 만큼 입증한 임직원을 대상으로 부여됩니다. 부여된 모든 승인은 관련 사유를 제시하지 않은 채 그룹의 단독 재량에 따라 언제든지 철회될 수 있습니다. 그러한 경우, 그룹은 임직원에 의해 완전히 면책된 것으로 간주되며, 이전에 부여된 승인에 대한 해당 철회 결정으로 인해 발생하는 일체의 영향과 관련하여 책임을 지지 않습니다.
- 3.6 이해 상충 및 잠재적 이해 상충이 완전히 공개되었고 그룹이 이를 공식적으로 허용한 경우에는 본 강령의 위반에 해당하지 않습니다.
- 3.7 보다 자세한 내용은 그룹의 **이해 상충(Conflicts Of Interest, COI) 정책**을 참조하십시오.

### 4. 기업 기회

- 4.1 임직원이 회사 자산, 정보 또는 본인의 직위를 이용하여 획득하게 된 기회를 활용하는 것은 금지됩니다. 임직원은 개인적 이득을 위해 회사 자산, 정보 또는 직위를 이용할 수 없으며, 그룹과 경쟁하지 않습니다.

## 5. 경쟁 및 공정 거래

- 5.1 모든 임직원은 그룹의 고객, 공급업체 및 경쟁사가 가진 권리를 존중하고, 이들과 공정하게 거래해야 합니다. 임직원은 조작, 은폐, 특권적 정보의 남용, 중대 사실의 허위 진술, 또는 기타 불법적 사업 관행을 통해 누군가로부터 이익을 취해서는 안 됩니다.
- 5.2 이는 공급업체, 거래처, 경쟁사, 정부 당국과의 활동 및 교류가 공정하고 적절한 사업 관행을 반영하도록 하면서도 그룹의 사업장이 있는 국가의 경쟁법을 규율하는 법률 및 규정이 준수되도록 보장하기 위함입니다.
- 5.3 사업상 접대 및 선물의 목적은 고객을 상대로 불공정한 이익을 취하는 것이 아니라, 건전한 업무 관계를 형성하는 것입니다. 그룹의 임직원은 (1) 통상적인 사업 관행에 부합하고, (2) 가치가 합리적이며, (3) 여하한 법률, 규정 또는 상대방의 해당 정책에 대한 위반이 아닌 경우를 제외하고, 선물 또는 접대를 제안, 전달, 제공 또는 수락해서는 안 됩니다.
- 5.4 자세한 내용은 해당하는 여행 및 접대 정책/절차와 그룹의 '**뇌물수수 및 부패 방지와 선물, 여행 및 접대 취급 정책**'을 참조하십시오.

## 6. 기밀 유지

- 6.1 모든 임직원은 그룹 또는 그 고객이 본인에게 위탁한 독점 정보의 기밀성을 유지해야 합니다. 독점 정보에는 공개 시 경쟁사에 의해 활용되거나 그룹 또는 그 고객에게 해가 될 가능성이 있는 모든 미공개 정보가 포함됩니다. 독점 정보의 보존과 관련한 의무는 고용계약서상에 구체적으로 기술된 바와 같이 고용 종료 이후에도 계속됩니다.
- 6.2 고용 종료 시, 임직원이 그룹에 근무하는 과정에서 획득한 일체의 정보는 그룹의 자산으로 남게 됩니다. 임직원은 그러한 모든 정보를 반환해야 하며, 어떠한 종류의 목적으로도 그러한 정보의 사본을 만들거나 이를 활용해서는 안 됩니다.

## 7. 뇌물수수 및 부패 방지

- 7.1 그룹은 뇌물수수와 부패에 대해 **무관용** 접근법을 취하고 있으며, 사업 거래 및 관계가 진행되는 모든 곳에서 전문적이고 공정하며 청렴하게 행동하는 한편 뇌물수수의 효과적 근절을 위한 시스템을 시행하고 집행하기 위해 최선의 노력을 다합니다.
- 7.2 모든 임직원은 다음에 주의해야 합니다.
  - a) 그룹 업무나 사업과 관련하여 여하한 행위를 하거나 하지 않는 것, 또는 이를 이미 했거나 하지 않은 것, 또는 그룹 업무나 사업과 관련하여 특정 당사자에게 호의를 베풀거나 불리한 행위를 삼가는 것 등에 대한 유인책 또는 포상으로서 일체의 뇌물 또는 향응을 자신이나 다른 당사자에 제공하도록 여하한 당사자에게 직간접적으로 요청하거나, 이를 수락하거나, 획득하거나, 그 수락에 동의하거나, 획득을 시도하는 것은 금지됩니다.
  - b) 그룹 업무나 사업과 관련하여 여하한 행위를 하거나 하지 않는 것, 또는 이를 이미 했거나 하지 않은 것, 또는 그룹 업무나 사업과 관련하여 그룹에게 호의를 베풀거나 불리한 행위를 삼가는 것 등에 대한 유인책 또는 포상으로서 일체의(급행료,

리베이트, 기부, 수수료의 형태나 기타 형태로 된) 뇌물을 직간접적으로 제안, 약속 또는 전달할 수 없습니다.

c) 자신 또는 본 강령의 적용을 받는 다른 누군가를 위해 여하한 사람을 상대로 직간접적인 **급행료**를 지불하거나 제공받는 것은 금지됩니다. 일반적으로 급행료란 일상적/행정상 직무나 기능을 수행하는 사람의 업무 처리를 보장받거나 촉진하기 위해 지급하는 금액을 의미합니다.

d) **정치적 기부**는 허용되지 않습니다.

7.3 그룹은 다양한 국가에서 사업을 영위하며, 때때로 사업 수행과 관련된 다양한 법률과 규제에 직면합니다. 아래 목록은 **민간 부문 및 공공 부문**과의 업무 협력 시 그룹에 영향을 미칠 가능성이 있는 뇌물수수 및 부패 방지 관련 법률이 있는 관할권입니다.

- |         |        |       |
|---------|--------|-------|
| • 호주    | • 일본   | • 태국  |
| • 중국    | • 한국   | • 미국  |
| • 인도    | • 홍콩   | • 영국  |
| • 인도네시아 | • 싱가포르 | • 베트남 |

7.4 모든 임직원은 그룹의 '**뇌물수수 및 부패 방지와 선물, 여행 및 접대 취급 정책**'에서 자세한 내용을 참조해야 합니다.

## 8. 자금세탁 및 테러리스트 자금 조달

8.1 자금세탁 및 테러리스트 자금 조달에 연루된 범죄를 상대로는 어떠한 사업 및 금융 거래도 주고받지 않음으로써 평판, 운영 및 재무 관련 리스크로부터 그룹을 보호하는 것은 모든 임직원의 최우선 임무입니다.

8.2 일반적으로 **자금세탁**이란 범죄자들이 범죄 활동 수익금의 실제 출처와 소유자를 숨기려는 목적에서 시도하는 처리 방식을 의미합니다. 성공 시, 해당 재산은 범죄와의 연관성을 가린 채 합법적으로 보일 수 있습니다. 즉, 범죄자는 자신의 재산이 추적되어 범죄가 밝혀지고 적발될 두려움 없이 범죄적 이익을 취할 수 있게 됩니다.

8.3 **테러 자금 조달**은 테러리즘 또는 테러리즘을 장려, 계획하거나 이에 참여하는 대상에 대한 모든 형태의 재정적 지원을 말합니다. 테러리스트 자금 조달은 해당 자금의 출처가 자선 기부와 같이 합법적일 수도 있다는 점에서 자금세탁과는 다릅니다.

8.4 그룹의 잠재적 거래상대방의 사업 및 배경을 이해하고 자금, 재산 및 서비스의 출처와 목적지를 판단할 수 있도록 적절한 거래상대방 확인을 실시해야 합니다.

8.5 범죄 수익금 또는 테러 자금과의 연관성을 알고 있거나 그렇게 믿을 만한 합리적 근거가 있는 거래에 대해 무관심한 태도를 취하거나 눈감는 행위는 각 현지 법규에 의해 유죄로 인정될 수 있습니다. 범죄 수익금이나 테러리스트 재산에 대한 인지 또는 의심 사례를 보고하지 않는 것은 그룹의 사업장이 있는 관할권에서 **형사 범죄**로까지 취급될 수 있습니다.

8.6 위와 관련한 일체의 거래 의심 사례는 현지 준법감시인, 또는 현지에 담당 부서가 없는 경우에는 그룹 준법감시인에게 보고해야 하며, 이를 자체적으로 조사해서는 안 됩니다.



8.7 모든 임직원은 그룹의 '자금세탁 및 테러 자금 조달 방지 정책'에서 자세한 내용을 참조해야 합니다.

## 9. 제3자 리스크 관리

9.1 그룹은 자사 소속 임직원 이외에도, 그룹, 그 고객, 투자자 및 기타 이해관계자들에게 고품질의 제품 또는 서비스를 제공해주는 방대한 제3자 네트워크에도 의존합니다. 이러한 제3자에는 벤더, 건설 계약업체, 자산관리자, 자산평가사, 부동산 중개인, 유통업체, 컨설턴트, 중개인, 라이선싱 대리인, 변호사, 회계사, 그리고 그룹이 사업 수행과 관련하여 계약을 체결한 기타 서비스 제공자가 포함될 수 있습니다.

9.2 그룹은 리스크, 비용 및 제공 서비스를 고려한 최선의 업무 파트너를 선택하기 위해 그룹과 협력하는 여하한 제3자의 정보를 수집하여 실사를 수행할 책임이 있습니다. 리스크 평가는 그룹이 가입한 제3자 리스크 실사 플랫폼, 또는 해당 제3자 리스크 실사 플랫폼을 이용할 수 없는 경우에는 그룹 규정준수 부서가 지정한 다른 수단을 사용하여 설문지에 답변하는 형태로 진행됩니다. 제3자 리스크 평가의 실행과 규정준수 부서의 승인이 완료되지 않은 상태에서는 어떠한 새로운 제3자와의 계약도 체결할 수 없습니다. 현지 사무소가 제3자 온보딩 절차에서 설정하는 모든 금전적 한도는 그룹 규정준수 부서의 승인을 거쳐야 합니다. 제3자와의 협력에 책임이 있는 해당 부서 또는 담당자는 계약서에 서명하기 전에 계약서상의 조건 및 약관이 포함된 승인 관련 증거를 법무 부서에 제출하여 검토 및 심사를 받고, 승인 관련 증거를 재무 부서에 제출하여 지급 협의를 진행해야 합니다.

9.3 그러한 제3자의 온보딩을 담당하는 부서 또는 담당자는 해당 제3자가 그룹의 행동 강령 및 기업윤리 정책과 공급업체의 공식 홈페이지에 게시된 행동 강령 및 정책을 읽고 이해했음을 인정하도록 해야 합니다.

## 10. 내부자 거래

10.1 그룹 관련(해당되는 경우), 또는 거래처, 공급업체, 투자자 또는 합작투자 파트너를 비롯하여 관련 증권이나 주식 또는 부채가 증권거래소 또는 조직화된 증권시장에서 거래 중인 기타 회사와 관련된 내부 정보를 보유한 모든 임직원은 이러한 회사의 증권 또는 그 가격이 이러한 회사의 증권에 직간접적으로 의존하고 있는 금융 상품을 거래할 수 없습니다.

10.2 모든 임직원은 내부자 거래에 관한 모든 관련 법률을 준수해야 합니다. 일반적으로 이는 스스로 내부 정보를 보유한 상태에서 주식 또는 기타 증권을 거래할 때, 또는 그러한 정보를 추후 해당 주식 또는 기타 증권의 거래에 나설 다른 사람과 공유할 때 해당됩니다.

10.3 내부 정보에 대한 접근 권한은 **알아야 할 필요성**에 기반하여, 즉 해당 업무의 유형과 범위와 관련하여 적절한 경우에 한해 주어져야 합니다. 그룹 규정준수 부서는 그룹이 사업 운영 과정에서 내부 정보를 보유하고 있는 시점에 임직원이 증권을 거래하는 것에 대한 승인, 모니터링 및 유사시의 조사를 위해 **내부자 목록**을 유지합니다. 여기에는 ESR 주식과 관련된 내부 정보도 포함됩니다.

---

<sup>1</sup> 내부 정보란 ESR 또는 내부자 증권의 다른 발행자와 관련한 모든 구체적 정보로서, 공개된 적이 없고, 공개적으로 알려질 경우에는 내부자 증권의 가격에 상당한 영향을 미칠 가능성이 높은 정보를 의미합니다. 그러한 가능성은 합리적인 투자자가 이를 증권 가격에 영향을 미칠 정보로서 간주할 만한 경우에 존재합니다. 또한 합리적인 투자자가 투자 결정을 내릴 때 해당 정보를 고려할 만한 경우에도 존재하는 것으로 간주됩니다.

- 10.4 임직원은 스스로 그러한 발행인에 관한 내부 정보를 보유하고 있는 경우에는 ESR 주식을 비롯한 발행인의 증권을 어떤 식으로도 거래해서는 안 됩니다. 임직원이 내부 정보를 획득했거나 우연 등에 의해 그러한 정보를 전달받았을 수 있다고 생각되는 경우, 그룹 또는 현지 준법 담당자에게 즉시 통지하여 이를 기록하고 모니터링 목적의 승인을 얻을 수 있도록 해야 합니다.
- 10.5 ESR 증권, 주식 또는 부채를 거래 시에는 그룹 규정준수 부서에 **임직원 거래 승인 양식**을 제출하거나 지정된 온라인 규정준수 관리 플랫폼을 통해 사전 승인을 받아야 합니다. 싱가포르 증권거래소에 상장된 ESR-REIT과 한국 증권거래소에 상장된 ESR Kendall Square REIT 주식의 경우, 승인 및 모니터링 목적의 현지 규제 요건을 준수하기 위해 각각의 현지 규정준수 정책에 의해 별도로 다루어집니다.
- 10.6 그룹 규정준수 부서는 그룹이 관련 내부 정보를 보유 중일 수 있는 상장 회사(들)에 대한 **'거래 제한'** 정보를 수시로 임직원에게 회람합니다.
- 10.7 내부자 거래는 그룹의 **임직원 거래 및 내부 정보 취급 정책**, 그리고 **공개 통제 및 절차**라는 또 다른 그룹 정책이 관장하는 내부 정보와 관련한 각각의 공개 요건에서 다루어집니다.

## **11. 그룹 정보 및 자산의 보호 및 사용**

- 11.1 모든 임직원은 그룹의 정보 및 자산을 보호해야 하며, 이를 오직 정당한 회사 관련 목적으로만 사용해야 합니다.
- 11.2 그룹 또는 그룹이 기밀유지 계약을 체결했거나 모든 유형의 사업 관계를 맺고 있는 제3자와 관련한 일체의 기밀 또는 독점 정보를 여하한 외부 당사자에게 공개하거나 본인의 사적 목적을 위해 사용하려면, 먼저 고위 경영진의 승인을 얻어야 합니다.
- 11.3 기밀 또는 독점 정보에는 개인 데이터, 고객 정보, 영업 비밀, 저작권, 특허, 사업/마케팅 계획, 디자인, 데이터베이스, 기록, 미공개 재무 데이터 및 보고서와 같은 지적 재산이 포함될 수 있습니다. 이 정보의 무단 사용 또는 배포는 회사 정책의 위반에 해당하며 징계 조치의 대상이 됩니다.

## **12. 클린 데스크 정책**

- 12.1 본 정책의 목적은 모든 임직원을 대상으로 보안과 신뢰의 문화를 확립하는 것이며, 직원, 투자자, 거래처 및 벤더 관련 민감/기밀 정보를 담고 있는 종이 및 전자 문서 모두를 보호하는 일은 임직원의 참여 및 지지에 의해 크게 좌우됩니다. 클린 데스크 정책의 공표는 개인 데이터 및 민감/기밀 데이터가 담긴 종이 및 전자 문서가 적절한 물리적 보호를 보장받을 수 있도록 도와줍니다.
- 12.2 다음과 같은 모범적 관행이 요구됩니다.
- a) 개인 데이터가 담긴 하드카피가 분실 또는 도난될 확률을 낮추고 개인 데이터의 적절한 폐기를 위한 작업을 줄일 수 있도록, 개인 데이터 또는 민감/기밀 데이터의 인쇄는 가급적 최소화되어야 합니다.
  - b) 개인 데이터 또는 민감/기밀 데이터를 인쇄하는 데 사용 가능한 일체의 프린터는 오직 개인 데이터 액세스 권한이 있는 사람들만이 동행이나 감독자 없이 접근할 수 있는

물리적으로 통제된 환경에 놓여있어야 합니다. 이렇게 하면 인쇄를 실행한 사람이 인쇄물에 접근하기 전에 누군가가 프린터에서 개인 데이터의 하드카피를 가져갈 위험을 방지할 수 있습니다.

- c) 특히 중요한 민감/기밀 데이터 또는 개인 데이터를 프린터에 인쇄해야 하는 경우, 이는 오직 직원의 개인 사무실이나 접근권 관리 환경과 같이 엄격하게 통제된 환경에서만 수행되어야 합니다. 이 조치는 주로 인쇄량은 적지만 개인 데이터의 손실 또는 공개에 따른 대가는 클 수 있는 상황에 적용됩니다.
- d) 개인 데이터나 민감 데이터의 인쇄 용도로는, 각 인쇄 작업에 암호를 설정할 수 있고 프린터에 올바른 코드를 입력할 때까지는 인쇄물이 출력되지 않는 등, 안전한 인쇄를 지원하는 프린터 또는 복사기를 사용하도록 장려되어야 합니다.
- e) 하드카피에 인쇄되어 휴대용 USB 드라이브와 같은 대용량 저장장치에 담긴 개인 데이터 또는 민감/기밀 데이터는 사용 시를 제외하면 잠금 장치가 있는 컨테이너(예: 파일 캐비닛 또는 책상 서랍)에 보관해야 합니다.
- f) 더는 필요하지 않게 된 개인 데이터나 민감/기밀 데이터의 하드카피는 교차 파쇄기 등을 이용하여 적절히 파기해야 합니다.
- g) 점심시간 등으로 인해 장시간 자리를 지우기 전에는 항상 근무 공간을 정돈하십시오.
- h) 서류 정리를 위한 시간을 월별 일정에 포함시키십시오.
- i) 책상을 떠날 때는 항상 컴퓨터 화면을 보호하고, 노트북이나 태블릿 등의 휴대용 컴퓨팅 기기를 잠그십시오.
- j) 책상을 정리하고, 책상서랍 및 파일 캐비닛을 잠그고, 일과 종료 시 데스크톱 컴퓨터를 로그오프하거나 종료하십시오.
- k) 비밀번호를 컴퓨터 위나 아래에 붙여놓은 포스트잇에 남겨두거나 접근 가능한 장소에 적어두면 안 됩니다.
- l) 민감/기밀 정보나 개인정보가 적혀 있는 화이트보드는 지워야 합니다.

### 13. 데이터 보호

13.1 바람직한 데이터 보호 정책은 데이터의 기밀성과 안전한 보관을 보장할 뿐만 아니라, 다음을 도와줍니다.

- a) 규제 준수 보장
- b) 평판 보호
- c) 거래처 및 임직원의 신뢰 유지
- d) 정보 인프라 및 자산의 철저한 보호
- e) 정보 가치 향상
- f) 데이터 손실 또는 도난 위험의 감소

13.2 이러한 **고위험 데이터**, 즉 손실 시 상당한 계약상 책임이나 법적 책임, 그룹 이미지 및 평판에 대한 심각한 손상, 또는 법적, 재무적, 사업적 손실로 이어질 수 있는 모든 정보에 대해서는 각별한 주의가 필요합니다. 고위험 데이터의 예는 다음과 같습니다.

- a) **이름 및 연락처 정보:** 이름 및 이니셜의 여하한 조합, 집 주소, 자택 전화번호, 이메일 주소, 휴대폰 번호, 생년월일.
- b) **개인 신상:** 연령, 성별, 결혼 여부, 국적, 성적 지향, 인종 또는 민족적 출신, 종교적 신념.
- c) **개인 식별 정보:** 정부 발행 신분증 번호, 어머니의 결혼 전 성, 운전면허증 번호, 여권 번호, 신용 기록, 범죄 기록.
- d) **금융 기관 데이터:** 신용카드 또는 ATM 번호, 은행 계좌번호, 금융 계좌에 대한 액세스를 허용하는 비밀번호 또는 보안 코드 또는 액세스 코드 및 암호.
- e) **고용 관련 정보:** 급여, 보너스, 기타 보상 정보, 신원조회 정보.

13.3 많은 사법권에는 다음과 같이 정의되는 **개인 데이터**의 보호와 관련한 구체적 규정이 마련되어 있습니다.

*“자연인과 직간접적으로 관련된 데이터로서, 해당 데이터로부터 개인의 신원을 확인하는 것이 실제로 가능한 모든 데이터”*

13.4 개인 데이터와 관련하여, 국가 간 데이터 전송 제한 및 각 규제 당국에 대한 위반 통지 의무는 그룹을 사업장 현지의 법률 및 규정준수 위험에 노출시킬 수 있는 위험 요인입니다. 확신이 서지 않는 경우에는 인사 부서나 규정준수 부서로부터 조언을 구해야 합니다.

13.5 개인 데이터 보호는 아래의 중요한 원칙에 의해 뒷받침됩니다.

- a) 공정하고 합법적으로 처리해야 합니다.
- b) 구체적이고 합법적인 목적을 위해서만 획득해야 합니다.
- c) 적절하고 관련성이 있으며 과도하지 않아야 합니다.
- d) 정확하고 최신 상태를 유지해야 합니다.
- e) 필요 이상으로 오래 보관하지 않아야 합니다.
- f) 데이터 주체의 권리에 입각하여 처리해야 합니다.
- g) 적절한 방식으로 보호해야 합니다.
- h) 법률이 허용하지 않는 한 국경을 넘어 전송하지 않습니다.

13.6 모든 임직원은 그룹의 데이터를 보호하고 관련 법률을 준수해야 합니다. 그룹 I.T 부서가 게시한 **정보 보안 정책**을 참조하십시오.

## 14. 재무 및 사업 보고

14.1 그룹은 자사의 재무 및/또는 연례 사업 보고서를 정확하고 시의적절한 방식으로 관련 정부 기관에 제출해야 합니다.

14.2 ESR의 경영진은 모든 임직원이 이러한 책임을 매우 진지하게 받아들이기를 기대합니다.

14.3 그룹은 각 그룹사에 적용 가능한 모든 재무 보고 및 회계 관련 규정을 준수한다는 방침을 가지고 있습니다. 회계 또는 감사 문제에 관한 우려사항이 있는 모든 임직원은, 최고재무책임자(“CFO”)나 현지 준법감시인, 또는 현지에 담당 부서가 없는 경우에는 그룹 준법감시인에게 그러한 우려사항을 제출해야 합니다.

## 15. 기록 보관 및 공개

- 15.1 그룹이 책임 있는 사업 결정을 내릴 수 있으려면 정보의 정확하고 시의적절한 기록과 보고가 전제되어야 합니다. 모든 사업상 경비지출보고서는 시의적절하게 문서화되고 정확하게 기록되어야 합니다.
- 15.2 그룹의 모든 장부, 기록, 계정 및 재무제표는 법적 용도 및 감사추적 용도로 합리적으로 상세하게 유지되어야 하고, 그룹의 거래 내역을 정확하게 반영해야 하며, 공개, 보고 및 기록 보존 목적과 관련한 모든 해당 법률 또는 규정을 준수해야 합니다.

## 16. 차별 및 괴롭힘

- 16.1 그룹은 모든 측면에서 동등한 고용 기회를 제공하고자 최선을 다하고 있으며, 인종, 피부색, 종교, 성별, 연령, 장애 또는 출신 국가에 근거한 모든 종류의 불법적인 차별 또는 괴롭힘을 용납하지 않습니다.
- 16.2 임직원은 언어적, 신체적, 시각적 또는 성적 괴롭힘을 비롯한 모든 형태의 괴롭힘이 없는 직장을 유지함으로써 상호 존중의 가치를 옹호해야 합니다.

## 17. 작업장 안전 및 환경

- 17.1 그룹은 자사 시설에서 근무하는 모든 임직원에게 안전하고 건강한 직장을 제공하는 한편, 회사 운영의 환경적 영향을 최소화하기 위해 노력하고 있습니다.
- 17.2 임직원이 그룹 구내 또는 외부에서 업무 활동을 수행하는 동안 유해 물질을 오용하는 행위는 엄격히 금지됩니다. 이는 업무 능력을 저해할 뿐만 아니라 건강, 안전 및 환경에 위협이 될 수도 있기 때문입니다. 이러한 유해 물질에는 모든 합법 또는 불법 약물, 알코올성 음료, 합법적 처방전 없이 획득하거나 사용하는 의사처방 항정신성 약물 또는 이와 유사한 약물이 포함될 수 있으나 이에 국한되지 않습니다.
- 17.3 그룹은 사업을 영위함에 있어 환경, 사회 및 거버넌스(“ESG”) 책임의 고려에 비중을 두고 잘 관리된 개발 및 관리 플랫폼을 갖춘 모범적인 사업 관행 표준을 따르는 것에 높은 우선순위를 두고 있습니다. 그룹은 자사의 영향력이 미치는 범위 내에서 환경적 책임성의 증대를 촉진하고 환경친화적인 기술과 프로세스의 개발 및 확산을 장려하기 위한 이니셔티브를 시행할 계획입니다. 자세한 내용은 그룹의 **ESG 정책** 을 참조하십시오.

## 18. 소셜미디어

- 18.1 그룹은 소셜미디어의 정의에 전문적 또는 사회적 네트워킹, 댓글 또는 의견 게시, 사진, 오디오, 비디오 또는 기타 콘텐츠의 공유와 같은 활동을 위해 설계된 온라인 플랫폼 및 애플리케이션을 포함시키고 있습니다. 또한 소셜미디어 포럼에는 블로그, 소셜 네트워크(예: Facebook, Twitter, YouTube, LinkedIn, Instagram, Tumblr, WeChat 등), 개인 웹사이트, 그리고 아직 개발되지 않은 동적 커뮤니케이션 분야의 기타 미디어가 포함될 수 있습니다.
- 18.2 그룹은 임직원의 커뮤니케이션 권리를 존중하며, 이를 방해하거나 제한할 의도가 없습니다.
- 18.3 소셜미디어상에서 커뮤니케이션할 때는 다음 원칙을 실천해야 합니다.

- a) 진실하고 투명하게 행동합니다.
- b) 정중하고 공손하게 대합니다.
- c) 기밀 및 개인정보를 보호합니다.
- d) 해당 규칙 및 규정을 준수합니다.
- e) 현명한 판단력을 발휘합니다.
- f) 자신의 행동에 책임을 집니다.

18.4 다음은 해야 할 일과 하지 말아야 할 일들의 일부 예시입니다.

#### 해야 할 일

- 참여하고자 하는 각 플랫폼의 참여 관련 약관을 검토
- 소셜미디어상에서 그룹을 대표하지 않고 본인의 이름과 개인 자격으로 참여
- 항상 진실되고 정확한 태도를 유지
- 대화 주제와 관련이 있는 경우에만 ESR 소속임을 언급
- 달리 승인받지 않는 한 모든 발언은 개인적 견해를 공개 진술을 통해 밝힘
- 직장 동료나 고객과 직접 대면 시와 마찬가지로 온라인에서 행동

#### 하지 말아야 할 일

- 비속어 사용
- 무례하거나 명예를 훼손하거나 부정직한 의견을 표시
- 그룹, 거래처, 공급업체, 직장 동료 또는 사업 파트너에 관한 민감정보를 공유
- 관련하여 명시적으로 승인을 받지 않은 상황에서 자신을 ESR의 대리인 자격으로 묘사
- 전담 커뮤니티 관리자의 사전 동의 없이 ESR 명의의 소셜미디어 계정을 생성

### **19. 불법적이거나 비윤리적인 행동의 신고**

19.1 모든 임직원은 불법적이거나 강령의 위반에 해당할 수 있는 실제적/잠재적 불법 또는 비윤리적 행동과 관련하여 현지 준법감시인, 또는 현지에 담당 부서가 없는 경우에는 그룹 준법감시인과 상의하고 이를 신고해야 합니다.

19.2 정직하게 문제를 제기하는 임직원에게 대한 일체의 보복 행위는 엄격히 금지되며, 이는 강령의 위반에 해당하지만, 고의로 허위 고발을 행하는 것 역시 강령의 위반입니다. 정직한 보고의 의미가 스스로 우려사항을 제기함에 있어 반드시 옳아야 한다는 것은 아니지만, 제공되는 정보는 항상 정확해야 합니다.

19.3 그룹은 내부고발자의 신원을 기밀로 유지하며, 부당한 해고, 개인적 희생 또는 비공식적인 징계 조치로부터의 보호를 포함한 공정한 대우를 보장합니다. 그러나, 조사가 잠재적 형사 고발로 이어지게 될 경우, 내부고발자가 증언을 제공하거나 관련 당국과 면담해야 하는 상황이 발생할 수 있습니다. **내부고발자 신고 양식**을 참조하시기 바라며, 신고는 보다 효과적인 모니터링과 기록 보관을 위해 전자적으로 이루어져야 합니다. 관련 시스템에 액세스하는 방법은 현지 또는 그룹 규정준수 부서에 문의주시기 바랍니다. 의견제출 및 신고 목적의 이메일 그룹([whistleblowing@esr.com](mailto:whistleblowing@esr.com))도 이용이 가능합니다.

19.4 **내부고발자 정책**은 그룹의 공식 홈페이지에서 누구나 액세스할 수 있도록 유지됩니다.

## 20. 강령 위반 및 징계 조치

- 20.1 본 강령의 원칙을 위반하는 임직원은 징계 조치를 받게 되며, 여기에는 약식 해고도 포함될 수 있습니다. 또한 본 강령의 위반 시에는 현지 법률 및 규정이 적용됨에 따라 잠재적 형사 범죄 및 고발로 이어질 수도 있다는 점에 유의해야 합니다.

2021년 7월 13일에 개정됨