

SK hynix

GLOBAL COMPLIANCE GUIDEBOOK



SK hynix Global Compliance Guidebook



Message from the CEO

Dear Colleagues,

I would like to thank you for your outstanding performance in support of SK hynix and its reputation for quality and ethical conduct around the world. This Global Compliance Guidebook marks a major step toward safeguarding the reputation that we have all worked so hard to build and is a cornerstone of our continuing success.

SK hynix has become a leading chipmaker in the global market, consistently delivering products of superior quality to our customers and consistent value to our shareholders. Our status as an industry leader is only possible through your continued dedication and our collective commitment to comply with all legal and ethical obligations everywhere we do business.

We expect that there will be many challenges and unpredictable obstacles in our business environment as we continue to innovate and develop new products. While we recognize that no company code or policy can address every ethical question employees may face, this Global Compliance Guidebook provides a strong foundation and framework to successfully address these challenges. This book will help everyone conduct the Company's business ethically and legally, enabling us to continue to produce sustainable growth in an uncertain world.

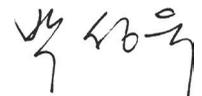
With our commitment to ethical conduct, the environment, and safety as a foundation for our success, we will ensure that all employees will unite and work together to achieve our greatest collective potential.

Finally, it is our ultimate goal and guiding principle to win in the marketplace the right way and share our success with all of our employees and other stakeholders. In addition to creating value for our stakeholders, we will serve as a key player in fostering an ethical business environment. Our commitment to ethical conduct is one of our most powerful driving forces and a key to our future success. I encourage you to read, understand and abide by our Global Compliance Guidebook. Please join me in supporting Global Compliance Guidebook and upholding the valued reputation of the Company.

Thank you.

Sung-wook Park

President/CEO of SK hynix
April 2015



Contents

SK HYNIX CODE OF BUSINESS CONDUCT AND ETHICS	04
1. Introduction to this Guidelines for Business Ethics and Conducts	05
2. Commitments to Our Customers	05
3. Respect for Our Colleagues	06
4. Conducting Our Business	07
5. Protecting Company Assets	10
6. Conflict of Interest	13
7. Social Responsibility	15
8. Violation of the Code	17
9. Commitment to Shareholders and Investors	18
ANTI-TRUST	19
1. Anti-trust Laws in General	21
2. Agreements that Unreasonably Restrain Competition	21
3. Information Sharing	23
4. Competitively Sensitive Activities	24
5. Unilateral Conduct That Could Unreasonably Restrain Trade	25
6. Collaboration among Competitors	26
7. Violation of Anti-trust Laws	27
8. Questions	27
ANTI-CORRUPTION	28
1. Purpose	29
2. Acceptance or Provision of Bribes	30
3. Charitable Contributions	33
4. Interactions with Government Entities & Officials	33
5. Third Parties	34
6. Facilitation Payments	35
7. Joint Ventures, Mergers, Acquisitions & New Market Entry	35
8. Books and Records & Related Internal Controls	36
9. Violation of this Policy	36
SUPPLIER MANAGEMENT	37
1. Labor and Human Rights	38
2. Health and Safety	38
3. Environment	39
4. Management System	39
5. Legal Operation of Raw Materials	39
6. Ethics	40

DATA PROTECTION	41
PERSONAL DATA POLICY	42
1. Collecting Personal Information	43
2. Using Personal Information	43
3. Notification of Company's Collection, Usage, and Disclosure of Personal Information	44
4. Sensitive Personal Information	44
5. Monitoring	45
6. Protection of Employee's Personal Information	45
7. Destruction of Personal Information	47
8. Third Party Request for Access to Personal Information	47
9. Employees' Obligations to Cooperate with Data Protection Authorities	48
10. Data Transfers and Third Party Service Providers	48
11. Known or Suspected Data Breaches	49
12. Resolving Complaints	49
13. Overseeing the Company's Information Security Program	50
CUSTOMER PRIVACY POLICY	51
1. Information We Collect	51
2. Using Customer Information	52
3. Sharing Our Customer Information	52
4. Information Collected Automatically : Cookies and Tracking on Our Websites	52
5. Third Party Links	54
6. International Transfers	54
7. Security of Customers' Information	55
8. Access to Customers' Personal Information	55
9. Choices Regarding Customers' Personal Information	55
10. Data Controller	55
CONFLICT MINERALS	56
1. Conflict Minerals Rules in General	58
2. Responsibility and Authority	59
3. Product Identification	60
4. Conflict Minerals Procurement	61
5. Supply Chain Due Diligence	62
6. Conflict Minerals Data Management System	63
7. Customer Conflict Minerals Requests	64
8. Violation of the Conflict Minerals Policy	64
EXPORT CONTROL	65
1. Export Control Laws in General	67
2. Export Compliance Management Organization	69
3. Violation of Export Compliance Policy	70
RECORD MANAGEMENT & RISK ASSESSMENT	71
FREQUENTLY ASKED QUESTIONS	73

01 SK hynix Code of Business Conduct and Ethics



SK hynix Code of Business Conduct and Ethics



01

Introduction to this Guidelines for Business Ethics and Conduct

These guidelines for Business Ethics and Conduct (the “Code”) for the members of SK hynix (collectively, “SK hynix”, “We”, “us”, “our” or the “Company”) and our partners provide guidelines for everything SK hynix does and therefore applies to all SK hynix directors, officers, and employees, as well as any subsidiary or business venture that SK hynix controls. We strongly believe that if a company does not appropriately address legal and ethical challenges, it may incur far more losses than earnings while disrupting sustainable growth. SK hynix is committed to conducting business the right way.

Violations of law or the Code are a serious matter and can lead to government investigation, fines, imprisonment, and other consequences for SK hynix and anyone involved in the violation. All employees have a duty to protect themselves, their colleagues, and the Company by reporting any violation or potential violation of applicable law, the Code, or a Company policy. Retaliation against those who do so is strictly prohibited.

02

Commitment to Our Customers

Our goal is to produce quality, innovative products that meet and surpass the expectations of our customers in a manner that complies with all legal and ethical obligations that apply to our business. SK hynix treats all our customers with sincerity and reasonableness and hold customers’ wants and needs as our priority and use efforts to find value in customers’ demands through innovative and creative measures.

SK hynix employees are not only obligated to follow the applicable laws and regulations, the Code, and Company regulations mentioned herein but also to uphold high ethical values, maintain their pride for themselves and the Company’s reputation, and strive for continuous growth of the Company.

SK hynix will not disclose any confidential information of our customers without customer’s prior consent. Any information customers should know will be disclosed transparently so that the customers can make appropriate and reasonable decisions.

03

Respect for Our Colleagues**Equal Opportunity, Compensation, and Assessment**

SK hynix strives to provide fair opportunities according to employee's ability and performance, and assess all employees and job applicants according to unbiased criteria.

In all employment practices – including hiring, promotion, compensation, and training opportunities- SK hynix does not discriminate based on sex, religion, race, skin color, marital status, language, nationality, social position, university attended, physical condition, handicap, property owned or any other categories protected by law.

Harassment

SK hynix prohibits all forms of harassment in the workplace. Harassment is any unwelcome or offensive language or behavior directed at another person on the basis of any identifying personal characteristic. Harassment also includes unwelcome sexual advances or innuendos, offensive jokes, derogatory slurs, and offensive visual images. Employees should promptly report any harassment to Ethics Management Team.

Workplace Health & Safety

All employees are entitled to a safe, clean, and healthy working environment. Accordingly, SK hynix has implemented safety and health management procedures to prevent safety-related accidents and minimize health risks. These measures include the Environment, Safety, and Health Experience Center; systems to prevent human error and monitor environmental conditions on production floors; and implementation of emergency drills. Employees must comply with all safety measures implemented by the Company.

Employees must comply with all workplace safety rules and instructions, such as :

- ☑ Regulations on workplace safety (if required by the applicable law);
- ☑ Laws and regulations, such as those requiring permits for certain activities or establishing standards for handling or transferring controlled substances;
- ☑ Posted safety notices;
- ☑ Instructions regarding equipment operation; and
- ☑ Instructions from managers or other employees responsible for workplace safety regarding any work-related task.

In the event of a natural disaster or other incident that could threaten health or safety or pose an environmental concern, employees must promptly report the issue to their manager.

Workplace Violence

SK hynix expects that all employees will conduct themselves in a civil and respectful manner while at work and will solve all conflicts in a cooperative manner. All employees shall report suspicious activities on or near Company premises.

Violence or threats of violence in the workplace are strictly prohibited. Abusive, intimidating or hostile words and actions often precede more serious violent behavior and should be reported immediately to Ethical Management Team.

Except for authorized security personnel, firearms and other weapons are prohibited on Company property regardless of whether an employee is permitted to possess or carry them.

Alcohol, Drugs & Intoxicating Substances

Employees must ensure that any use of alcohol outside of working hours does not impair their ability to perform their duties for SK hynix in a safe manner. Employees who report to work under the influence of alcohol may be sent home without pay or terminated at the discretion of the Company's management.

Alcohol may be consumed on Company premises only at events approved in advance by management. Employees who consume alcohol during the workday at events off Company property must ensure that doing so does not impair their ability to exercise sound business judgment on SK hynix's behalf. Employees should always ensure that any consumption of alcohol at a work-related event is appropriate and not excessive.

SK hynix maintains a zero-tolerance policy regarding other intoxicating substances and illegal drugs. Employees may not work under the influence of such substances or use them during the workday. Use of such substances is grounds for immediate termination. Employees who observe a colleague impaired due to alcohol, drugs, or other intoxicating substance must promptly notify their manager.

04

Conducting Our Business**Anti-trust**

We treat our competition fairly and comply with all laws designed to protect competition. Fair dealing and anti-trust laws protect industry competition by generally prohibiting formal or informal agreements between business entities and coordinated actions that seek to manipulate

prices or unfairly impact competitors. These laws also prohibit actions aimed at improperly excluding, restricting, or eliminating competition. Employees should avoid any conduct that could be interpreted as an illegal agreement with other business entities to restrict or diminish competition. Examples include price fixing, limiting production or allocating markets or territories between the entities.

Anti-dumping laws preclude manufacturers from exporting a product to another country at a price below the cost of production or below the price charged in its home market. The purpose of these statutes is to prevent manufacturers using surplus product to harm competitors in other countries.

Understanding the requirements of anti-trust and anti-dumping laws can be challenging, and violation of these statutes can result in severe penalties for SK hynix and any employee involved in the violation. Employees should refer to the Anti-trust Policy, and should seek assistance as described in that Anti-trust Policy for questions related to these laws.

Bribery & Corruption

SK hynix abides by anti-corruption laws everywhere it does business. These laws prohibit offering, paying, requesting, accepting, or promising to accept anything of value in order to improperly influence the recipient. Examples of items that could be used to exert improper influence include meals, entertainment, gifts, and political contributions. Anti-corruption laws focus on the intent underlying the benefit, not on its size or value. Thus, even a small gift or contribution is improper if it is given with the intent to influence the recipient's independent judgment.

In addition, SK hynix never pays bribes or kickbacks to any government official or to any individual or commercial entity with which it does business, even if those payments would not violate the law in the country where the payment is made. Facilitation payments are strictly prohibited.

Providing or accepting gifts, travel, entertainment, meals, and charitable contributions could all have the potential to be viewed as a bribe. For this reason, employees may be required to obtain preapproval before providing or accepting such benefits, especially if the recipient is a government official.

Employees should refer to the Anti-Corruption Policy for more information about the types of transactions that must be reviewed in advance and how to obtain preapproval.

International Trade and Import/Export Controls

International trade and import/export laws and regulations sometimes restrict a company's ability to conduct business with certain nations, companies, entities, and individuals. International sanctions imposed by national governments are the best example of these types of laws. In addition, import and export controls may:

- ☑ Prohibit the export of goods, software, and technology to certain countries or groups;
- ☑ Establish limits on the amount or value of product that can be exported to a particular country; or
- ☑ Prohibit companies from boycotting a particular country, entity, or person.

Money Laundering

Money laundering is any attempt to make illegal funds appear legitimate, usually by concealing their true source. SK hynix does not participate in money laundering and will not assist others in money-laundering activity.

Employees must be aware of the following warning signs that could indicate money laundering:

- ☑ Orders that are inconsistent with a customer's or supplier's usual practices;
- ☑ Requests to pay in cash;
- ☑ Requests to make payments to or accept payments from third parties;
- ☑ Requests to make payments to suppliers or agents to accounts in a country where the supplier or agent is not located; or
- ☑ Requests to ship products to a country other than the buyer's or seller's home country.

Employees who observe any of these warning signs should report them to their manager or to Ethics Management Team.

Delegated Authority

Employees must understand the limits on their authority to bind the Company and never take any action outside the limits of their authority.

Employees may not speak on behalf of SK hynix unless they have been authorized to do so. Employees permitted to speak for SK hynix must always be truthful, complete, and respectful in

their communications. Employees not authorized to speak on SK hynix's behalf may not accept a public speaking engagement or publish any article related to SK hynix's business or products unless the speech or article has been preapproved by the employee's manager. In any such speech or publication, employees must disclose that they are not speaking on SK hynix's behalf.

Compliance with Laws and Regulations

All business activities of the Company in any and all jurisdictions must comply with applicable laws and customs of the relevant country and origin.

The Company should voluntarily operate a compliance system to continuously encourage its employees to voluntarily comply with the applicable laws and customs.

The Company must satisfy regulations and requirements with respect to the Conflict Minerals (Tantalum, Tungsten, Tin, Gold) and acquire transparent supply chains of raw materials by strictly managing the origin and distribution of the Conflict Minerals.

Cooperation with Partner Companies

SK hynix will apply fair and reasonable standard and provide equal participation opportunities to qualified supplier/vendor companies. Employees will work efficiently and effectively by engaging in active cooperation and communication with other members of the Company and/or partners of the Company.

Transactions with partner companies shall be conducted in a transparent and reasonable way by discussing different aspects of the transactions. No unfair trade practices by the Company will be conducted by abusing its position.

05

Protecting Company Assets

Use of SK hynix Assets

Employees should use the Company assets only as necessary to carry out their duties and responsibilities for SK hynix or as otherwise authorized by the Company.

Employees may not use the Company assets to compete with SK hynix or for the benefit of any personal business or political venture outside of their employment with SK hynix. Personal use of the Company assets (such as telephones, computers, printers, etc.) should be minimal and should not interfere with employees' duties and responsibilities to SK hynix.

Keeping SK hynix's Assets Secure

All employees have a duty to protect SK hynix's assets from misuse. As a semiconductor Company, SK hynix's trade secrets and other intangible proprietary information are some of its most valuable assets. Examples of these assets include:

- ✓ Technical specifications;
- ✓ Information about new product development;
- ✓ Manufacturing information, such as processes for manufacturing products and information about the Company's capacity and output;
- ✓ Information about the Company's suppliers and the terms on which SK hynix acquires raw materials;
- ✓ Information about the Company's customers; and
- ✓ Marketing strategies and plans.

Employees must exercise care to safeguard these, and all other, Company assets. Employees authorized to access SK hynix's physical and technological assets must exercise caution to ensure that unauthorized individuals or those outside the Company do not gain access to those assets.

All access control devices, such as badges, keys, passwords, and magnetic access cards must be secured against loss or theft. Employees must promptly report any loss or theft of these access devices. Computers and servers must also be secured against theft or loss and placed in a secure mode when not in use. Employees may not circumvent or attempt to circumvent any security measure.

Intellectual Property

Intellectual property is a valuable asset of the Company and includes the Company's patents, trade secrets, trademarks, copyrights (including moral rights) and proprietary knowhow and information. Any intellectual property created by an employee during his or her employment belongs exclusively to the Company and is the Company's intellectual property. The Company's intellectual property should be safeguarded and may not be used for an employee's personal benefit or for the benefit of a third party.

Likewise, it is important to respect the property rights of others. The Company does not tolerate the unauthorized use of anyone else's intellectual property. Before soliciting, accepting, or using another company's or an individual's intellectual property, make sure there is an appropriate licensing agreement in place or seek guidance from the Legal Department.

While working for SK hynix, employees may gain access to confidential information, including information about SK hynix (such as confidential financial information), its business partners (such as customer requirements), and other employees (such as personal identifying information).

All confidential information must be protected, stored properly, and disclosed only to individuals authorized to access the information or as required by law. Employees must comply with all laws governing privacy, data security, and transfer of personal information to third parties or to other countries.

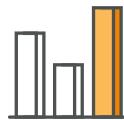
Employees should refer to the Data Protection Policy for more information about SK hynix's protection of and right to access employees' personal information.

Creating and Maintaining Accurate Records

Employees must comply with SK hynix's system of internal controls and must ensure that corporate records are truthful and accurate. All business records must:

- ■ ■
- ✓ Fully and accurately describe the transaction being recorded;
- ✓ Comply with applicable accounting standards;
- ✓ Be supported by accurate documentation; and
- ✓ Be promptly reported.

No cash or other assets may be maintained in any off-the-books account. In addition, employees must comply with all applicable record management policies and legal hold notices that they receive.



06

Conflict of Interest

Respect for the Rights of Our Employees

SK hynix respects the right of all employees to manage their personal affairs. However, employees' personal interests must never affect (or appear to affect) the performance of their duties for SK hynix. The following principles are designed to help employees identify and respond to potential conflicts of interest.

SK hynix is committed to working with employees affected by a conflict of interest to resolve or mitigate the conflict in a manner that does not affect the employee's position with the Company. However, if SK hynix determines that the conflict cannot be resolved, the employee may be required to cease the activity from which the conflict arises.

Outside Employment, Directorships, & Other Activities

Outside employment must never interfere with an employee's duties to SK hynix, and employees may not use Company time or resources in furtherance of employment with any other entity. Employees may not provide services to an individual or entity that competes with SK hynix (including as an employee, board member, officer, trustee, partner or consultant) without prior written approval from the employee's manager.

An employee must also obtain prior written approval from the employee's manager before providing services to a foundation, charity or non-profit organization if the employee will be paid for his or her service. Unpaid service as a director of a charitable or religious organization need not be reported or preapproved.

If an employee owns stocks in a competitor of SK hynix, he may need to report to SK hynix, especially when he or she owns a large amount of the stock of a competitor or hold a sensitive position with the Company. The employee should check with his manager or Ethics Management Team.

An employee must report to his manager, the Legal Department or the Global Compliance Team if any of his family members is employed by any competitor, customers or suppliers, in whatsoever nature.

Competition & Business Opportunities

Employees must not compete with SK hynix while employed by SK hynix.

Employees may not take advantage of business opportunities that they learn about through their position with SK hynix or direct those opportunities to a third party unless SK hynix has been offered and declined the opportunity. The term "business opportunity" refers to any op-

portunity to engage in an activity that may generate a profit for SK hynix, even if the opportunity does not relate to the semiconductor industry.

Personal Relationships

Employees' relationships with relatives, close friends, and members of their household should never influence their duties to SK hynix. Employees may not participate in any business decision on behalf of SK hynix that could benefit an individual with whom the employee has a close personal relationship.

SK hynix does not allow employees to influence employment-related decisions that affect a relative or a member of their household. Employees are not permitted to directly or indirectly supervise relatives or other members of their household who also work for SK hynix. Potential conflicts of interest arising from personal relationships should be reported to the affected employee's manager.

Gifts & Entertainment

Modest gifts and business entertainment can help create goodwill and build strong relationships with SK hynix's business partners. However, gifts and entertainment can also create a conflict of interest (or the appearance of a conflict) if they have the potential to interfere with the business judgment of the individual receiving them.

Employees are permitted to exchange gifts and entertainment with SK hynix's business partners provided that doing so is permitted by law and is consistent with the Code and any policy that applies to the gift or entertainment. As discussed below, special rules further restrict the exchange of gifts and entertainment with government officials.

- ☑ Gifts and entertainment should always be viewed as courtesies and may never be exchanged to influence a business decision, to gain an improper advantage, or to obtain something in return.
- ☑ Gifts must have a legitimate business purpose or be exchanged in connection with a recognized gift-giving holiday or event. Gifts of cash or cash equivalents, such as loans, gift cards, or stock, are always improper when exchanged with SK hynix's business partners. Employees should not accept gifts of more than nominal value from anyone soliciting business from SK hynix. Employees should use their best judgment when offering or accepting any gift, and should consult their manager or the Chief Compliance Officer for guidance about whether a particular gift is appropriate.
- ☑ Business entertainment, such as travel, lodging, meals, and entertainment, may be given or accepted if appropriate to the occasion.

Gifts and business entertainment must never embarrass SK hynix if publicly disclosed, and may not be exchanged with the same person or entity on a regular or frequent basis. Employees should refer to the Anti-Corruption Policy for more information.

- ☑ Responding to Improper Gifts or Entertainment. Offers of improper gifts or entertainment should be politely declined. Improper gifts of cash or cash equivalents must promptly be returned. For other gifts, if they cannot be declined (for example, because they were delivered by a third-party courier), the gift should be forwarded to Gift Returning Center for Company use or for donation to a charitable entity and you should alert the Chief Compliance Officer. The employee should send a letter to the individual or entity that provided the gift indicating that, under SK hynix's Code, the employee could not personally accept the gift, and that the gift was used for either Company or charitable purposes.
- ☑ Gifts and Entertainment Provided to Government Officials. In addition, many governments restrict the ability of their officials and employees to accept gifts or entertainment. Providing gifts and entertainment to government officials also entails a heightened risk that the benefits could be viewed as a bribe. For this reason, employees must generally obtain preapproval before providing gifts or entertainment to government officials regardless of the value of the gift or the entertainment. Employees should refer to the Anti-Corruption Policy for additional requirements applicable to such gifts and a description of the preapproval process.

07

Social Responsibility

Political Activities

SK hynix employees may be given opportunities and means to be a part of political activities. Employees must keep their personal political activities separate from their duties to SK hynix. Employees must never use Company time or resources to support a political position.

Employees must not represent that SK hynix supports a particular political position or candidate unless they are authorized to make such a representation on SK hynix's behalf.

Unless applicable law provides otherwise, an employee may not seek or hold public office (either elected or appointed, paid or unpaid) without prior approval from Ethics Management Team.

Cooperation with Government Entities

From time to time, SK hynix receives subpoenas, notices of investigation, and other requests for information from government entities. SK hynix is committed to responding to these requests fully and fairly within the requirements of applicable law.

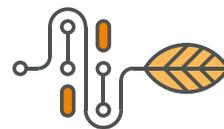
Employees who receive such requests should promptly notify their manager and forward the request to the Legal Department and should never respond to requests for information from the government or conduct an investigation in response to such requests unless they have been authorized to do so. All investigations and responses must be managed by the Legal Department to ensure that the response or investigation complies with applicable law and that SK hynix's trade secrets and privileged information are adequately protected.

Environment Friendly Management

SK hynix has been on the front line to build a sustainable future by fulfilling its environmental, and economic responsibilities through active environmental management. To realize our environmental vision, SK hynix has implemented measures to conserve water, reduce greenhouse gas emissions, develop replacements for perfluorocarbons (PFCs), and recycle waste heat. Employees must comply with the Company's initiatives to carry out its business in an environmentally responsible manner.

Employees must comply with all applicable laws and regulations regarding environment emissions and pollution. However, SK hynix views these regulations as a minimum baseline for environmental responsibility. Employees should actively seek ways to reduce the environmental effects associated with SK hynix business, and should bring opportunities for improving environmental practices to the attention of management.

SK hynix shall strive to take measures to prevent any pollution are detrimental to the public's health and safety and to improve the environment by preventing abnormal changes in the ecosystem and climate caused by human activities such greenhouse gas emission and to promote effective use of energy and raw materials and protection of water resource.



Building Partnerships in Our Communities

SK hynix is committed to supporting the communities where it operates through partnerships with local organizations. To that end, SK hynix maintains multiple initiatives to support local needs such as :

- ☑ The Happiness Sharing Fund, which allows employees to make donations matched by SK hynix. Funds are used to support underprivileged children and to support science-training programs for juniors.
- ☑ Partnerships with local service organizations. Employees are permitted to take time off of work to volunteer with SK hynix's partner organizations.
- ☑ Financial support for local festivals and events in the communities where our employees live.

SK hynix views these local support initiatives as important ways that it serves its communities. Employees are encouraged to take advantage of these and other opportunities offered by the Company to build a brighter future for our local communities.

08

Violation of the Code

Non Retaliation

SK hynix maintains a non-retaliation policy that applies to :

- ☑ All reports of actual or potential violations of law, the Code, or any Company policy or procedure;
- ☑ All complaints received by the Company about accounting, internal controls, or auditing matters; and
- ☑ Participation in any internal investigation conducted by SK hynix or any external investigation conducted by a government agency.

The term "retaliation" refers to any consequence imposed on an employee for the conduct above.

SK hynix will not tolerate retaliation against any employee for the conduct above. Violation of this non-retaliation policy will result in disciplinary action, up to and including termination. Any employee who believes he or she has been retaliated against should promptly report it to Ethics Management Team.

Consequences for Violating the Code

SK hynix requires that all directors, officers, and employees comply with all applicable laws and this Code. Violation of any law or this Code is a serious matter. Anyone who violates any applicable law or the Code may be subject to disciplinary action, up to and including, termination, suspension, loss of employment-related benefits, and criminal or civil liability, if applicable.

09

Commitment to Shareholders and Investors

Protection of shareholders and investors' interests shall be optimized through sustainable development and growth of the Company. SK hynix shall diligently provide, in accordance with relevant laws and general industry customs, credible information on overall management of the Company include business activities, structure, financial status, and performance.

In addition, for the purpose of the managing the risks related to strategic investments (including establishment of new facilities, upgrading existing facilities, and local or foreign real estate investments), any item that requires the Company board of directors' approval must include to which risk category such item belongs and a contingency/exit plan to monitor such risk. If any material change is made to such approved item, the changed item must be re-submitted to the board as a new item. Until the new item is approved by the board, any change made to the previously approved item shall not be deemed effective.

02 Anti-trust





Anti-trust

SK hynix and its subsidiaries are committed to competing ethically, and complying with the spirit and letter of all anti-trust laws in the countries where it does business. No person—either employees or others acting on SK hynix’s behalf—is permitted to violate these laws or deviate from this Anti-trust Policy (“Anti-trust Policy”).

Violation of anti-trust laws can have severe consequences for both SK hynix and for the person involved in the violation. In most countries, violations can lead to fines and imprisonment for individuals, and severe financial liability and loss of business for SK hynix. For example, in the United States, an individual can receive a maximum sentence of ten years for being found guilty of price fixing, and a corporate fine can be as high as \$100 million. Violations can also lead to expensive and time consuming litigation, as well as civil penalties, including trebled monetary damages. Importantly, violations of the anti-trust laws can harm the reputation and goodwill of SK hynix.

This Anti-trust Policy contains important information to help employees comply with anti-trust laws, and to prevent, detect, and respond to anti-trust issues when they arise. This Anti-trust Policy uses the term employee(s) to refer collectively to all employees, officers, directors, and agents of SK hynix. Compliance with this Anti-trust Policy is mandatory. All of SK hynix employees are required to read, comply with, and understand how this Anti-trust Policy applies to their job functions.

Key Anti-trust Terms

-  A competitor is a party who is or reasonably could be offering any products or services that compete with those offered by SK hynix. The term includes any individual connected to the competitor, such as its officers, directors, employees, agents, and vendors. In some cases, where a company is reasonably perceived by customers as a potential market entrant, it should be treated as though it were an existing competitor.
-  An agreement may take the form of explicit understandings, either verbal or written. Also, informal agreements, even unspoken ones, are often treated the same as formal agreements. Thus, a wink, nod, handshake, or any other indication of assent could be enough to infer an agreement for anti-trust purposes.
-  A monopoly exists when a company possesses such a large share of the market that it has the power to set prices or exclude competitors from the market. Mere market possession of monopoly power alone is not illegal. For an anti-trust violation to exist, there must be acquisition or maintenance of monopoly power through illegal or predatory acts as distinguished from growth or development as a result of a superior product, business acumen, or other legitimate reason.

01

Anti-trust Laws in General

It is the policy of SK hynix to comply fully with both the letter and spirit of all of the anti-trust laws. If local law or a business unit imposes stricter requirements than those articulated in this Anti-trust Policy, employees must comply with those stricter requirements.

Anti-trust laws aim to promote competition, protect consumers, and prevent companies from unreasonably harming competition. Thus, anti-trust laws make it illegal for two or more parties to unreasonably restrain trade. Anti-trust laws also prohibit a company from illegally monopolizing a market or attempting to do so.

This Anti-trust Policy is intended to identify the key areas in which employees need to be cautious and aware of anti-trust concerns. This Anti-trust Policy is not intended to be exhaustive, and each employee of SK hynix has a duty to know, understand, and comply with the anti-trust laws, as well as to ask questions if further information is required.

Employees of SK hynix should presume that their activities, particularly interactions and communications with competitors, will be subsequently scrutinized by third parties, including government enforcement agencies. Because anti-trust law suits and investigations are often fueled by poorly worded, informal, or exaggerated statements in documents, particularly emails, employees should avoid writing anything that could be misinterpreted as evidence of anticompetitive conduct. For example, the following language should be avoided: “dominate the marketplace” or “destroy or eliminate competitors.”

02

Agreements that Unreasonably Restrain Competition

The anti-trust laws prohibit two or more parties from agreeing to unreasonably restrain trade. The risk of an anti-trust violation is particularly high when the parties to the agreement are competitors. For example, anti-trust laws forbid agreements between competitors to fix prices, reduce output, bid rigging, allocate markets or customers, or boycott a particular person or group.

Any agreement between competitors—i.e., a horizontal agreement—raises serious anti-trust concerns and creates a high risk of an anti-trust violation. However, even certain agreements between SK hynix and its suppliers or customers—i.e., vertical agreements—have the potential to violate the anti-trust laws.

Reaching a formal agreement is not necessary for an anti-trust violation to occur. For example, an attempt to fix prices with a competitor may be unlawful, even if the attempt ultimately



proves to be unsuccessful. Also, even mere attendance at a meeting where competitors engage in an illegal discussion may imply acquiescence and make a nonparticipant responsible and subject to the same penalty as the active participants in the discussion. In such event, the participant must immediately leave the meeting and report it to the Global Compliance Team.

The following agreements between competitors (horizontal agreements) are almost always deemed to violate the anti-trust laws :

- ✔ An agreement to fix prices is an agreement between competitors on prices charged to others for products or services. Such agreements are illegal, whether they are meant to raise, lower, or stabilize prices.
- ✔ An agreement to engage in bid rigging is an agreement between competitors on any method by which prices or bids will be determined, submitted, or awarded, or any agreement to refrain from submitting bids against each other.
- ✔ An agreement to fix volume or production is an agreement between competitors to increase or restrict production or services.
- ✔ An agreement to allocate markets is an agreement between competitors on the division or allocation of customers or territories.
- ✔ An agreement to boycott is an agreement between parties that they will boycott or refuse to buy from a particular supplier or to sell to a particular customer. Such an agreement encompasses a situation where parties jointly insist upon certain terms with potential suppliers or customers. An anti-trust violation is more likely if the parties are competitors.

The following agreements with suppliers or customers (vertical agreements) may violate the anti-trust laws :

- ✔ An exclusive deal is an agreement where a buyer agrees to deal only with a particular seller or a seller agrees to deal only with a particular buyer. While such agreements are generally not prohibited, they can be unlawful depending on the length and terms of the exclusive deal, and the market power of the parties to the exclusive deal. For example, exclusive agreements can be problematic if they are for a long duration of time or can be used by an entity with market power to block existing or potential competitors from entering the market.
- ✔ Resale price maintenance involves a manufacturer requiring a distributor or customer to resell a product at or above a particular price point.
- ✔ A territorial or customer restraint involves a manufacturer precluding a distributor or a customer from reselling a product in a certain geographic area or to a particular party or parties.

Before a contract is signed, be sure to contact the Global Compliance Team if there are anti-trust questions or concerns.

03

Information-Sharing

The anti-trust laws prohibit competitors from sharing, directly or indirectly competitively sensitive information, including information on marketing, research and development, pricing, costs, profit margins, and capacity. The risk of violating the anti-trust laws is high when competitors have the opportunity to exchange, directly or indirectly, competitively sensitive information. Such risk is particularly high during trade association meetings or other types of gatherings that provide an opportunity for competitors to interact and communicate with each other.

Employees must not provide or receive from competitors any of the following information :

- ✔ Pricing
- ✔ Profit Margins
- ✔ Marketing Strategies
- ✔ Promotional Plans
- ✔ Costs
- ✔ Output or Capacity
- ✔ Market Share
- ✔ Research and Development or Improvement of Products

If a competitor offers to exchange information that raises anti-trust concerns, employees must decline the offer and immediately report the offer to their supervisor.

Obtaining and using information about competitors can be a legitimate part of the competitive process if gathered properly. Employees can obtain information lawfully from the following sources :

- ✔ Public documents and records
- ✔ Media reports
- ✔ Vendors (e.g., marketing firms)
- ✔ As voluntarily offered by customers (customers should not be asked to provide information on competitors)



04



Competitively Sensitive Activities

Any activity involving interaction between competitors raises anti-trust concerns. The following are examples of such activities :

- ✔ **Mergers & Acquisitions** : Potential mergers and acquisitions present the opportunity for competitors to exchange competitively sensitive information. Thus, employees must obtain legal clearance prior to engaging any party regarding a potential merger or acquisition. Even after legal clearance is obtained, employees must not exchange any information beyond what is necessary for the merger or acquisition. In addition, while conducting due diligence, competitively sensitive information of the other company should only be seen and evaluated by a designated, select group of individuals. Those individuals can be executives, managers, or employees at any level, but it is important to limit the number of people who have access to the other company's competitively sensitive information to as great an extent as practicable. Should the merger or acquisition not take place, for any reason, future actions could fall under increased scrutiny if a government agency thinks the decision was based on knowledge gained from the competitively sensitive information.
- ✔ **Trade Associations** : Trade association meetings provide an opportunity for competitors to interact and share competitively sensitive information. Also, members of trade associations must be careful in developing industry standards, certification programs, and codes of ethics. While these activities are generally considered lawful, they can violate the anti-trust laws if they have the effect of fixing prices or if they result in competitors improperly being boycotted or excluded from effectively competing in a market.
- ✔ **Strategic Alliances & Joint Ventures** : While not generally prohibited, joint ventures between SK hynix and a competitor can run the risk of violating the anti-trust laws because it creates an opportunity for competitors to exchange competitively sensitive information. Prior to discussing a potential strategic alliance or joint venture with any competitors, employees must obtain approval from their supervisors.
- ✔ **Speaking Engagements** : Prior to speaking at an event where competitors will be in attendance, employees must obtain approval from their supervisor by submitting an outline of the proposed speech. Such speeches should not include any competitively sensitive information.
- ✔ **Lobbying** : Although SK hynix has the right to petition governments, such petitioning can violate the anti-trust laws if its purpose is to unreasonably restrain competition. Employees should not make fictitious statements about competitors to government officials. Government participation does not necessarily preclude a violation of the anti-trust laws.

05

Unilateral Conduct That Could Unreasonably Restrain Trade

An anti-trust violation does not require the direct involvement or cooperation of another party. The anti-trust laws also place limitations on unilateral conduct if it will unreasonably restrain competition or involve “predatory” conduct by a party with dominant market power. The anti-trust laws generally prohibit the illegal monopolization or the attempt to illegally monopolize a product or service.

The following are the primary examples of predatory conduct that may violate anti-trust laws if a company has a monopoly in a market :

- ✔ Tying occurs when a party refuses to sell a product that a customer wants to purchase unless the customer also purchases another product that the customer does not want or would rather purchase separately or from another party. While coupling products is not necessarily illegal, it does raise anti-trust concerns.
- ✔ While refusing to deal with a particular supplier or customer is generally allowed under the anti-trust laws, it can present an anti-trust concern if it has the effect of preventing the supplier or customer from dealing with one of SK hynix's competitors (e.g., refusing to deal with a customer if the customer deals with a competitor of SK hynix). Refusing to deal can also present anti-trust concerns where the refusal lacks any objective justification and significantly impairs competition in the downstream market.
- ✔ Below-cost pricing is a form of predatory pricing and occurs when a company uses pricing that is below its costs in order to drive out competitors and, after successfully driving out competitors, increases prices to above-market levels in order to recoup its losses.
- ✔ Antidumping laws prohibits predatory pricing and price discrimination. Dumping occurs when a company sells a product in a foreign market at a price that is less than its normal value, which can often be defined by the price for which the product is sold in its home market. The antidumping laws also prohibit below-cost pricing. If such pricing is deemed to materially injure an industry in the foreign market or to present a threat of such an injury, then the product can be subjected to an antidumping duty in an amount that is equal to the difference between the actual price and the normal value of the product.

06

Collaboration Among Competitors

In many courts and anti-trust enforcers recognize that competitor collaborations can be, and often are, precompetitive and efficiency-enhancing. However, collaborations between competitors may create opportunities for unlawful collusion, increase the firms' market power, limit the firms' independent decision-making authority, or otherwise cause or facilitate competitive harm, all of which are prohibited by anti-trust agencies and courts. Anticompetitive collaborations may involve agreements to produce, market, purchase, research, and develop. Therefore it is crucial that the parties to collaboration ensure: 1) that the collaboration is indeed combination of complementary technologies, expertise, or other assets; 2) that each firm's independent decision-making authority is maintained; 3) that improper communications and disclosures are guarded against; 4) that the collaboration's activities are not unduly exclusionary; and 5) that the arrangement does not undermine the incentive or ability of either firm to compete.



07

Violation of Anti-trust Laws

Violation of anti-trust laws, or this Anti-trust Policy is a serious matter and can result in criminal or civil penalties against SK hynix and the individual involved in the violation, as well as harm to SK hynix's reputation. It can also result in debarment from selling to the government. Employees, officers, directors, or others involved in a violation will be subject to discipline, up to and including termination. Any violation of law or this Anti-trust Policy may result in a loss of incentive compensation, stock options, bonuses, or other awards, to the extent permitted by law.

All employees have a duty to report violations or suspicious circumstances that might indicate a possible violation of law or this Anti-trust Policy to Global Compliance Team. Employees MUST report all suspicious conduct, and must not delay such a report merely because the employee is not sure whether sufficient "proof" of a violation exists. Often reports of suspicions, made early enough, will allow the Company to intervene in a timely manner to prevent an actual violation from occurring.

Employees, managers, or other individuals must submit reports to the Global Compliance Team. Any manager or other individual who receives a report of a violation or a possible violation must promptly forward it to the Chief Compliance Officer or the Global Compliance Team and must refrain from conducting any independent investigation. SK hynix will not tolerate retaliation against any individual who submits a good faith report of a violation or possible violation of law or this Anti-trust Policy. Any employee who is the target of retaliation should promptly report it to the Chief Compliance Officer or the Global Compliance Team.

08

Questions

Questions regarding how to comply with this Anti-trust Policy should be directed to your direct supervisor, manager or the Global Compliance Team.



03 Anti-Corruption



Anti-corruption

01

Purpose

SK hynix and its subsidiaries are committed to competing ethically and complying with all anti-corruption laws in the countries where it does business. No one—either employees or others acting on SK hynix’s behalf—is permitted to offer, accept, request, promise, or pay a bribe or to make any improper payment to further SK hynix’s business.

Violation of any anti-corruption laws such as the U.S. Foreign Corrupt Practices Act, UK Bribery Act, or South Korea’s Act on Combating Bribery of Foreign Public Officials in International Business Transactions can have severe consequences for both SK hynix and for the person involved in the violation. Violations can lead to fines and imprisonment for individuals and severe financial penalties and losses of business for SK hynix.

If the respective local anti-corruption laws or policy imposes stricter requirements or adopts stricter standards, then such stricter local requirements or standards must be observed.

This Anti-corruption policy (“Anti-Corruption Policy”) contains important information to help employees comply with anti-corruption laws and to prevent, detect, and respond to anti-corruption issues should they arise. All SK hynix employees, officers, directors, and agents (defined below) must :

- ☑ Read, comply with, and understand how this Policy applies to their job functions;
- ☑ Ask their direct supervisor, manager, Ethics Management Group, or the Global Compliance Team for guidance when they are uncertain about how to comply with this Anti-Corruption Policy;
- ☑ Complete all required training and certifications related to this Anti-Corruption Policy; and
- ☑ Report violations or potential violations of this Policy as described in SK hynix’s Code of Business Conduct and Ethics (the “Code”).

SK hynix managers must also :

- ☑ Ensure that members of their team understand and comply with this Anti-Corruption Policy;
- ☑ Ask the Global Compliance Team or Ethics Management Group for guidance if they are uncertain how to implement this Anti-Corruption Policy in their area of responsibility; and
- ☑ Promptly forward reports of violations or potential violations to the Ethics Management Team

02



Acceptance or Provision of Bribes

Bribery & Corruption Generally

SK hynix's rule about corruption is simple : **WE NEVER PAY, PROMISE, OFFER, DEMAND, ACCEPT, OR PROMISE TO ACCEPT BRIBES OR ACT CORRUPTLY, OR ALLOW SUCH ACTIONS TO BE DONE FOR US BY SOMEONE ELSE. EMPLOYEES, OFFICERS, DIRECTORS, MANAGERS AND AGENTS ACTING ON BEHALF OF SK HYNIX MUST NEVER OFFER, AUTHORIZE, PROMISE, DEMAND, ACCEPT, OR PROMISE TO ACCEPT A BRIBE OR ANYTHING OF VALUE OR TAKE ANY CORRUPT ACTION ON SK HYNIX'S BEHALF.** For example, providing, demanding or accepting gifts, meals, tickets to sporting events, and other entertainment to or from our business partners can be viewed as a bribe if they are offered for the purpose of influencing the recipient's independent business judgment.

- ✔ A bribe is any benefit (regardless of its form or value), tangible asset (e.g. securities, other property including any property rights) or other advantage (e.g. gratuitous rendering of services, release from obligations) made or offered to influence improperly a decision-maker (or someone who may exert influence with regard to business decisions) or to obtain a business advantage through means other than fair competition and legitimate, transparent conduct.
- ✔ Anything of value is a broad term and includes anything with objective or subjective value, such as cash, entertainment, promises of future employment, or charitable contribution. Anti-corruption laws focus on the intent underlying a benefit, not on the size or value of the benefit itself. Thus, even a small gift, informal meal, or occasional ticket to a sporting event can be improper if it is given with the intent to influence the recipient.
- ✔ An act is corrupt if it is performed to secure an improper advantage, either by paying a bribe or through other means. Corrupt intent can also be inferred if an act is done secretly, steps are taken to disguise the act, or if the action is taken contrary to company policy, such as delegations of authority. The corrupt action need not be completed or successful to violate the law or this Anti-Corruption Policy.
- ✔ An agent is any consultant, distributor, joint venture partner, contractor or other third party who acts formally or informally to further SK hynix's business interests. This includes a party who makes business contacts for SK hynix, a party who sells SK hynix's products, a customs broker or freight forwarder, or any other person or entity who interacts with government entities or officials.

Bribery of all forms is prohibited. This includes corrupt activity among private sector actors, such as an employee of one privately owned business paying a kickback to an employee of another private company, as well as the bribery of public officials. Particular vigilance is necessary when interacting with government entities or officials.

- ✔ The term government entity refers to any :
 - legislative, executive, administrative or judicial bodies (national and local);
 - public international organization;
 - department, agency, or instrumentality (i.e., an entity owned or controlled by a government such as a state-owned manufacturer or university) of such a government or organization;
 - political party;
 - company or entity owned or controlled by or acting on behalf of any of the above.
- ✔ A government official is any individual working for or on behalf of a government entity. Examples include a foreign customs official; an inspector from a tax, health, or environmental agency; a journalist employed by a state-owned media company; a professor or researcher at a state-owned university; and an executive at a state-owned entity. Employees of state-owned manufacturers with which SK hynix maintains a business relationship also qualify as government officials.

Conducting Business with Individuals Related to SK hynix Employees

While SK hynix respects rights of its employees' personal business affairs, the Company prohibits certain business activities of its employees. SK hynix employees may not proceed with a transaction with the Company under the name of the Interested Persons ("Interested Persons") unless such transaction is preapproved by the Company pursuant to the Company's internal procedures. For the purpose of this section, Interested Persons shall mean any person or persons whose rights or benefits are influenced by certain actions although he is not directly involved with such actions. Beneficiary ("Beneficiary") shall refer to an individual or group whose rights and benefits can be influenced directly or indirectly through SK hynix employees' conducting duties at work.

First, Interested Persons may not jointly acquire any assets (including without limitation condominiums, country club memberships, joint venture business, etc.) with a Beneficiary. Regardless of whether an asset was obtained under a disguised name, if such asset is virtually owned by such Interested Persons and the beneficiary, the asset shall be deemed to have been jointly acquired by the Interested Persons and the Beneficiary for the purpose of this section. Second, SK hynix employees or Interested Persons may not borrow money from a Beneficiary, lend a property to a Beneficiary, lease any real estate to a Beneficiary or accept any property from a Beneficiary, from which all of the involved parties may gain financial advantage. Third, SK hynix employees or Interested Persons may not request or promise future employment.



Relatives, Friends & Colleagues of Government Officials

Making payments to relatives, friends, or colleagues of a government official to improperly influence the individual with whom the recipient is affiliated is a type of corruption and is prohibited. This includes the hiring of relatives of government officials with the hope of influencing a decision of a government official, or even offering an unpaid internship to such a relative. Any proposed hiring of a relative of a government official should be reviewed with your Human Resources representative and the Ethics Management Team.

Hosting & Gifts for Government Entities & Officials

Employees may appropriately provide hosting or gifts to government entities or officials while performing their duties for SK hynix provided that they are not exchanged for an improper purpose.

•••

- ✓ Hosting refers to anything of value provided to another individual by SK hynix or its employees in connection with a business event. Examples include travel, lodging, meals, and tickets for entertainment (if a SK hynix employee will accompany the recipient to the event).
- ✓ A gift is any item of value given on SK hynix's behalf. Examples include gift baskets, items (such as golf balls or coffee mugs) imprinted with the SK hynix logo, and tickets for entertainment (if a SK hynix employee will not accompany the recipient to the event.)

Before providing hosting or gifts to government entities or officials, employees must ensure that the hosting or gift meets the minimum standards set forth in the Code and obtain written (e-mail correspondence is acceptable) preapproval from Ethics Management Team.

Employees may not use personal funds, regardless of whether they seek reimbursement from SK hynix, to provide hosting or gifts that do not comply with this Anti-Corruption Policy.

In some countries, local laws limit the ability of government officials to accept hosting or gifts or impose preapproval procedures on hosting and gifts. Employees must comply with any such laws when providing hosting or gifts, even if they impose stricter requirement than discussed in this Anti-Corruption Policy.

03

Charitable Contributions

A charitable contribution is any payment or other support given to a charitable organization or to a formal or informal entity organized to provide a public benefit. Charitable contributions help SK hynix generate goodwill and give back to the communities where it operates. Examples include donation of products to trade schools, sponsorship of educational events, and contributions in the form of cash or other in-kind donations.

Charitable contributions can present corruption risks, especially if a government entity or official controls or has influence over the organization that receives them. All charitable contributions made by SK hynix must be preapproved by the Global Compliance Team.

Local laws may contain additional regulation regarding charitable contributions. Employees must comply with any such laws when providing charitable contributions on SK hynix's behalf.

This Anti-Corruption Policy does not apply to any contribution given by employees on their own behalf using personal funds. Employees may not make contributions on SK hynix's behalf using personal funds.



04

Interactions with Government Entities & Officials

Employees may, at times, interact directly with government entities or officials while performing their duties for SK hynix. Employees may conduct transactions with a government entity without obtaining preapproval if the transaction is a routine government interaction.

A transaction is a routine government interaction if :

•••

- ✓ it involves the payment of taxes or fees, the purchase of goods or services, or a request that a government entity perform an action or refrain from doing so;
- ✓ the amount of payment (if any) is objectively calculated, such as by a predetermined fee schedule or a published tariff;
- ✓ the government entity is required to accept the payment or to provide the goods/services.

At no time, however, can payment for routine government interaction be made individually to a government official. Instead, payment must be made to the governmental entity, with all documentation related to the transactions showing that payment was rendered to the entity and not to any individual. Examples of routine government interactions include payment of taxes, patent registration fees, opening an account with a state-owned bank, and purchasing electricity from a state-owned utility.

Employees must obtain preapproval for all other transactions with government entities and all transactions with government officials by contacting the Ethics Management Team.

05

Third Parties

SK hynix may, at times, retain third parties to conduct business or perform services on its behalf. Examples of third parties include consultants, lawyers, distributors, accountants, raw material suppliers, lobbyists, logistics providers, visa processors, and public relations representatives.

Retention of third parties can pose corruption risks, especially when the third parties are likely to interact with government entities or officials on SK hynix's behalf. SK hynix and its employees may be held liable for bribery or other corrupt conduct performed by third parties regardless of whether SK hynix knew about or authorized the improper action.

SK hynix's interactions with government entities and officials should be conducted without relying on third parties whenever practical.

Third parties retained to act on behalf of SK hynix must be selected on the basis of their commercial and technical expertise and SK hynix's need for the products or services. No person or entity may be retained solely on the basis of a special relationship with a government official.

Third parties subject to review must certify that they have adopted a policy that sets forth standards consistent with the values described in SK hynix's Code, or that they will act in accordance with SK hynix's Code when acting on its behalf.

06

Facilitation Payments

A facilitation payment is a payment made to a government official in accordance with local custom for the purpose of securing or expediting a routine, nondiscretionary government action. Employees or others acting on SK hynix's behalf are not permitted to make facilitation payments.

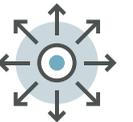
07

Joint Ventures, Mergers, Acquisitions & New Market Entry

SK hynix sometimes expands its business by launching new products, competing for new business, or entering a new geographic market. SK hynix may conduct these activities through joint ventures, mergers, acquisitions, or new market entries.

Joint ventures, mergers, acquisitions, and new market entries can all present corruption risks. SK hynix can be held liable for improper conduct by its joint venture partners or by a joint venture subject to its control. SK hynix can also be held liable for past bribery or corruption by a company that it acquires or merges with. New market entries can present concerns because SK hynix may not have prior experience with government regulations, local customs, or local business practices.

Before entering into a joint venture, completing a merger or acquisition, or undertaking a new market entry, employees must contact the Global Compliance Team, who will provide guidance about how to address anti-corruption aspects of the proposed transaction.



08



Books and Records & Related Internal Controls

Anti-corruption laws require SK hynix to maintain records that accurately reflect its business transactions. Employees who conduct transactions on SK hynix's behalf must ensure that all transactions (no matter how small) are recorded promptly and accurately, contain sufficient detail, and are supported by objective documentation. Such records must be retained as required by law and SK hynix's Document Management Policy. Please refer to the Document Management section below for further details.

09

Violation of this Policy

Violation of anti-corruption laws or this Anti-Corruption Policy is a serious matter. Violations can result in government investigations and criminal and civil penalties for SK hynix, as well as harm to the Company's reputation.

Employees, officers, or directors involved in a violation will be subject to discipline by SK hynix, up to and including termination of employment. Individuals may also incur criminal or civil penalties imposed by government authorities, such as investigation by government agencies, fines, criminal prosecution, and imprisonment. Any violation of law or this Anti-Corruption Policy may result in a loss of incentive compensation, stock options, bonuses, or other awards, to the extent permitted by law.

All employees have a duty to identify anti-corruption violations in their area of responsibility, and to report violations or suspicious circumstances that might indicate a possible violation of law or this Anti-Corruption Policy. Employees should report all suspicious conduct, and must not delay such a report merely because the employee is not sure whether sufficient "proof" of a violation exists. Often reports of suspicions, made early enough, will allow the Company to intervene in a timely manner to prevent an actual violation from occurring.

Employees should submit reports to their manager or the Ethics Management Team. SK hynix will not tolerate retaliation against any individual who submits a good faith report of a violation or possible violation of law or this Anti-Corruption Policy. Any employee who is the target of retaliation should promptly report it to the Ethics Management Team.

04 Supplier Management





Supplier Management

As a member of Electronic Industry Citizenship Coalition (“EICC”), SK hynix has adopted EICC Code of Conduct (the “Code”). We regard the Code as a total supply chain initiative requiring its next tier suppliers to acknowledge and implement SK hynix Supplier Management Policy which reflects the Code. All subcontractors engaging in business relationship with SK hynix must obtain qualification as a global company and work to satisfy our company and our customers by following the requirements given below.

01

Labor and Human Rights

SK hynix subcontractors must strive to create a work site that is completely free from illegal discrimination and harassment in its employment practices, and should have no unreasonable restriction, severe or inhumane treatment of workers. In addition, all work should be accomplished voluntarily without any forced labor such as slavery or trafficking of persons, and the freedom of working ages, working hours, wages and labor union memberships established by current laws and regulations should be provided.

02

Health and Safety

Subcontractors must remove all risk factors for industrial safety, take preventative measures to ensure safety, and provide appropriate individual safety equipment to workers in order to prevent exposure to risk factors. Also, damages should be minimized by establishing the appropriate countermeasures and response procedures. In addition procedures and systems to manage industrial disasters and work-related illnesses should be controlled in advance, and the safety risks of production facilities and other equipment should be evaluated.

03

Environment

Subcontractors should follow the environmental permit, reporting requirements, and environmental/quality management standards of our company. Furthermore, the related laws for solid waste, waste water and air pollutants should be obeyed, and efforts should be made to prevent environmental pollution and reduce resources use. Related laws or regulations on products containing certain regulated substances and all customer requirements should be obeyed.

04

Management System

Subcontractors should follow relevant laws, regulations, and customer requirements by selecting and establishing a management system. In relation to this, an expression of willingness to comply, clear management responsibility, compliance to relevant laws and regulations, recognition and monitoring of customer requirements, risk evaluation and management of ethics related to company management, goals and evaluation performance, training programs for related persons, and regular self-evaluation will be used to determine whether the subcontractors are following our business policy.

05

Legal Operation of Raw Materials

Subcontractors should clarify the source of raw materials distributed in the whole supply chain, and assure/manage that their products do not contain conflict minerals or their derivatives determined to be directly or indirectly financing or benefit armed groups in the DRC or an adjoining country (Sudan, Uganda, Rwanda, Burundi, United Republic of Tanzania, Zambia, Angola, Central African Republic etc.)

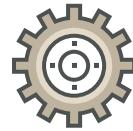
06

Ethics

Subcontractors doing business with our company should pursue free competition in business relationship, following all laws and regulations completely for all business activities, perform business by respecting the business customs, and work consistently to ensure that their businesses follow the laws of our fair trade compliance system.

Furthermore, various programs should be developed and performed for mutual promotion with the subcontractors. Mutual efforts are required to maintain ethical and fair business practices.

Subcontractors doing business with our company have an obligation to follow the above contents, and will be evaluated to ensure compliance. The contents may be changed to reflect the changing circumstances of the global business environment. Please refer to http://www.skhy-nix.com/ko/resources_buy/subcontractors.jsp for SK hynix Supplier Management Policy and contact the Global Compliance Team for any question.



05

Data Protection





Data Protection

Personal Information Privacy Protection Policy ("Personal Data Policy")

SK hynix and its subsidiaries have employees and customers in many jurisdictions worldwide, and is thus subject to a number of different data protection laws and obligations. We have adopted this Personal Data Policy to establish and maintain an adequate level of protection for Personal Information, as required by law. This Personal Data Policy sets the minimum applicable standards for the treatment of Personal Information received from any jurisdiction in which the Company operates and applies to all Company records (whether paper or electronic) containing Personal Information, whether held by the Company or by a service provider, contractor or other third party on behalf of the Company.

All Employees and Affiliates are expected to comply with the requirements in this Personal Data Policy and to adopt local policies and procedures to conform to this Personal Data Policy. This Personal Data Policy sets forth how Company will comply with its requirements related to Company's processing of Personal Information: including notice to data subjects, consent from data subjects where required, limits on the purposes for which Personal Information may be processed, data subjects' rights to access and amend Personal Information, reasonable security, and rules governing third party transfers of Personal Information.

Key Terms



- ✔ "Customer" means a prospective, current or former partner, vendor, supplier, customer, or client of the Company, and the term shall also include any individual agent, employee, representative, customer, or client of a Company Customer where SK hynix has obtained his or her Personal Information from such Customer as part of its business relationship with the Customer.
- ✔ "Employee" means any applicant for employment with the Company, or any current or former employee, contractor and other personnel of the Company, as well as their respective dependents and beneficiaries.
- ✔ "Personal Information" means any data that identifies or could be used to identify a natural person, including name, photos, contact information, government identification number, a unique identifier, and other information that alone or in combination with other data could be used to identify an individual, as well as any other data associated with such identifying data.
- ✔ "Sensitive Personal Information" includes any Personal Information relating to race, ethnicity, religion, trade union or party membership, sexual orientation, criminal history, medical history, or health information, or, in some countries, any Social Security number, financial account or credit card number, credit report/history, background check report, driver's license or other government identifier, biometrics, genetic information, login credentials.

01

Collecting Personal Information

Employees

SK hynix may process the Personal Information of its Employees and, in certain limited circumstances, their immediate family members in connection with normal and legitimate business activities and in order to administer the employment relationship. The Company has created and maintains databases that contain information about the Company's Employees (and, where applicable, their family members). Only the HR Department may collect Personal Information about Employees.

Customers and Suppliers

SK hynix provides services to businesses, not individual consumers. However, we collect information in the course of conducting our business operations or in furtherance of our legitimate business interests that may lead to the incidental collection of Personal Information, such as name, contact information and job position of certain employees of its business customers, or it may conduct business with sole proprietors.

02

Using Personal Information

The Company will limit the collection of Personal Information from Employees and Customers to the amount reasonably necessary to accomplish its business objectives, administer its employment relationships, and comply with applicable law; Company will not collect excessive or unnecessary Personal Information.



- ✔ Personal Information : The Company will only collect Personal Information as necessary to perform its legitimate business purposes, including to administer its customer and employment relationships and to satisfy legal obligations, or as otherwise permitted by applicable law or subject to Employees' consent.
- ✔ Sensitive Personal Information : The Company will limit its collection of Sensitive Personal Information, and will only collect and process Sensitive Personal Information as is reasonably necessary to perform a specific, legitimate employment-related function and as permitted or required by law. No Sensitive Personal Information will be collected from Customers. Company will obtain express consent before collecting any Sensitive Personal Information from EU data subjects.



Company will, generally, collect Personal Information directly from the individual data subject, and use as little data as possible to achieve the specific purpose for which the data were collected.

03

How Does the Company Notify Individuals of How it Collects, Uses and Discloses Personal Information?

In general, applicable privacy laws require SK hynix to provide notice of its information practices to data subjects. In furtherance of this requirement, SK hynix will publish and make available to individuals a privacy notice that informs them about the purposes for which it collects Personal Information.

- ☑ **Customers** : Company shall provide Customers a privacy notice by: (1) including applicable privacy language in customer contracts, and (2) posting a website privacy policy.
- ☑ **Employees** : Company shall provide Employees a copy of the applicable SK hynix Employee Privacy Notice. This Privacy Notice shall be included in hiring paperwork, and acknowledged by employees during the hiring process. It shall also be posted on the SK hynix intranet.

Company will use the information it collects in accordance with its applicable privacy notices. Employees will be notified of any material changes in the treatment of their information.

04

Sensitive Personal Information

Applicable laws strictly restrict Company's collection, use and disclosure of Sensitive Personal Information. Company will only collect Sensitive Personal Information where strictly necessary for a legitimate business purpose or where required by law. The Company will obtain consent from Customers and Employees before it collects and processes any Sensitive Personal Information. Unless Company has obtained express consent from relevant data subjects, Company will not use any Personal Information for marketing purposes.



05

Monitoring

Employee's use of Company information resources is subject to the SK hynix's internal policy. Provided that adequate notice has been provided and consent obtained from Employees, Company may monitor Company-owned resources in accordance with its applicable monitoring policy, subject to any limitations imposed by applicable local laws.

Company premises may be subject to closed circuit television (CCTV) monitoring, provided (i) notice is prominently posted where the monitoring occurs and employees have been notified of the CCTV monitoring by way of the Employee Privacy Notice, (ii) no monitoring occurs in private places such as restrooms and changing rooms or other places as restricted by applicable law, and (iii) where required by applicable law (such as in certain EU jurisdictions) the local Company Affiliate has notified its CCTV activities to the data protection authority.



06

Protection of Employees' Personal Information

Data subjects have the right to know what information about them is included in the databases and to ensure that such information is accurate and relevant to the purposes for which the Company collected the data. Data subjects will be notified of this right in the applicable privacy notice. Upon request, individuals will be permitted to review their own Personal Information stored by the Company, and to correct, erase, or block any data that is incorrect. Each Affiliate is responsible for tracking requests received from the identified subject of the Personal Information in order to ensure such requests are handled and responded to appropriately and as required by law.

Employees with responsibilities for data security and information management are trained at least annually by the Corporate Security Team.

All Employees will receive training on acceptable use of company resources and data protection obligations that are relevant to the employee's position and duties within the Company. Training will include the proper use of the computer security system and the importance of Personal Information security.

In addition, all Employees are asked to sign a confidentiality agreement or privacy pledge, agreeing to protect Personal Information held by Company.

SK hynix has implemented safeguards to protect the Personal Information it accesses, processes and stores, in accordance with applicable laws and standards. As part of its information

security program, Company will maintain, monitor, test, and upgrade information security policies, practices, and systems to assist in protecting the Personal Information that it collects, in accordance with applicable laws on employee monitoring. The Corporate Security Team and their designee(s) will regularly evaluate the effectiveness of the SK hynix program, and will recommend changes, as appropriate. As part of the Company's ongoing risk assessment, the Company will review and identify whether any new Employee, Customer, product, or database triggers any new risks. In addition, SK hynix will review any security incidents to determine whether the Company should revise existing procedures to prevent the recurrence of such an incident.

In order to protect SK hynix information and information assets that are managed or accessed by each Affiliate, each Affiliate is responsible for adopting and implementing procedures that comply with the requirements set forth in the SK hynix corporate security policies and with applicable local laws.

SK hynix retains Personal Information for as long as reasonably necessary for the purposes for which such Personal Information were collected, or as otherwise required by applicable law or subject to a legal hold. Applicable retention periods shall be set forth in the in a written retention policy and schedule.

Once the retention period has expired, Personal Information shall be securely deleted unless such Personal Information must legally be maintained for an additional period of time, is subject to a legal hold, or is approved by General Affairs Team, HR Department, or Corporate Security Team to be retained for an additional period of time.

Paper records containing Personal Information must be destroyed in a way that makes it impossible to reconstruct the data, such as by shredding and incineration. Electronic data, media or files containing Personal Information shall be destroyed in a way that makes the information impossible to recover.

Any time a third party is engaged to securely destroy any Personal Information, whether in paper or electronic form, on behalf of the Company, a data processing contract will be put in place, which complies with the requirements for data transfers and third party service providers (see below) and the Company will obtain a certificate of destruction from such third party.

07

Destruction of Personal Information

Paper records containing Personal Information must be destroyed in a way that makes it impossible to reconstruct the data, such as by shredding and incineration. Electronic data, media or files containing Personal Information shall be destroyed in a way that makes the information impossible to recover.

The Corporate Security Team will maintain a written inventory of the databases that it maintains, which may contain Personal Information about Customers and Employees, and the purpose for which it maintains such database. In addition backups of all Company systems are maintained onsite by SK hynix in Korea, in a separate location from the live database and servers.

Each Affiliate is responsible for maintaining a written inventory of any databases that it maintains locally, as set forth above, and for establishing appropriate backup and disaster recovery procedures.

Company Employees and service providers may access and use Personal Information only if (i) they have a legitimate business need to know the information, (ii) are authorized to do so, and (iii) only access it for the purpose for which they are authorized. Furthermore, each Affiliate (and its personnel) shall have access only to Personal Information related to that Affiliate's Employees and Customers, except as expressly noted herein. An Affiliate may access and process the Personal Information belonging to another Affiliate in its capacity as a service provider or data processor to the Affiliate who is the data controller of such Personal Information provided that Affiliates have entered into a written agreement governing the processing that complies with the rules herein regarding data transfers and third party service providers (see below).

The Corporate Security Team is responsible for administering Employee access to Company information systems, subject to the approval of the Employee's supervisor.

08

Third Party Request for Access to Personal Information

Company will track each of the following and will provide notice to the appropriate parties under law and contract when it receives any legally binding request for disclosure of the Personal Information by a law enforcement authority or other third party, unless prohibited by law or regulation. Each local Affiliate shall be responsible for managing any such requests received by that local Company Affiliate, and shall notify the Global Compliance Team when appropriate.



09

Employees' obligations to Cooperate with Data Protection Authorities

The Company may be subject to regulatory reviews and audits with respect to its compliance with applicable privacy and security laws. Employees are expected to cooperate with such authorities where directed to do so by the Company, and to notify Global Compliance Team of any such reviews or audits.

All Company Employees have an obligation to be vigilant in safeguarding Employee and Customer privacy and Personal Information. Company personnel must immediately report any actual or suspected Data Breach to their immediate supervisor and the Corporate Security Team.

10

Data Transfers and Third Party Service Providers

Personal Information in Company databases may be processed outside the country in which it was collected, for legitimate business activities as described under national and/or regional law in the country in which the Company collected the data, as long as (1) data subjects have been notified of the possibility that their data may be transferred, and where required by applicable law have consented; (2) the Company has in place the appropriate written contract with any third party or group company, as required by law; and (3) where Personal Information will be transferred outside the European Economic Area to a jurisdiction that does not have adequate data protection laws as recognized by the European Commission, additional steps are taken such as the execution of EU Standard Contractual Clauses.

Notwithstanding the foregoing, when the Company engages a service provider/vendor to perform activities that may require access to Personal Information, it will take steps to ensure that the service provider acts in accordance with Company's existing policies and procedures and applicable laws. At a minimum, the Company will enter into a written agreement with the third party requiring the third party (1) to comply with all applicable laws, (2) maintain the confidentiality of all Company data including any Personal Information, (3) to have in place appropriate security measures and to maintain secure systems in the transmission of information to and from the Company; and (4) to notify Company of any Data Breach. With respect to transfers of Personal Information amongst SK hynix group companies, SK hynix has implemented an intragroup data transfer agreement to govern transfers of Personal Information amongst group companies.

11

Known or Suspected Data Breaches

The Company will track any loss or accidental or unauthorized access to, disclosure of, and use of Personal Information a ("Data Breach"). Each Company Affiliate is responsible for tracking and responding to Data Breaches as required by applicable law and contractual requirements, and notifying the Company's Corporate Security Team where the Data Breach involves Company's corporate information systems or databases, or any Personal Information contained therein.

Upon notification of an actual or suspected Data Breach, the Company's Corporate Security Team, in consultation with the Global Compliance Team, the Legal Team, the local Company Affiliate whose data was impacted, and other relevant departments and personnel, will investigate the suspected Data Breach to determine, where possible (1) whether a breach occurred, (2) the personal data and individuals affected by the breach, (3) the source of the breach, (4) whether any misuse of data has occurred or is likely to occur, and (5) the appropriate steps to mitigate and remediate any harm, and to prevent a reoccurrence of such incident.

Company management will confer with internal and/or external counsel to determine legal and contractual obligations relating to such breach, and, if required, will provide notice of the data breach to the appropriate parties under law and contract. Company management will evaluate whether any changes to its procedures and policies should be made as a result of the breach.

12

Resolving Complaints

Company is committed to cooperate in good faith to remedy any breach of a data subject's third party rights under this Personal Data Policy. Employees that have a complaint may contact the Corporate Security Team. Employees may also contact their local HR department or supervisor to report any complaints. Company will respond to all complaints it received from Employees and Customers, and will maintain a record of such complaints and the steps Company took to respond to such complaints.



13

Overseeing the Company's Information Security Program

The Company has designated its Corporate Security Team to manage and oversee the Company's information security program. The Corporate Security Team may designate certain activities and obligations, where appropriate, to other Company Departments and certain designated employees. The Corporate Security Team or their designee(s) will review and approve any material changes to the Company's information security policies.

Corporate Security Team will oversee and approve any material changes to this Personal Data Policy. Corporate Security Team will consult with the appropriate Company departments and employees as necessary when approving any changes to this Personal Data Policy. In addition, where required by applicable law, each local Company Affiliate shall appoint a data protection officer to manage that Affiliate's compliance with this Personal Data Policy, privacy notices and applicable privacy rules.



Data Protection

Customer Privacy Policy

SK hynix values our customer's privacy. In this section, we describe how we collect, use, and disclose personal information that we receive about current and future customers, including through our websites (each a "Site").

01

Information We Collect

Business Contact Information

We may collect name, email, phone and other contact information, company name and title, as well as other related information from our business contact persons.

Other Information We Collect Directly From Our Customers

We collect information directly from our customers when you provide it to us. The information we collect may include name, phone number, email address, address, and business information of our customers. For example, we collect our customers' name, business contact information and email address if you contact us through our Site. We may also collect our customers' information when they make a purchase from us, on behalf of your company or employer, or send us an email.

Information We Collect Automatically

We may automatically collect information about our customers' use of our Site or services through cookies, web beacons, and other technologies. The information that we automatically collect includes the following: customers' domain name; customers' browser type and operating system; web pages that customers view; links that customers click; customers' IP address; the length of time that customers visit our Site and or use our services; and the referring URL, or the webpage that led customers to our Site. We may combine this information with other information that we have collected about customers. Please see the section "Cookies and Tracking Mechanisms" below for more information.

02

Using Customer Information

We use information we receive about customers for the following purposes :

- ✎ For customer service purposes, including to fulfill orders or respond to inquiries.
- ✎ For marketing and promotional purposes, if customers have consented. For example, we may send customers news and newsletters, special offers, and promotions, or to otherwise contact customers about products or information we think may interest our customers.
- ✎ For research and analytical purposes, including to better understand our customers, both on an aggregated and individualized basis, and to improve our services, products, and Site.
- ✎ As required by law.

03



Sharing Our Customer Information

We may share the information we receive about our customers. With our customers' consent and/or subject to and in accordance with the terms and conditions of any and all agreements we executed with our customers, we may disclose our customers' information 1) to our affiliates, subsidiaries, service providers, etc; 2) in the event of M&A or bankruptcy proceeding; 3) as required by law; 4) to protect us and others where we believe it is necessary to prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, or as evidence in litigation in which SK hynix is involved; or 5) as de-identified or aggregate form for marketing, advertising, researching, or other purpose.

04

Information Collected Automatically : Cookies and Tracking on our Website

We and our service providers use cookies and other tracking mechanisms to track information about our customers' use of our Site or services. We or our service providers may combine this information with other information we have received about our customers.

- ✎ Do-Not-Track : Currently, our systems do not recognize browser "do-not-track" requests and we do not track visitors to our Site after they leave our Site. Our customer may disable certain tracking as discussed in this section (e.g., by disabling cookies).
- ✎ Cookies : Our Site uses cookies. A cookie is a text-only string of information that a website transfers to the cookie file of the browser on your computer's hard disk so that the website can remember who you are. A cookie will typically contain the name of the domain from which the cookie has come, the 'lifetime' of the cookie, and a value, usually a randomly generated unique number. This helps us to provide our customers with a good experience when they browse our Site and helps us improve our Site and services. We may use cookies in the following ways:
 - Where they are essential to make our Site work.
 - To compile anonymous, aggregated statistics that help us to understand how customers use our Site and to help us improve the structure of our Site.
 Our customers have the ability to accept or decline cookies by modifying the settings in their browser. However, our customers may not be able to use all the interactive features of our site if cookies are disabled.
- ✎ Clear GIFs, pixel tags and other technologies : Clear GIFs are tiny graphics with a unique identifier, similar in function to cookies. In contrast to cookies, which are stored on your computer's hard drive, clear GIFs are embedded invisibly on web pages. We may use clear GIFs (a.k.a. web beacons, web bugs or pixel tags), in connection with our Site to, among other things, track the activities of Site visitors, help us manage content, and compile statistics about Site usage. We and our third party service providers also use clear GIFs in HTML e-mails to our customers, to help us track e-mail response rates, identify when our e-mails are viewed, and track whether our e-mails are forwarded.
- ✎ Third Party Analytics : We use automated devices and applications, such as Google Analytics, to evaluate usage of our Site. We also may use other analytic means to evaluate our services. We use these tools to help us improve our services, performance, and user experiences. These entities may use cookies and other tracking technologies to perform their services. We do not share your personal information with these third parties.

Google Analytics is a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses cookies, which are text files placed on your computer, to help the website analyze how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. In case of activation of the IP anonymization, Google will truncate/anonymize the last octet of the IP address for Member States of the European Union as well as for other parties to the Agreement on the European Economic Area. Only in exceptional cases, the full IP address is sent to and shortened by Google servers in the USA. On behalf of the website provider Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage to the website provider. Google will not associate your IP address

with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser. However, please note that if you do this, you may not be able to use the full functionality of this website. Furthermore you can prevent Google's collection and use of data (cookies and IP address) by downloading and installing the browser plug-in available under <https://tools.google.com/dlpage/gaoptout?hl=en-GB>.

Further information concerning the terms and conditions of use and data privacy can be found at

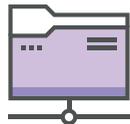
- ➔ <http://www.google.com/analytics/terms/gb.html>
- ➔ https://www.google.de/intl/en_uk/policies/

05

Third-Party Links

Our Site and services may contain links to third-party websites. Any access to and use of such linked websites is governed by the privacy policies of those third-party websites only. We are not responsible for the information practices of such third-party websites.

06



International Transfers

We may process information we have received about our customers outside the country in which it was collected. For example, any information we collect about our customers may be transmitted to, processed and stored in South Korea, where SK hynix is based, and the United States or other jurisdictions in which we have affiliates and service providers. These jurisdictions may not have equivalent data protection laws to those of our customers' home jurisdictions. Our customers expressly consent to our transfer of their personal information as described in this section.

07

Security of Customers' Information

We have implemented physical and technical safeguards to protect Personal Information from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. Please be aware that despite our best efforts, no data security measures can guarantee 100% security.

08

Access to Customers' Personal Information

Our customers may modify personal information that they have submitted to us. Please note that copies of information that our customers have updated, modified or deleted may remain viewable in cached and archived pages of the Site or Application for a period of time.

09

Choices Regarding Customers' Personal Information

With our customers' consent, we may send periodic promotional or informational emails to them. Our customers may opt-out of such communications at any time, by following the opt-out instructions contained in the e-mail. Please note that it may take up to 10 business days for us to process opt-out requests. If our customers opt-out of receiving emails about recommendations or other information we think may interest them, we may still send them e-mails about their account or any Services they have requested or received from us.

10

Data Controller

The data controller for the personal information collected on our Sites is SK hynix, Inc.; the data controller for the information collected offline is the SK hynix group company with whom our customers have a business relationship.

06

Conflict Minerals



Conflict Minerals

SK hynix and its subsidiaries are committed to establishing fair trade practices and creating an open and clean company culture which fulfills social responsibility. Certain conflict minerals mined from the Democratic Republic of Congo or its adjoining countries (the “DRC Countries”) can be a source of financing for armed groups perpetrating human rights violations in those regions and can make their way into the supply chains of products used around the world, including those in the electronics industry. In recent years, it has become a global concern that, by using conflict minerals sourced from the DRC Countries, companies could be inadvertently financing conflict in those regions. As part of its commitment to fair trade practices, SK hynix for itself, by virtue of its membership in the Electronic Industry Citizenship Coalition (“EICC”), and to better serve our customers who are subject to laws governing the use of conflict minerals, has determined to practice responsible sourcing of conflict minerals by creating an internal policy with respect to conflict minerals sourcing (the “Conflict Minerals Policy”).

EICC standards and laws governing conflict minerals do not presently ban or impose a penalty on conflict minerals sourced from the DRC Countries. Rather, regulators and the EICC require supply chain diligence and public disclosure, which presents a reputational risk to companies that use conflict minerals. It is the goal of SK hynix to use conflict minerals that are responsibly sourced, making sourcing decisions based upon supply chain due diligence and providing the supply chain information that customers request from us, thereby preserving the Company’s hard-earned reputation for social and environmental integrity.

The Conflict Minerals Policy contains important information to help employees comply with the applicable conflict minerals requirements found in the EICC Code of Conduct (the “EICC Code”), EICC conflict minerals guidance, the Organization for Economic Co-operation and Development (“OECD”) Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected High-Risk Areas (the “OECD Guidelines”), and the SEC Conflict Minerals Rules (defined below), collectively referred to in the Conflict Minerals Policy as the “Conflict Minerals Guidance.” The Conflict Minerals Policy uses the term employee(s) to refer collectively to all individuals and entities to which it applies.

Compliance with the Conflict Minerals Policy is mandatory. All SK hynix employees, officers, directors, and agents must read, comply with, and understand how the Conflict Minerals Policy applies to their job functions and ask their direct supervisor, manager, or the Global Compliance Team for guidance when they are uncertain about how to comply with the Conflict Minerals Policy. SK hynix managers must also ensure that member of their team understand and comply with the Conflict Minerals Policy, ask their direct supervisor or the Global Compliance Team for guidance if they are uncertain how to implement the Conflict Minerals Policy in their area of responsibility, and promptly forward reports of violation or potential violations to relevant team or Global Compliance Team.

Key Conflict Minerals Terms



- ✓ The conflict minerals are Tantalum, Tin, Tungsten and Gold — often referred to as the 3TGs.
- ✓ A smelter is an entity that uses heat and chemical agents to produce metal from an ore.
- ✓ A refiner is an entity that purifies a material—in this case, a metal—to create a final material that is chemically identical to the original material, only purer.
- ✓ The Democratic Republic of Congo is sometimes referred to as the DRC. The term adjoining country refers to the countries that are adjoining the DRC and share an internationally recognized border with the DRC. These are presently Angola, Burundi, Central African Republic, the Republic of Congo, Rwanda, South Sudan, Tanzania, Uganda, and Zambia (collectively, with the DRC, the DRC Countries).
- ✓ Regulators (particularly in the United States and in the European Union) and organizations (including the EICC) have raised concern that, by sourcing conflict minerals from the DRC Countries, in which conflict minerals can be a source of financing for armed groups, companies are inadvertently contributing to conflict in the DRC Countries. Generally speaking, an armed group is a militant group causing serious social and environmental issues in a region, including by perpetrating violence over the control and taxation of conflict minerals resources, serious human rights abuses, and forced and child labor.

01

Conflict Minerals Rules in General

Conflict minerals are commonly found in electronics and semiconductor products, such as those manufactured and sold by SK hynix. It is the policy of SK hynix to comply fully with both the letter and spirit of the applicable conflict minerals requirements found in the Conflict Minerals Guidance.

The EICC is an industry group committed to developing standards on social, environmental and ethical issues in the electronics industry supply chain. As a member of the EICC, SK hynix follows the EICC Code, which requires EICC members to: (1) adopt a conflict minerals sourcing policy; (2) exercise due diligence on the source and chain of custody of conflict minerals in their supply chain; and (3) make such due diligence measures accessible to customers upon request. The EICC recommends that its members use the OECD Guidelines as a mechanism for compliance with the conflict minerals supply chain due diligence requirements of the EICC Code.



Some SK hynix customers are subject to laws of the United States that require them to disclose whether any conflict minerals extracted from the DRC Countries are used in their products, and if so, to disclose, among other matters, the measures taken to exercise due diligence on the source and chain of custody of those minerals. These laws are Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the “Dodd-Frank Act”) and Section 13 (p) of the Securities exchange act of 1934, the rules developed by the United States Securities and Exchange Commission (the “SEC”) to implement the Dodd-Frank Act (the “SEC Conflict Minerals Rules”). Although SK hynix is not directly subject to the Dodd-Frank Act or the SEC Conflict Minerals Rules, some SK hynix customers are, and they rely on SK hynix to conduct due diligence on its supply chain and provide information about the Company’s due diligence measures so that they may fulfill their obligations under those laws.

For these reasons, SK hynix conducts conflict minerals supply chain due diligence in accordance with the EICC Code and OECD Guidelines (which incorporate many aspects of compliance with the SEC Conflict Minerals Rules). Requirements of the Conflict Minerals Policy apply to all SK hynix business units and products worldwide. SK hynix will oversee the implementation of the Conflict Minerals Policy and will ensure compliance with the Conflict Minerals Policy, as well as compliance with the Conflict Minerals Policy statement found in the SK hynix Supplier Code of Conduct. SK hynix is considered a “downstream” company since it does not directly interact with smelters or refiners. As such, our diligence is mostly focused on ensuring the transparency of the supply chain down to the smelters or refiners.

02

Responsibility and Authority

In order to implement regulations/laws enforced by various international organizations, to conform to and satisfy global standards, and to abide by all of SK hynix regulations and customer requirements, SK hynix has numerous departments to monitor our compliance with the policies and regulations.

In managing overall performance of conflict free minerals systems within the Company, Quality Assurance Department reviews and responds to different requirements of conflict minerals, controls the raw materials and product data base, operates verifications systems for conflict minerals in all relevant departments within the Company, communicate information regarding conflict minerals regulations and customer requirements to relevant teams, responds to customer regarding their requirements, etc.

We also have teams such as Customer Satisfaction Team to respond to various customer inquiries and requests with respect to procurement of non-conflict minerals. SK hynix Procurement Team not only procures conflict free minerals but also is responsible for acquiring information on the origin of the raw materials procured by the Company. Our Global Compliance Team supports the Procurement Team in auditing the raw material suppliers, informs SK hynix's policies and guidelines regarding conflict free minerals and any modifications/revisions thereof, and responds to national and international SR evaluation requests. Our Marketing Department directly communicates with customer must understand SK hynix Conflict Minerals Policy as well as the Company's status and verification system with respect to conflict free minerals and communicate customer's requirements promptly, clearly, and responsibly to relevant teams within the Company. Our Legal Teams and Global Compliance Team provide consultation for any legal issues regarding conflict free minerals, settle any dispute, and review any document signed or to be signed by SK hynix.

The main topics with respect to SK hynix conflict minerals management system discussed here are Product Identification, Conflict Minerals Procurement, Supply Chain Due Diligence, Conflict Minerals Data Management System, and Customer Conflict Minerals Request.

03

Product Identification

Our Quality Assurance Team will identify the products that it manufactures or contracts to manufacture that both contain conflict minerals and for which conflict minerals are necessary to such products' "functionality" or "production," as such terms are defined in the SEC Conflict Minerals Rules. SK hynix will lead an initial assessment, as well as periodic assessments, to determine which products contain conflict minerals. All SK hynix business units purchasing materials and components and/or fabricating, manufacturing, or subcontracting out hardware activities must assess their materials and components to determine whether they are affected by the rules set out in the Conflict Minerals Policy. SK hynix will aggregate the data from these assessments so that the findings can be communicated to the appropriate SK hynix teams.



04

Conflict Minerals Procurement

All purchases of conflict minerals or products containing conflict minerals on behalf of SK hynix that may then be incorporated into products sold by SK hynix must be identified and approved, including, but not limited to:

- ✓ the types and quantities of conflict minerals intended to be purchased;
- ✓ if applicable, a description of the products containing conflict minerals intended to be purchased, including the amount of the conflict minerals contained therein;
- ✓ the type and the amount of the product sold by SK hynix that will contain the conflict minerals;
- ✓ the name and address of the supplier from whom these conflict minerals or products containing conflict minerals will be purchased; and
- ✓ the country of origin from which these conflict minerals, including the conflict minerals contained in any product purchased by SK hynix, were sourced.

To ensure that SK hynix does not manufacture or produce products containing improperly sourced conflict minerals, SK hynix will not, subject to its reasonable discretion, approve the purchase of any conflict minerals or products containing conflict minerals without first receiving the following from the supplier :

- ✓ the identity of the smelter that processed the conflict minerals;
- ✓ written certification that the conflict minerals did not originate in the DRC Countries or came from recycled or scrap sources; and
- ✓ documentation that (a) the smelter has received a "conflict-free" designation by a recognized industry group that requires an independent private sector audit of the smelter or (b) the smelter itself has obtained an independent private sector audit that is made publicly available.

Copies of all documentation associated with SK hynix's purchase of conflict minerals or products containing conflict minerals that will then be incorporated into products shall be provided within reasonable time after the receipt of said conflict minerals. Documentation related to conflict minerals shall be preserved and retained for no less than five (5) years, in accordance with the OECD Guidelines.

05

Supply Chain Due Diligence

To ensure that any conflict minerals in the supply chain are responsibly sourced, SK hynix will conduct regular assessments of the materials and components found in its products and flow down the applicable requirements to all suppliers through purchasing terms and conditions. Pursuant to the Conflict Minerals Guidance, SK hynix will oversee the collection of supplier due diligence in accordance with the OECD Guidelines.

In order to undertake a reasonable country of origin inquiry for each conflict minerals in its supply chain, SK hynix will oversee the collection of supply chain information pursuant to procedures adopted in accordance with the Conflict Minerals Policy, by, among other methods, collecting data about conflict minerals sourcing from SK hynix suppliers using the EICC Conflict Minerals Reporting Template (“CMRT”) (which suppliers are required to complete pursuant to the SK hynix Supplier Code of Conduct). SK hynix will also complete a CMRT for the Company based upon the results of its supply chain due diligence.

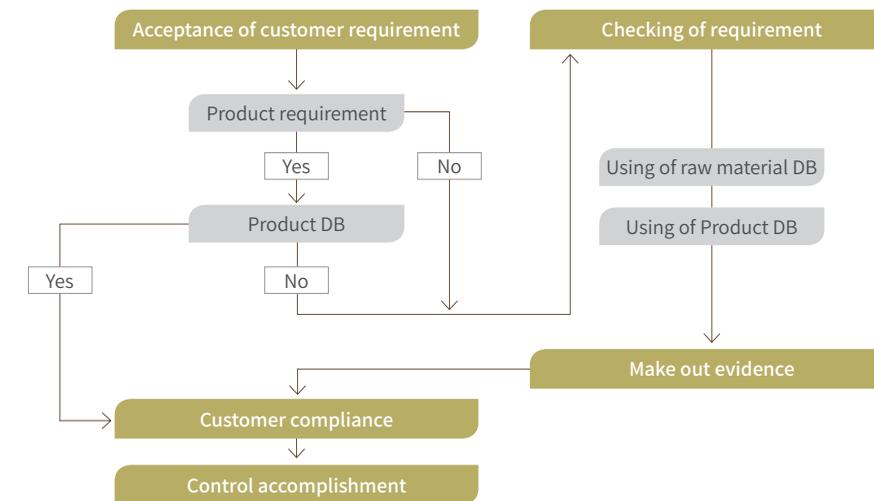
Conflict minerals that come from “recycled or scrap” resources are also excluded from the due diligence required under the SEC Conflict Minerals Rules. Conflict minerals are derived from recycled or scrap resources when they come from reclaimed end-user or post-consumer products, or scrap processed metals created during product manufacturing. Minerals that are partially processed, unprocessed, or a bi-product from another ore are not considered recycled metal.

If SK hynix becomes aware that improperly sourced conflict minerals (conflict minerals from the DRC Countries which originated or reasonably likely originated from a mine, smelter, or refinery that benefits an armed group) are present in its supply chain, the Company will determine which SK hynix products may contain improperly sourced conflict minerals. SK hynix will take appropriate action pursuant to procedures adopted in accordance with this Policy, including, but not limited to: supplier notifications, exploration of alternative sourcing, and termination of supplier relationships.

06

Conflict Minerals Data Management System

To properly manage any and all data related to conflict minerals, SK hynix keeps and maintains a data base system for conflict free minerals. In the event of purchase of any new materials or change in the materials to be used in manufacturing SK hynix products, the Procurement Team or Customer Compliance Team will collect the data in accordance with EICC regulations/guidelines and distribute to the relevant teams within the Company. All teams must review and check whether there is any issue, error, abnormality, etc. upon receipt of which Quality Assurance Team will update the data base system to reflect accurate data.



07

Customer Conflict Minerals Requests

SK hynix will address requests related to conflict minerals sourcing from SK hynix's customers or other third-parties, including, but not limited to: (1) requests for certifications or representations as to whether SK hynix's products contain conflict minerals sourced from the DRC Countries; (2) requests for contract terms pursuant to which SK hynix takes responsibility for violations of conflict minerals laws or regulations; (3) requests for copies of a CMRT completed by SK hynix; or (4) requests for information about SK hynix's supply due diligence measures.

08

Violation of the Conflict Minerals Policy

Violation of the law or the Conflict Minerals Policy is a serious matter, and can lead to impairment of customer relationships and, in some cases, breach of customer contracts, which could result in lawsuits against SK hynix. Violation of the Conflict Minerals Policy can result in reputational harm to SK hynix and possible pressure from industry organizations (such as the EICC), non-governmental organizations, human rights activists, and consumer or other market forces to prove that the products of SK hynix are conflict-free. All employees have a duty to report violations or suspicious circumstances that might indicate a possible violation of law or the Conflict Minerals Policy. Employees MUST report all suspicious conduct to the Global Compliance Team and must not delay such a report merely because the employee is not sure whether sufficient "proof" of a violation exists. Often reports of suspicions, made early enough, will allow the Company to intervene in a timely manner to prevent an actual violation from occurring.



07

Export Control





Export Control

As a world leader in the field of memory semiconductor R&D and manufacturing for a broad spectrum of industries, SK hynix and its subsidiaries are keenly aware that export control laws and regulations in many different countries apply to our businesses. We recognize that these laws typically are intended to protect the safety and well-being of the public and to prevent products, services, information, and technologies from falling into the hands of terrorist groups or hostile nations. SK hynix places a high value on this protection. It is our Company's policy to comply fully with all applicable laws and regulations that govern the export, temporary import, and re-export of goods, services, and technology where we conduct business, and we expect our customers and business partners to do the same.

Any violation of export control laws, even a technical or inadvertent one, could subject SK hynix, as well as the individual employees involved, to severe criminal penalties (including jail time for individuals), civil penalties (including very large fines), the loss of export privileges, and suspension or debarment from certain contracting opportunities. Our corporate Export Compliance Policy ("Export Compliance Policy") is, therefore, a matter that needs to be treated with the utmost seriousness.

It is the responsibility of each individual employee to be aware of and comply with the applicable export control laws in performing their jobs. Non-compliance with the applicable policies and procedures by SK hynix employees may also result in corporate discipline, including dismissal in appropriate cases.

This Export Compliance Policy governs the export, temporary import, and re-export of goods, services, and technology.

This Export Compliance Policy is particularly important for employees who participate in the sale or shipment of products, services, or technical data. The international business activities governed by this program include, but are not limited to :

- ✓ Proposals and sales contracts;
- ✓ Procurement contracts;
- ✓ Processing requests of quote or contracts;
- ✓ Product sales;
- ✓ Transfers of technical data and products; and
- ✓ Export, temporary import, and re-export of goods, services, and technology

01

Export Control Laws in General

Exporting our products in a safe and lawful manner is critical to SK hynix's business performance. However, export control and economic sanctions laws are complicated. Every country has its own export compliance and sanctions regime, and as an international company, SK hynix is dedicated to comply with all laws that apply to our business, wherever conducted. This Export Compliance Policy reflects best practices in global export control compliance and is designed to ensure compliance with export control laws where the company does business.

Some key terms to understand as you review this policy include :

- ✓ An export is the transfer of an item to another country. The item can be a physical commodity, software, or technology. A transfer that constitutes an export may occur when: 1) an employee in possession of technology developed in one nation engages in technical discussions with a "foreign" person (a person who is not a citizen or permanent resident of the nation where the technology was developed) - wherever the discussion takes place; or 2) a "foreign" person tours facilities of an operating unit, or 3) a "foreign" person accesses technology of an operating unit as an employee, consultant, or subcontractor.
- ✓ The term U.S. item or U.S.-origin item refers to any item that: (1) is designed, developed, produced, engineered, or manufactured in the United States (including software or technology); (2) contains a part or parts that were designed, developed, produced, engineered, or manufactured in the United States; or (3) is exported from the U.S.
- ✓ The term technology means specific information necessary for the "development", "production" or "use" of a product. The information takes the form of "technical data" or "technical assistance".
- ✓ An end user is the person that receives and ultimately uses the exported or re-exported items. The end-user is not a forwarding agent or intermediary but may be the purchaser or ultimate consignee.
- ✓ A dual-use item is an item that may serve two purposes. Dual-use items include items that can be used for both civil and military purposes.
- ✓ Economic sanctions are a tool of foreign policy used by national governments. Sanctions laws and regulations vary widely in their scope to meet foreign policy needs - which change from circumstance to circumstance and from time to time. Some sanctions are comprehensive or nearly comprehensive, while other sanctions are more limited. Sanctions may be imposed against or related to: (1) certain countries; and (2) persons or entities engaged in certain activities.
- ✓ A Specially Designated National (SDN) is an individual or entity that has been designated by the U.S. Department of the Treasury under a sanctions program. These individuals' / entities' assets are blocked or frozen in accordance with U.S. law and may also be the subject of other countries' sanctions programs. U.S. persons are prohibited from dealing with them. Transactions with SDNs may also be limited by other national laws.



- ✓ Screening procedures are the necessary due diligence activities that must be conducted in order to ensure compliance with export and economic sanctions laws and regulations. Screening procedures are generally comprised of assessing whether parties to an export or the items being exported are of concern and require further review by the compliance officer before being approved for export.

Employees, officers, directors and agents acting on behalf of SK hynix must exercise due diligence and good faith when exporting our products to ensure that under no circumstances will any sale, shipment, transfer of information, service, or transaction of any kind occur contrary to the export control, embargoes and economic sanctions laws and regulations where we do business in order to avoid civil and criminal penalties. In worst case scenarios, violations may result in SK hynix being blacklisted (for example, SK hynix could be placed on the U.S. Denied Persons List) and be prevented from engaging in business transactions with entities from certain nations. Such penalties, and the adverse publicity and expense which could result even from an accusation of an export violation, could seriously damage the Company.

For reference, the following countries are currently subject to trade sanctions, which may prohibit our doing business with them: North Korea; Iran; Cuba; Belarus; Sudan; and Syria.

Employees must keep in mind that an export can occur not only by shipping products or technology to another country, but also by other activities. For example, an export can also occur when an employee discusses SK hynix technology with :

- ✓ a person who is not a citizen or permanent resident of the country in which the technology was created, wherever the discussion takes place;
- ✓ a person who is not a citizen or permanent resident of the country in which the technology was created tours SK hynix facilities; or
- ✓ a person who is not a citizen or permanent resident of the country in which the technology was created uses or reviews SK hynix technology as an employee, consultant, or subcontractor.

These activities result in exports referred to as “deemed exports” because it is assumed that the technology accessed by the foreign person has moved, or inevitably will move, to the country of which he/she is a citizen. That is not to say that any of these activities is improper. To the contrary, these activities routinely take place and must for SK hynix to succeed. However, SK hynix must be vigilant to ensure that it shares its technology with only our most trusted employees, business partners and visitors.

02

Export Compliance Management Organization

SK hynix Export Control Management Committee and Global Logistics Team manage the export control compliance of strategic materials. The Export Control Management Committee shall have responsibilities as below :

- ✓ To enact and amend the SK hynix's internal export control policy;
- ✓ To determine strategic materials
- ✓ To approve strategic materials, domestic transactions report
- ✓ To review export transactions screening results;
- ✓ To manage post verification of exported goods;
- ✓ To manage related document; and
- ✓ To request reports from the head of relevant department, conduct inspections, and/ or take corrective measures.

Because export and economic sanctions laws and regulations are a tool of foreign policy, they change at the discretion of national leaders (e.g., the South Korean President or the U.S. President). While some of these changes are well publicized, like E.U. and U.S. sanctions in response to Russia's actions in Ukraine, changes to export controls and economic sanctions can occur often and with little advance warning. For example, the designation of a new drug trafficking kingpin will not generally make news, but SK hynix is expected to know of this addition and comply with it. Not knowing that the designation of an item, individual, or entity has changed is NOT a defense against a violation of export controls or economic sanctions. Thus, it is imperative that SK hynix be aware of changes in export and economic sanctions laws and regulations of the countries in which SK hynix does business. SK hynix may do so by regularly monitoring relevant government websites.

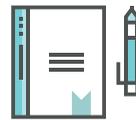


03

Violation of Export Compliance Policy

Violation of export control and economic sanctions laws or this Export Compliance Policy is a serious matter and can result in criminal or civil penalties against SK hynix and the individual involved in the violation, as well as harm to SK hynix's reputation. It can also result in a prohibition from trading with individuals or entities. Employees, officers, directors, or others involved in a violation will be subject to discipline, up to and including termination. Any violation of law or this Export Compliance Policy may result in a loss of incentive compensation, stock options, bonuses, or other awards, to the extent permitted by law.

All employees have a duty to report violations or suspicious circumstances that might indicate a possible violation of law or this Export Compliance Policy to the Export Control Management Committee. Employees MUST report all suspicious conduct, and must not delay such a report merely because the employee is not sure whether sufficient "proof" of a violation exists. Often reports of suspicions, made early enough, will allow the Company to intervene in a timely manner to prevent an actual violation from occurring. Employees, managers, or other individuals must submit reports to the Export Compliance Management Committee.



08 Record Management & Risk Assessment



Record Management



Employees who conduct transactions on SK hynix's behalf must ensure that all transactions (no matter how small) are recorded promptly and accurately, contain sufficient detail, and are supported by objective documentation. SK hynix also maintains controls designed to identify and prevent improper transactions. These controls require employees to obtain approval before executing transaction on SK hynix's behalf, use SK hynix funds and other assets only as permitted by management, report and record transactions as required by SK hynix accounting department and generally accepted accounting principles; and maintain procedures to reconcile differences between accounting records and actual assets. Any and all information related to SK hynix business shall be kept and maintained subject to SK hynix Document Retention Rules.

Risk Assessment



As this Guidebook applies to all SK hynix directors, officers, and employees, as well as any subsidiary or business venture that SK hynix controls, any and all such parties or individuals are subject to the Company's occasional monitoring for the purpose of risk assessment. Such risk assessment results are reported to the management and/or appropriate departments in order to take corrective measures, ensure compliance, and improve applicable system(s).



Frequently Asked Questions

- 74 Anti-trust Laws in General
- 75 Bribery & Corruption in General
- 76 Relatives, Friends & Colleagues of Government Officials
- 77 Hosting & Gifts
- 78 Charitable Contributions
- 79 Interactions with Government Entities & Officials
- 79 Third Parties
- 80 Facilitation Payments
- 80 Books, Records, & Related Internal Controls
- 81 Export Control
- 86 Data Protection in General

Frequently Asked Questions

Anti-trust Laws in General

What are some of the consequences of violating the anti-trust laws?

The consequences for violating the anti-trust laws can be severe for SK hynix and the culpable individuals involved with the violation. Such violations can result in criminal penalties, including imprisonment and fines, being levied against the Company and the individuals involved in the violation. For example, an individual can receive a maximum sentence of ten years for being found guilty of price fixing. In addition, the corporate fine for an anti-trust violation can be as high as \$100 million. Violations can also lead to expensive and time consuming litigation, as well as civil penalties, including trebled monetary damages. Importantly, violations of the anti-trust laws can harm the reputation and goodwill of SK hynix.

What are the consequences of violating the Anti-trust Policy?

All employees, officers, directors, or others involved in a violation of the Anti-trust Policy will be subject to discipline, up to and including termination. Moreover, violation of the Anti-trust Policy may result in a loss of incentive compensation, stock options, bonuses, or other awards.

What actions are prohibited by the anti-trust laws and the Anti-trust Policy?

It is not possible to provide an exhaustive list of activities that could violate the anti-trust laws. Generally, the anti-trust laws prohibit an individual or company from unreasonably restraining competition. An individual or company can unilaterally violate the anti-trust laws if they have significant market share and engage in a predatory conduct. The Anti-trust Policy highlights the types of predatory conduct that would violate the anti-trust laws. An individual or company can also violate the anti-trust laws by entering into an agreement with a third party, particularly a competitor. The Anti-trust Policy highlights the types of agreements that would violate the anti-trust laws.

Is it okay to be a member of a trade association?

Typically, a company will join a trade association and send an employee to attend meetings of the trade association on behalf of the company. While membership to a trade association is not prohibited by the anti-trust laws, employees should exercise caution when they are engaged in membership activities and interacting with other members, on behalf of the company. Such membership provides opportunities for competitors to interact and share competitively sensitive information. That exchange of information runs the risk of violating the anti-trust laws. Also, members of trade associations must be careful in developing industry-wide standards. As the

Anti-trust Policy notes, while these activities are generally considered lawful, they can violate the anti-trust laws if they have the effect of fixing prices or if they result in competitors improperly being boycotted or excluded from effectively competing in a market.

What should I do if I learn of a violation or possible violation?

All employees have a duty to report potential violations of the anti-trust laws or the Anti-trust Policy to the Chief Compliance Officer or the Cyber Opinion Center. Employees must promptly report even suspicious conduct, even if the employee is not sure whether sufficient proof of an anti-trust violation exists. Early reports of suspicions may provide SK hynix with the opportunity to intervene in a timely manner to prevent an actual anti-trust violation from occurring. SK hynix will not tolerate retaliation against any individual who submits such a report in good faith, and any suspected retaliation should be reported to the Chief Compliance Officer or the Cyber Opinion Center.

Bribery & Corruption in General

SK hynix has responded to an RFP issued by a private automaker to supply microchips for the onboard computers in its vehicles. I know that the automaker's procurement officer is a football (soccer) fan, and I'd like to take him to an upcoming match to develop a relationship with him. Is this acceptable?

No. If the tickets are offered with the expectation of influencing the procurement officer to award the contract to SK hynix, then the transaction is improper. Offering the tickets for that purpose would constitute a bribe, and the Anti-Corruption Policy prohibits all forms of bribery in SK hynix's dealings with its business partners and with the government. Even if the tickets are not expressly offered to exert influence over the procurement officer, a regulator could view this transaction as a bribe. It is best to defer the gift until after SK hynix has won the contract on the merits, and the circumstances otherwise raise no possibility of being offered for an improper purpose.

We have a long-standing relationship with a private customer who has placed significant orders with SK hynix. We haven't provided any gifts or entertainment to the customer in the past year, and I'd like to take her and her spouse to a modest dinner and a local theater production to show that we appreciate her business. May I do this?

Probably. This entertainment appears appropriate, since the event is not lavish, and would probably not raise an inference of being offered in exchange for the customer's business. Typically, gifts and entertainment should not include the recipient's spouse if doing so could be viewed as an attempt to obtain an improper benefit from the recipient. However, given that SK hynix has an established relationship with this customer and has not provided gifts or entertainment recently, it is unlikely that inclusion of the customer's spouse on this occasion would create the appearance of impropriety. Similar entertainment should not be provided on a frequent basis to this customer in the future, as doing so could increase the risk that it will be viewed as a bribe.

SK hynix is applying for a patent for a new microchip, and we would like to retain a professor at a governed-owned university to review the application and assist us with the approval process. Can we do this?

Yes. The professor may qualify as a government official because he is employed by a state-owned institution. SK hynix may be able to retain him, provided that SK hynix does not offer the professor anything that could be viewed as a bribe, and that the professor will not provide bribes to government officials involved in the patent process. Retention of the professor qualifies as a non-routine government interaction under SK hynix's Anti-Corruption Policy, and must therefore be preapproved by Regional Compliance.

Relatives, Friends & Colleagues of Government Officials

Our manufacturing facility is inspected on a semiannual basis by the provincial workplace safety agency. I am responsible for accompanying the local regulator on these inspections. During the last inspection, he indicated that his son, who is attending college, is looking for an internship for the summer, and he asked whether we have any positions available. We typically hire two unpaid interns each summer. May I offer this opportunity to the regulator's son?

No. Offering the internship to the official's son could create the appearance that SK hynix is attempting to influence the official by providing a benefit to his son. You should contact the Chief Compliance Officer to review this situation.

The internship should be competitively awarded through SK hynix's standard recruitment process, and the son should be invited to apply through that process. The individuals that interact with the official should not participate in the hiring decision, in order to guard against the appearance that SK hynix has offered the position to exert influence over the official.

Hosting & Gifts

I am planning to attend a trade association conference next month. During the event, I would like to host a modest dinner for a few representatives of SK hynix's customers, some of whom are employees of state-owned manufacturers. Is this acceptable?

Yes. Entertainment of this type is likely proper, if it is provided without the expectation of influencing the government officials, is not lavish, does not recur on a frequent basis. The event must also be permitted under local law, and be related to the promotion, demonstration, or explanation of SK hynix's products. You should contact the Chief Compliance Officer before attending the conference to obtain preapproval for the dinner.

I am responsible for purchasing silicon from a state-owned supplier in China. I speak on a weekly basis with one of the supplier's sales representatives, who mentioned that his daughter has recently become engaged. I would like to provide the consultant with a small cash gift for his daughter, which is consistent with local custom and practice. May I do so?

No. The Code of Business Conduct & Ethics prohibits employees from providing gifts of cash to government officials or individuals affiliated with them. However, because the engagement is a recognized gift-giving occasion, you may provide small a non-cash gift, provided that you obtain preapproval from the Chief Compliance Officer.

Officials from the national labor department periodically inspect our facility to ensure compliance with health and safety regulations. I accompany the officials during the inspections and sometimes offer to buy them lunch in our company cafeteria afterward, or provide them with a pen or other item imprinted with the SK hynix logo. Is this acceptable under our Anti-Corruption Policy?

Probably. Generally, the Anti-Corruption Policy permits employees to provide these types of hosting and gifts to government officials, provided that they are not offered to improperly influence the officials. However, some countries limit the ability of government officials to accept gestures of this type. You should only provide these benefits if they are permitted under the local law in your jurisdiction. Even if applicable law allows you to do so, you should obtain preapproval from the Chief Compliance Officer before providing such benefits.

We are currently negotiating a supply contract with a state-owned mining company that supplies SK hynix with gold, tungsten, and tantalum. The company's sales officer enjoys fine food and entertainment, and has a reputation for negotiating contracts over expensive dinners or in the luxury suites during sporting events. Most companies provide these benefits to the official as a "cost of doing business." Can we give the official such benefits to assist with negotiations?

No. This practice is problematic for multiple reasons. Because the sales officer works for a state-owned entity, may be qualified as a government official for anti-corruption purposes. It appears that the meals and tickets are offered to influence his decision-making, and therefore constitute bribes under anti-corruption laws. In addition, the expensive dinners and luxury tickets appear to be lavish in light of the circumstances, and are therefore inappropriate even when offered to individuals unaffiliated with the government. SK hynix is committed to obtaining supply contracts on their merits, and does not provide these types of benefits to influence decision-making of its suppliers.

Charitable Contributions

SK hynix is planning to open operations in a new country and requires a permit from the local business regulatory authority before operations begin. One of our local consultants is friendly with the head of the authority and has advised that that we should make a contribution to a local charity founded by the official's wife "if we want quick action on our permit application." The charity provides food and educational benefits to disadvantaged children in the community. Make we make the contribution in an effort to show that we want to be a good neighbor in this community?

No. While the charity may serve a beneficial purpose, anti-corruption regulators would likely conclude that this payment was made to influence the government official to speed up the approval process. The contribution would therefore qualify as a bribe under anti-corruption laws. SK hynix should decline to make the contribution.

Interactions with Government Entities & Officials

Are we required to obtain approval before purchasing electricity or natural gas from a state-owned utility?

No, provided that the rates for the service are objectively determined, such as by a predetermined fee schedule. The Anti-Corruption Policy does not require preapproval for these types of routine government interactions.

My department is planning to negotiate a lease for office space in a state-owned office park. Does this transaction require preapproval?

Yes. The Anti-Corruption Policy requires that non-routine government interactions be preapproved by the Chief Compliance Officer. This includes any transaction in which SK hynix will negotiate with the government regarding the price or scope of services that the government will provide to the company. Contracts will typically be approved if they are negotiated at arm's length, consistent with market prices, and executed for a proper purpose.

Third Parties

Why do we need to obtain preapproval for some types of third parties?

Under anti-corruption laws, SK hynix and its employees can be held liable for illegal acts committed by third parties retained by the company. A bribe paid by an agent, consultant or customs broker could potentially implicate SK hynix or its employees in criminal and civil proceedings and subject them to fines and other penalties. Prosecutors around the world are focusing on third-party relationships and have made it clear that conducting an anti-corruption review of third parties before retaining them is a core component of an effective ethics and compliance program.

How do I determine whether a particular third party must be preapproved?

Any third party that will interact or is likely to interact with a government official or entity on SK hynix's behalf must be preapproved by the Chief Compliance Officer. Common examples include customs brokers, consultants who obtains permits or negotiate with government officials on SK hynix's behalf, accountants who assist with filing tax documents, and lawyers who represent SK hynix in court or before government agencies.

I am responsible for identifying a location for a new SK hynix manufacturing facility. I've found a community in Malaysia that offers skilled labor and low production costs, but obtaining the necessary zoning permits is likely to be time-consuming and difficult. A local zoning official informed me that his brother-in-law has a thorough knowledge of the regulatory system and can assist with obtaining the permits in a timely manner. He recommended that we hire his brother-in-law as a consultant to "speed the process along." May I retain the brother-in-law?

No. You should decline to retain the brother-in-law. The official's recommendation raises a warning sign that he is attempting to direct business to his brother-in-law in exchange for expedited permit approvals. Even though the consulting payments would be made to the brother-in-law, anti-corruption regulators in most countries would consider these payments made for the benefit of the zoning official, and therefore improper under anti-corruption laws. SK hynix's Code of Business Conduct and Ethics and the Anti-Corruption Policy prohibit such payments.

Facilitation Payments

I am responsible for paying customs duties on SK hynix products entering Brazil. Some customs inspectors are willing to expedite processing of imports in exchange for a fee R\$45, which is equal to approximately ₩20,000. May I make these payments to expedite the customs process?

No. Anti-corruption laws and the Anti-Corruption Policy prohibit these type of payments, known as facilitation payments, from being made anywhere in the world.

Books, Records, & Related Internal Controls

I am a sales representative responsible accounts in southeast Asia, where many of SK hynix's customers are state-owned. I sometimes take procurement officers from these companies out for lunch, usually at a local street market. Because the cost is minimal, I don't always report it or request reimbursement from SK hynix. Is this allowed?

No. Reporting of expenses—especially those associated with benefits provided to government officials—must be properly tracked and accounted for under anti-corruption laws. You must properly report these expenses as benefits provided to government officials, even though their value is small.

Export Control

What parts of SK hynix's business are affected by the export compliance policy?

The following international business activities are governed by this policy: proposals and sales contracts; procurement contracts; processing requests of quote or contracts; provision of samples; product sales; transfers of technical data and products; and export, temporary import, and re-export of goods, services, and technology.

What countries are subject to trade sanctions?

In order to make this determination, you must first determine which countries' laws apply.

Under UK law, the sanctioned country list includes Armenia, Azerbaijan, Belarus, Burma, Cuba, Democratic Republic of Congo, North Korea, Eritrea, Iran, Iraq, Ivory Coast, Lebanon, Liberia, Libya, Republic of Guinea, Sierra Leone, Somalia, Syria, South Sudan, Sudan, Zimbabwe.

Under US law, the sanctioned country list is Cuba; Iran; North Korea; Sudan; and Syria.

What government agencies oversee export and trade sanctions regulations?

In the United States, the following agencies oversee various parts of export compliance: Department of Commerce Bureau of Industry and Security (BIS); Department of Treasury Office of Foreign Assets Control (OFAC); Department of State Directorate of Defense Trade Controls (DDTC).

SK hynix also has subsidiaries in Belarus, Italy, China, Germany/UK, India, Japan, Singapore, and Taiwan. Some of those other export and trade sanctions regulations oversight agencies include :

- ☑ Canada : Public Works and Government Services
- ☑ Germany : Federal Office of Economics and Export Control
- ☑ UK : Her Majesties Revenue & Customs (HMRC) and The Department for Business Innovation and Skills (BIS)

Governments where we do business maintain lists of countries and individuals who are the subject of trade sanctions or embargoes. SK hynix must refer to these lists as appropriate before engaging in transactions.

What is an export?

An export can occur not only by shipping products or technology to another country, but also by other activities. For example, an export can also occur when: an employee discusses SK hynix technology with a person who is not a citizen or permanent resident of the country in which the technology was created, wherever the discussion takes place; a person who is not a citizen or permanent resident of the country in which the technology was created tours SK hynix facilities; or a person who is not a citizen or permanent resident of the country in which the technology was created uses or reviews SK hynix technology as an employee, consultant, or subcontractor. Some of these scenarios may not be applicable in every jurisdiction where SK hynix operates, however best practice is to assume that they are applicable, unless you are certain they are not applicable in any particular set of circumstances.

What should I do if I learn of a violation?

All employees have a duty to report violations or suspicious circumstances that might indicate a possible violation of law or this Policy. Employees MUST report all suspicious conduct, and must not delay such a report merely because the employee is not sure whether sufficient “proof” of a violation exists. Employees should submit reports to the Chief Compliance Officer or the Cyber Opinion Center.

What are the consequences of a violation?

Violations of export control laws may trigger severe sanctions against SK hynix and the individual involved in the violation, including criminal and civil penalties such as imprisonment for a period of years and fines that reach into the millions of dollars, as well as reputational damage. Employees, officers, directors, or others involved in a violation will be subject to discipline, up to and including termination. Furthermore, any violation of law or this Policy may result in a loss of incentive compensation, stock options, bonuses, or other awards, to the extent permitted by law.

Why do we have a Conflict Minerals Sourcing Policy?

SK hynix and its subsidiaries (collectively, “SK hynix” or the “Company”) are committed to establishing fair trade practices and creating an open and clean company culture which fulfills social responsibility. Responsible sourcing of conflict minerals with the objective of establishing a “conflict-free” supply chain is important to SK hynix. SK hynix will not tolerate deviations from SK hynix’s Conflict Minerals Sourcing Policy and other relevant policies and procedures adopted pursuant thereto, or violations of the applicable Conflict Minerals Guidance (as defined in the Conflict Minerals Sourcing Policy).

1. Is SK hynix subject to the United States SEC Conflict Minerals Rules?

No; but some of our customers are, and they rely on us to help them satisfy obligations under the SEC Conflict Minerals Rules (as defined below).

In the United States, Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, effective July 2010, requires the United States Securities and Exchange Commission (the “SEC”) to adopt rules (the “SEC Conflict Minerals Rules”) requiring certain public companies to disclose whether any conflict minerals extracted from the Democratic Republic of Congo or its adjoining countries (the “DRC Countries”) are used in their products, and if so, to disclose, among other matters, the measures taken to exercise due diligence on the source and chain of custody of those minerals. SK hynix is not directly subject to the SEC Conflict Minerals Rules, but follows similar requirements by virtue of its membership in the Electronic Industry Citizenship Coalition (“EICC”) and to better serve its customers.

As an EICC member, SK hynix is required to implement a conflict minerals sourcing policy, adopt procedures for conducting supply chain due diligence, and make its due diligence measures available to its customers, much like companies that are subject to the SEC Conflict Minerals Rules. The EICC has recommended that downstream companies like SK hynix use the Organisation for Economic Co-operation and Development (the “OECD”) Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected High-Risk Areas (the “OECD Guidelines”) in order to diligence their supply chains. In addition, some SK hynix customers are subject to the SEC Conflict Minerals Rules, and require SK hynix to conduct due diligence on its supply chain in accordance with the OECD Guidelines and to provide information about its due diligence measures. SK hynix customers that are subject to the SEC Conflict Minerals Rules expect to rely upon SK hynix’s supply chain due diligence in meeting their due diligence and disclosure obligations pursuant to those rules. For these reasons, SK hynix conducts conflict minerals supply chain due diligence in accordance with the OECD Guidelines (which incorporate some aspects of compliance with the SEC Conflict Minerals Rules).

Who must comply with the Conflict Minerals Sourcing Policy?

Compliance with this policy is mandatory for all SK hynix employees, officers, directors, and agents.

What am I required to do?

1. Are products purchased for the internal purposes of SK hynix subject to the supply chain due diligence required under the Conflict Minerals Guidance?

No. Supplies and equipment acquired for the internal use of SK hynix are not within the scope of required supply chain due diligence under the Conflict Minerals Guidance.

2. What products will be examined in order to comply with conflict minerals due diligence requirements?

SK hynix will examine each product that it supplies to its customers for the presence of conflict minerals. There is no de minimis exception to the Company's inquiry. Thus, any product that contains any amount of a conflict minerals will be examined.

3. What does it mean to "contract to manufacture" a product?

The degree of influence a company exerts over the manufacture of a product determines whether the company is deemed to have "contracted to manufacture" that product, as defined in the SEC Conflict Minerals Rules. It is important to note that SK hynix does not need to have substantial influence or control over the manufacturing of a product before it is considered to have contracted the manufacture. However, a company is not required to perform due diligence on products it simply buys and resells, or on generic products manufactured by a third-party upon which it simply affixes or etches its brand, marks, logo, or label.

4. What suppliers is SK hynix most concerned about?

SK hynix is considered a "downstream" company since it does not directly interact with smelters or refiners. As such, our diligence is mostly focused on ensuring the transparency of the supply chain down to the smelters or refiners. SK hynix is most concerned with those suppliers that supply products that go into the items we deliver to customers.

5. Will SK hynix seek representations from suppliers as to the reasonable country of origin?

Yes. The EICC guidance and the SEC Conflict Minerals Rules require a good faith "reasonable country of origin inquiry" with respect to any conflict minerals included in our products. SK hynix will seek and obtain representations from its suppliers that indicate the facility at which any conflict minerals in its supply chain were processed and that the conflict minerals did not originate in the DRC Countries.

In order to rely upon such representations to satisfy the reasonable country of origin inquiry standard, a company must have reason to believe the representation is true. Any red flags (such as discovering that a smelter processes conflict minerals from many countries, including the

DRC Countries, but that the company is unable to determine whether the conflict minerals from the "mixed smelter" were from the DRC Countries, or receiving a representation from a supplier that its conflict minerals originated from a country that has limited known reserves of the mineral) should trigger further due diligence by SK hynix.

In order to complete the supply chain due diligence mandated by the EICC guidance and the SEC Conflict Minerals Rules, SK hynix will require its suppliers to disclose (a) whether materials or components provided to SK hynix contain conflict minerals and (b) the source of such conflict minerals, in each case, even if the conflict minerals are not necessary to production or functionality, are outside the supply chain, or are from recycled or scrap sources.

In general, SK hynix expects to apply reasonable skepticism and judgment and generally be aware of any red flags that could be counter indicative to a supplier's statements, such as the pricing of materials, location of the supplier, purity/quality of materials, etc. SK hynix expects to proceed with due diligence if there is any reason to believe that the conflict minerals may not have come from recycled or scrap resources (despite the supplier's assertions).

What are the consequences of violating the Conflict Minerals Sourcing Policy?

1. What if SK hynix suppliers will not provide the requested information?

The EICC guidance and the SEC Conflict Minerals Rules require SK hynix to perform due diligence on its supply chains and to undertake a good faith inquiry to determine the reasonable country of origin for conflict minerals contained in products supplied to customers. Although SK hynix will endeavor to maximize responses from our suppliers, not every supplier will be cooperative.

In addition to educating suppliers about the SK hynix conflict minerals sourcing and due diligence requirements and encouraging suppliers to provide the necessary data (using the leverage of our buying power where possible), we will seek to negotiate terms requiring cooperation into our supplier contracts.

2. What if SK hynix determines that its supply chain or products contain improperly sourced conflict minerals?

The Conflict Minerals Guidance does not ban or impose a penalty on conflict minerals sourced from conflict-affected regions. Rather, regulators and the EICC require supply chain diligence. It is the goal of SK hynix to practice responsible sourcing of conflict minerals, with the objective of establishing a conflict-free supply chain. If improperly sourced conflict minerals are identified through supply chain due diligence or other means, SK hynix will work with its existing suppliers to explore alternative sourcing, using the leverage of its buying power where possible. If appropriate or applicable, SK hynix may seek contractual remedies for a supplier's breach

of representations or warranties as to the sourcing of conflict minerals supplied to SK hynix. SK hynix will ensure that all of the information obtained through supply chain due diligence is accurately reflected in the Conflict Minerals Reporting Template completed on behalf of the Company. SK hynix will work to identify the products which may contain improperly sourced conflict minerals.

What should I do if I learn of a violation or possible violation?

All employees have a duty to report potential violations of the law, the SK hynix Code of Business Conduct and Ethics, or the Conflict Minerals Sourcing Policy to the Global Compliance Team. Employees must promptly report even suspicious conduct, even if the employee is not sure whether sufficient proof of a violation exists. Early reports of suspicions may provide SK hynix with the opportunity to intervene in a timely manner to prevent an actual violation from occurring. SK hynix will not tolerate any retaliation against an individual who submits such a report in good faith, and any suspected retaliation should be reported to the Global Compliance Team.

Below are some examples of violations of the Conflict Minerals Sourcing Policy :

- ✓ Intentional misrepresentations regarding SK hynix's use of conflict minerals;
- ✓ Failure to adequately investigate the source of conflict minerals used by SK hynix; and
- ✓ Failure to follow SK hynix's prescribed procedures for procuring conflict minerals, including conflict minerals contained in any product purchased by SK hynix, or determining and reporting on SK hynix's use of conflict minerals.

Data Protection in General

Why do we have this Policy?

SK hynix, and its subsidiaries (collectively, "SK hynix") are committed to protecting the privacy of its employees and customers, including partners, vendors, and suppliers, and operating in accordance with privacy laws in the countries in which SK hynix operates. We have therefore developed and implemented – and will enforce – our Personal Information Privacy Protection Policy ("Policy"). SK hynix will not tolerate violations of privacy laws and deviations from this Policy.

Who must comply with this Policy?

Compliance with this Policy is mandatory for all SK hynix employees, officers, directors, and agents.

What are some of the consequences of violating privacy laws?

The consequences for violating privacy laws vary. In South Korea, depending on the type of violation, the consequences could be as high as 3 years imprisonment or a fine of 30 million won. In the United States, violations of privacy laws may be enforced through class action litigation, which often entails significant statutory damages and attorney's fees, or regulator actions. In European Union countries, violations may result in regulator investigations and the imposition of civil, and in some cases, criminal penalties. Moreover, violations of privacy laws could cause reputational damage to SK hynix.

What are the consequences of violating this Policy?

All employees, officers, directors, or others involved in a violation of this Policy will be subject to discipline, up to and including termination.

What actions are prohibited by the privacy laws and this Policy?

It is not possible to provide an exhaustive list of activities that could violate privacy laws. Generally, however, privacy laws restrict the types of personal information that may be collected, how it may be processed, and how the personal information may be shared or transferred. For example, in many jurisdictions, businesses must provide a privacy notice to consumers prior to collecting their personal information. The notice must describe how the business will use the personal information that it collects. Further, a business may not use the personal information for purposes not disclosed in the notice, without first obtaining express consent. Some jurisdictions, such as Korea and Japan, require a business to obtain consent to the transfer of personal information to a third party, other than a third party service provider. Further, many jurisdictions require a business to obtain prior consent from its customers in order to contact them for marketing purposes. Thus, it is SK hynix's policy that personal data only be used for the following purposes, provided individuals have been notified that their data may be used for such purposes :

- i as necessary to satisfy the purposes for which the information was collected;
- ii in furtherance of a specific and legitimate business purpose of SK hynix provided the use does not materially infringe upon the privacy interests of individuals;
- iii to satisfy legal obligations; or
- iv with the express consent of the individual.

Can I send marketing materials to customers?

It is the general policy of SK hynix not to market to customers, unless they have consented. We also do not send mass marketing emails and other communications to customers.

Can I access my Personal Information?

Yes, SK hynix gives employees the right to review most of the personal data we maintain as part of your employee record with us. You should contact your direct supervisor or your local HR coordinator for information on how to access and update your personal information on file with SK hynix.

How Can I Protect Personal Information?

It is the responsibility of all SK hynix employees to safeguard personal information. There are a number of important ways you can do this. Here are some examples of simple but important steps :

- ■ ■
- ✓ Always log off of or lock your computer, prior to stepping away, and log out of company systems when you are finished with the task you were performing within the system.
- ✓ Do not share your login credentials with anybody else, including other SK hynix employees.
- ✓ Keep your desk clear of documents containing personal information (and follow the SK hynix clear desk policy).
- ✓ Do not store personal information locally on your computer or on any other mobile device.
- ✓ Do not share personal information with others, unless you know they are approved to receive the information.
- ✓ Make sure to place documents containing personal information in shred bins so that they may be properly disposed of.
- ✓ Do not discuss or review personal or sensitive information in public places.
- ✓ Report suspected violations of confidentiality and data protection obligations and policies.

What about transfers of personal data across national borders?

A number of jurisdictions restrict the cross-border transfer of personal information, even where such information is being transferred to a group company. For example, under Singapore law, personal information may not be transferred outside of Singapore unless the recipient of the information provides protections for the information that are comparable to those available in

Singapore – usually these requirement can be satisfied by putting in place a written agreement that contractually requires protections for the personal information that are equivalent to those required under Singapore law.

European Union countries require (1) a written data processing agreement be in place any time personal data is entrusted to a third party (including group companies) for processing, and (2) if personal data are transferred outside of the European Economic Area, to a jurisdiction that does not have “adequate” privacy laws, EU data protection law requires another step be taken, such as executing the EU Standard Contractual Clauses between the EU-based company and the third party located outside the EU. Notably, neither the U.S. nor most Asian jurisdictions are considered by the EU to contain “adequate” privacy laws. Thus, any transfers of employee or customer personal data to group companies or third party service providers, or across national borders, needs to be reviewed for compliance with applicable local laws.

Must we notify regulators of SK hynix processing of personal information?

Maybe. Certain EU jurisdictions do require data controllers established within such jurisdictions to file a registration or multiple registrations with the authority regarding the data controller’s processing activities. These requirements will typically apply to the SK hynix local affiliate in the EU, not SK hynix corporate. It is the responsibility of SK hynix local affiliates to identify and comply with such requirements.

What should I do if I learn of a violation or possible violation?

All employees, officers, directors, and SK hynix agents have a duty to report potential violations of privacy laws to the Global Compliance Team. Employees must promptly report suspicious conduct, even if the employee is not sure whether sufficient proof of a privacy violation exists. Early reports of suspicious activity may provide SK hynix with the opportunity to intervene in a timely manner to prevent an actual anti-trust violation from occurring. SK hynix will not tolerate retaliation against any individual who submits such a report in good faith, and any suspected retaliation should be reported to Ethics Management Team.

What should I do if I learn of a security breach?

All employees, officers, directors, and SK hynix agents have a duty to report known or suspected security breaches. You should report any known or suspected data breaches to your direct supervisor immediately, who will make sure that the breach is reported appropriately to the Global Compliance Department and the Corporate Security Team.

—

This Guidebook is issued by Global Compliance Team.
Please address any concerns, questions, and/or comments regarding
this Guidebook to Global Compliance Team.

SK hynix Global Compliance Guidebook

SK hynix Inc.

April 2015

SK hynix Global Compliance Team

2091, Gyeongchung-daero, Bubal-eub, Icheon-si,

Gyeonggi-do, KOREA

Tel : 82-2-3459-3657

www.skhynix.com

Copyright © 2015, SK hynix Inc. All Rights Reserved.