

KONE GENERAL TERMS AND CONDITIONS OF PURCHASE ("GTC")

1 Definitions

The below capitalized terms shall have the meanings defined below, unless otherwise defined in the Agreement:

"Agreement" shall mean the agreement to which this GTC is attached. In the case of a discrepancy between such Agreement and this GTC, the Agreement shall prevail. If the parties have not entered into any separate agreement, the Agreement shall mean this GTC and any purchase order made between the parties;

"Products" shall mean the products to be delivered by the Supplier to the purchaser as specified in the purchase order, including any specified services to be performed in connection with the delivery, such as installation and testing of the Products.

2 Delivery

2.1 The delivery time and delivery terms for the Products are defined in the purchase order. If no delivery time is defined in the purchase order, the Supplier shall deliver the Products as soon as possible.

2.2 The Products shall be packed in a manner suitable for the means of transportation and the nature of the Products. The Supplier shall mark the Products and their packages as instructed by the purchaser and as may be required by applicable regulations.

2.3 In case the delivery of a Product is in delay, the purchaser shall be entitled to liquidate damages in the amount of 1% of the price of the Products per each day of delay. The maximum amount of the liquidated damages for delay shall be 15% of the price of the Products in delay. This does not restrict the purchaser's right to any further compensation for damages caused by the Supplier's delay.

2.4 If the Supplier has, or ought reasonably to have, reason to believe, that it will not be able to comply with the agreed delivery time, it shall immediately notify the purchaser of such delay, the reason for it and the expected duration of the delay. The Supplier's liability for late deliveries shall not be limited as a consequence of the Supplier's above-mentioned notice.

3 Prices and payment terms

3.1 The purchaser shall make all payments for Products within 60 days from the receipt of a valid invoice provided at all times that the Supplier has received a valid confirmation that the corresponding Products have been received at the purchaser's premises in accordance with the Agreement and/or the respective purchase order. The Supplier shall use electronic invoicing when submitting invoices to the purchaser provided that there are no legal restrictions in a specific country requiring paper-based invoicing to be used.

3.2 The prices of the Products is detailed in the purchase order. The prices include transportation costs and packing and packing materials, as well as all taxes, duties, levies and other possible charges, unless otherwise set out in the purchase order or the Agreement but excluding Value Added Tax (VAT), General Sales Tax (GST) or similar tax.

3.3 The Supplier's invoices shall include all the following information for each invoiced item: item number, item description, invoiced quantity, unit price of item, taxes, purchase order number and purchase order line item that the invoiced item is referring to. The Supplier shall ensure that the invoice is issued in accordance with applicable taxation and other relevant laws.

4 Quality

4.1 The Products shall have been manufactured with the highest level of craftsmanship and precision and shall be free from any defect in materials, workmanship or design. The Products shall comply with the Supplier's product specifications and any specifications provided by the Purchaser.

4.2 The Products shall comply with and be manufactured in accordance with all applicable laws, regulations and standards in the country of origin.

5 Warranty

5.1 The Supplier warrants that the Products comply in every respect with the requirements and specifications set forth in the Agreement.

5.2 The Supplier warrants all Products for a period of 24 months from the date of delivery of the Product (the **"Warranty Period"**). If the

warranty that the purchaser has given to its customer for the end-product is still valid after 24 months from the delivery of the Product by the Supplier, the Warranty Period shall be extended for as long as the purchaser's warranty for the end-product is in force, however not longer than 42 months from the date of the Supplier's delivery of the Product.

5.3 The Supplier shall correct any non-compliance or defect in the Products appearing during or dating from the Warranty Period by a new delivery of replacement Product free-of-charge, or, upon the purchaser's discretion, by repairing the defective Product. The Supplier shall be liable for the costs of inspection, shipping (including by air freight in urgent cases), replacement and/or repair of the affected Products as well as disassembly of the end-product necessary for the corrective measures. This shall include compensation for the time spent by the purchaser's employees or contractors on the corrective measures.

5.4 The Supplier shall not be liable for defects or costs arising out of the purchaser's specifications for the Products. The Supplier's liability does not cover defects, which are caused by the purchaser or its agents or customers e.g. through incorrect installation or use.

6 Indemnification

6.1 The Supplier shall indemnify and hold the purchaser harmless against any injuries to persons or damage to property caused by the Products. The Supplier's liability shall be reduced proportionately to the extent the purchaser or its agents contributed to such injury or damage.

6.2 The Supplier shall indemnify and hold the purchaser harmless against all consequences of any infringement by the Products on third party patents, trademarks, copyrights or other intellectual property rights, other than those resulting directly from the design or specifications of the purchaser.

7 Confidentiality

7.1 The Supplier shall not disclose to third parties nor use for any other purpose than the proper fulfillment of the Agreement any information of confidential nature, such as technical information and data, drawings, price structures, costs, volumes, administrative and operational information, commercial information or know-how received from the purchaser, in whatever form (the **"Information"**), without the prior written permission of the purchaser, except Information which (i) was in possession of the Supplier prior to disclosure hereunder; (ii) was or becomes part of the public domain without breach of the confidentiality obligations herein; or (iii) was independently developed by personnel of the Supplier having no access to the Information.

7.2 The Supplier shall not be entitled to use the purchaser as a reference or in any way publicize its cooperation with KONE (e.g. in social media) without the prior written consent of the purchaser.

8 Documentation

8.1 The Supplier shall deliver the Products with all necessary documentation to enable the correct use and installation of the Products. The purchaser shall have the right to use and distribute such documentation for the sales and maintenance of the Products.

8.2 The Supplier shall upon request provide the purchaser with information on the country of origin of the Products, including any applicable preferential origin, the correct tariff classification codes for the Products and whether the Products classify as dual-use items under the applicable export control laws and regulations.

8.3 All safety components (as defined in the EU Lifts Directive 2014/33/EU) delivered under the Agreement (whether as stand-alone Products or as parts of the Products) to be used within the EU, shall be labeled with (i) a type, batch or serial number or other element allowing their identification, (ii) the name or brand of the manufacturer and (iii) the postal address of the manufacturer. Further, to the extent any safety components provided to the purchaser are not manufactured by the Supplier, but are purchased from third parties, the Supplier shall keep records of the company from which the Supplier purchased the safety component for at least 10 years from the delivery to the purchaser. The Supplier shall upon request make such records available to the purchaser.

9 Term and termination

9.1 The Agreement shall remain in force until all Products have been delivered and all obligations under the Agreement have been met (including the warranty obligations).

9.2 Notwithstanding the above, and in addition to any termination rights under applicable law, either party may terminate the Agreement with immediate effect at any time by written notice to the other party if the other party is in material breach of the Agreement and fails to remedy such breach, if capable of remedy, within 14 days after issuance of a written notice thereof, or the other party files for bankruptcy or liquidation or becomes insolvent.

9.3 The sections on warranty, indemnification, confidentiality and any other sections that by their nature are deemed to survive, shall survive the termination of the Agreement.

10 Miscellaneous

10.1 The Agreement constitute the entire agreement between the parties relating to the subject matter hereof. For the avoidance of doubt, any references to the Supplier's general terms of sales included in an order confirmation or otherwise shall not be binding upon the parties.

10.2 Any amendments to the Agreement must be made in writing signed by the authorized representatives of both parties.

10.3 The Supplier shall maintain adequate insurance to cover any general liability (including product liability) the Supplier may incur in connection with or as a result of the performance of its obligations under the Agreement. The Supplier shall upon request present the corresponding insurance certificates to the purchaser.

10.4 The Supplier may not transfer or assign the Agreement or any part of it without the prior written consent of the purchaser. The purchaser may freely transfer or assign this Agreement or any part thereof to any company affiliated with the purchaser.

10.5 The Agreement shall be governed by and construed in accordance with the laws the domicile of the purchaser.

10.6 Any disputes relating to this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce. The seat of the arbitration shall be Helsinki, Finland and the language of the arbitration English.

10.7 The Supplier confirms that any Product provided to purchaser shall be free from viruses, malware and other vulnerabilities and shall be connected to network with secure means and protected against any unauthorized disclosure or alteration of business information. The Supplier shall have the capability to prevent, monitor and patch vulnerabilities and respond to IT security and privacy incidents relating to the Product.

10.8 The Supplier ensures that any processing of personal data under the Agreement is done in accordance with all applicable data protection laws, including the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council). The Supplier operates as a data controller, as defined in GDPR, and shall be responsible for lawful processing of the personal data and ensuring that all applicable legal requirements are complied with. The Supplier agrees that personal data of the Supplier's representatives will be processed by KONE group and entities operating at KONE's request under the Agreement and for Supplier relationship management purposes. The Supplier shall ensure it is entitled to share such personal data under this Agreement.

11 Compliance

11.1 The Supplier shall ensure that it, and its supply chain, complies with all applicable export control laws and regulations, including but not limited to international trade restrictions and dual use-items. The Supplier shall immediately notify the Purchaser in writing if there is any non-compliance or anticipated non-compliance by the Supplier or any part of its supply chain. The Supplier shall, upon the Purchaser's request, provide the Purchaser with all necessary information and documentation relating to the Products in order for the Purchaser to comply with applicable export control laws and regulations, including but not limited to international trade restrictions and dual-use items (including all relevant technical specifications and other documentation necessary for the Purchaser to verify whether the Products or components supplied under this Agreement qualify as dual-use items). Further, should there be any change in the dual-use qualification of the Products or components, the Supplier shall inform the Purchaser thereof in writing immediately. The Supplier shall not sell the Products and shall ensure that the Products are not sold or circumvented, into the Russian Federation and/or Belarus, or for use in the Russia Federation and/or Belarus. The Supplier shall immediately notify the Purchaser in writing upon any breach or anticipated breach.

11.2 The Supplier shall provide the Purchaser with information on the country of origin and the correct tariff classification codes for the Products. The Supplier shall also provide any preferential origin documentation, such as the Supplier's declaration or similar, to the Purchaser when applicable. Should there be any change to such information, the Supplier shall inform the Purchaser thereof in writing immediately. The Supplier shall obtain all necessary licenses and/or permits from relevant authorities for the export, re-export, or in-country transfer of Products.

11.3 The Supplier confirms that at the time of signing the contract, neither the Supplier nor any director, officer, representative, or owner of the Supplier is subject to international trade restrictions or trade sanctions, including without limitation those imposed by the United Nations, European Union and/or United States ("International Trade Sanctions"). Should the Supplier or any of its directors, officers, representatives, or owners during the term of the Agreement become subject to International Trade Sanctions, it shall immediately notify the Purchaser thereof. If the Supplier, directly or through its owners or beneficiaries, is or becomes subject to International Trade Sanctions including without limitation being or becoming listed on the OFAC's Specially Designated Nationals (SDN) list, Sectoral Sanctions Identification (SSI) list or any other such restricted party list as may be published by the United Nations, European Union and/or United States, the Purchaser shall have the right to terminate this Agreement with immediate effect and without any liability for damages and the Purchaser shall be released from any further contractual obligations towards the Supplier.

11.4 The Purchaser may use third party service providers to carry out and conduct automated compliance screening and due diligence on the Supplier before and during the term of this Agreement in order to ensure the Purchaser's compliance with international laws, regulations and standards and to assess the Supplier's conformity with the terms and conditions of this Agreement and the KONE Supplier Code of Conduct.

11.5 The Supplier confirms that it (i) assures the adequate level of security of its supply chain, (ii) prohibits any unauthorized access or interference by third parties to the facilities, goods, files and documentation related to the supply of the Products, (iii) only uses reliable personnel in the supply of the Products and (iv) assures the adequate level of know-how to ensure compliance in accordance to applicable customs regulations. The Supplier shall train its personnel providing the Products to the Purchaser on the applicable requirements of the Authorized Economic Operator (AEO) guidelines. The Supplier shall also ensure that all its subcontractors (and their possible subcontractors) involved in the manufacturing and supply of the Products are informed about and comply with the above requirements.

11.6 The Supplier confirms that it complies with **Annex 1 (KONE Supplier Code of Conduct)** and **Annex 2 (Security Requirements)**.

11.7 Each Party recognizes the importance of compliance with international human rights standards and commits to respecting and endorsing internationally recognized human rights, including but not limited to those set out in the International Bill of Human Rights, the UN Guiding Principles on Business and Human Rights, and the principles set out in the International Labor Organization's Declaration on Fundamental Principles and Rights at Work.

12 Supplier Environmental Information

12.1 The Supplier shall provide to the Purchaser all data and information in relation to greenhouse gas emissions, energy production & consumption, life cycle inventory, recycled material content, material declarations, and any other environmental or sustainability matters in connection with any Products in a form as may be nominated by the Purchaser from time to time:

- a) within 14 days of written request by Purchaser;
- b) at least 30 days before:
 - a. the introduction of any new Products;
 - b. any modifications to the specifications of any Products;
 - c. any modifications to the manufacturing process of any Products;
 - d. any changes to any materials or inputs used in, or in connection with, any Products.

12.2 The Supplier shall provide to the Purchaser any supporting material reasonably requested by the Purchaser within 14 days of written request by Purchaser.

12.3 The Supplier warrants that all documents and materials provided to the Supplier under this clause are complete and accurate. The Supplier hereby indemnifies the Purchaser against any loss, cost, or expense suffered or incurred by, and any fine or penalty levied against, the Purchaser as a result of any incompleteness or inaccuracy.

12.4 If the Supplier does not provide the documents and materials set out above by the date for provision, the Purchaser may withhold payment of any amount due and payable to the Supplier under this Agreement until the documents and materials are received, and liquidated damages in the amount of EUR500 for each day that the documents and materials are outstanding and due and payable to the Purchaser.

12.5 The Supplier shall do all things necessary to assist the Purchaser in complying with any obligations the Purchaser may have in connection with any sustainability or environmental reporting legislation, regulations, or rules in connection with any Products.



KONE SUPPLIER CODE OF CONDUCT

INTRODUCTION

KONE wants to be an attractive business partner and seeks reliable and fair relations with its suppliers for the mutual benefit of KONE and its suppliers. KONE expects from its suppliers competence and continuous improvement in quality, cost control, innovation, reliability, and sustainability.

The KONE Supplier Code of Conduct ("Code") illustrates the values according to which KONE operates globally. KONE expects its suppliers to comply with the requirements of the Code in their dealings with KONE, their own employees and suppliers, as well as third parties including government officials.

1. LEGAL COMPLIANCE

The supplier shall comply with all applicable laws and regulations.

The Code is not a substitute for, nor should it be considered to override, applicable laws and regulations, but sets the minimum standards of behavior that are to be followed by the supplier. To the extent the supplier is unable to comply with the Code due to laws and regulations, the supplier shall, to the extent reasonably possible, adhere to the spirit of the Code.

If local customs or practices are in contradiction with the Code, the supplier shall comply with the Code.

2. BUSINESS CONDUCT

2.1 Ethical Conduct

The supplier shall in all its operations be committed to high ethical standards in its business practices and shall prohibit any corrupt or fraudulent practices or money laundering activities.

2.2 Prohibition of Corrupt Practices

KONE expects its suppliers to have zero tolerance towards bribery and corruption. The supplier shall ensure that its directors and employees or any third parties acting on its behalf do not offer, promise, give or accept any bribes, or make or accept improper payments to obtain new business, retain existing business, or secure any other improper advantage. In particular, the supplier shall not engage in any form of bribery or kickback scheme or otherwise offer any incentive to KONE employees or their family or friends in order to obtain or retain any business.

The supplier should not provide any gift, corporate hospitality (including business lunches, dinners or entertainment) or other benefit to, or at the request of, a KONE employee in any situation in which it might influence, or appear to influence, an employee's decision in relation to the supplier.

KONE employees are not permitted to accept gifts, corporate hospitality or other benefits from a supplier who is involved in any ongoing or imminent tender or contract negotiations with KONE, or if the employee is in a position to influence the choice of supplier.

In other circumstances, suppliers may offer modest business courtesies, provided they comply with applicable laws, and are limited in their scope, value and frequency. Cash or equivalent, such as gift cards, can never be offered. Supplier must never provide any gifts, corporate hospitality or other benefits to a KONE employee's family members.

2.3 Conflicts of Interest

The supplier should avoid any interaction with KONE employees that may conflict, or appear to conflict, with that employee's duty to act in the best interests of KONE. The supplier shall disclose to KONE all conflicts of interest or situations giving the appearance of a conflict of interest in its engagement with KONE.

The supplier must inform KONE if a KONE employee or his/her immediate family member holds a material financial or other interest in the supplier, holds a managerial position at the supplier, or works for the supplier.

2.4 Fair Competition

The supplier shall compete in a fair manner in compliance with all applicable competition laws and regulations. For example, the supplier shall not enter into any agreements with its competitors to increase prices or to restrict the availability of products.

3. TRADE COMPLIANCE

The supplier shall comply with all applicable export control laws and regulations, including but not limited to international trade sanctions issued by the UN, EU or US authorities.

The supplier is required to inform KONE without undue delay if (i) the supplier itself, its immediate owner or ultimate beneficial owner, or any director, officer or representative of the supplier, is or becomes subject to international trade sanctions or restrictions, or (ii) the supplier becomes subject to a sanctions compliance investigation, or (iii) the supplier is or becomes aware that any of the products, software or technology it supplies to KONE is subject to any export controls or export license requirements.

The supplier is required to provide KONE upon request with information about the manufacturing location of the products it supplies to KONE together with proof of origin.

4. LABOR AND HUMAN RIGHTS

The supplier is expected to respect internationally recognized human rights, including those set out in the International Bill of Human Rights, the UN Guiding Principles on Business and Human Rights, and the principles set out in the International Labour Organization's Declaration on Fundamental Principles

and Rights at Work.

4.1 Non-discrimination

The supplier shall treat its employees in a fair and equal manner. The supplier shall not discriminate in the hiring, compensation, promotion, discipline, termination or retirement of employees based on gender, gender identity, age, religion, marital status, sexual orientation, disability, social class, political opinion, or national or ethnic origin, or any other characteristic that does not relate to the individual's qualifications or the inherent requirements for the job.

4.2 Child or Forced Labor

The supplier shall not use workers under the age of 15 or under the local legal minimum age for work or mandatory schooling age, whichever is higher. No young worker shall do work that is mentally, physically, socially or morally dangerous or harmful or interferes with their schooling by depriving them of the opportunity to attend school. The supplier shall under no circumstances use forced labor (including trafficked, indentured, or bonded labor) or contract with subcontractors or suppliers using child labor or forced labor. Mental and physical coercion, slavery and human trafficking are prohibited.

4.3 Respect and Dignity

The supplier shall treat its employees with dignity and respect and shall ensure that no worker is subject to any physical, sexual, psychological or verbal harassment, abuse or other form of intimidation.

4.4 Terms of Employment

The supplier shall ensure that compensation paid to its employees (including contractors, temporary or part-time employees) complies with all applicable wage laws, including those relating to minimum wages, overtime hours, paid leave and mandatory benefits. The supplier shall ensure that all employees are provided with employment documents that are freely agreed and which respect their legal and contractual rights.

4.5 Freedom of Association

The supplier shall respect its employees' right to freely associate and bargain collectively in compliance with all applicable laws and regulations. Employees shall not be intimidated or harassed in the exercise of their legal right to join or refrain from joining any organization.

4.6 Grievances

The supplier shall provide its employees with the means to raise their concerns about any of the compliance requirements outlined in this Code, and any employee who make such a report in good faith shall be protected from retaliation.

4.7 Community Rights

The supplier shall respect community rights, such as access to land, land usage rights and the right to a safe environment, in all its operations. The supplier should

assess, anticipate and avoid negative impacts on local communities within which it operates whenever possible, with a particular emphasis on vulnerable groups such as children, ethnic minorities and indigenous people

5. HEALTH AND SAFETY

The supplier shall ensure that its employees have a safe and healthy working environment in compliance with all applicable laws and regulations.

Appropriate health and safety information, training and equipment shall be provided to the supplier's employees. The supplier shall also have effective safety programs in place covering at least human safety, emergency preparedness and exposure to dangerous chemicals, biological substances, epidemics and pandemics. The supplier's employees shall not be under the influence of alcohol or drugs while working for KONE.

6. ENVIRONMENT

The supplier shall make all reasonable efforts to protect the environment, and to minimize any negative environmental impact of its activities.

The supplier shall comply with all applicable environmental laws and regulations, as well as any KONE requirements regarding the prohibition, restriction, labeling for recycling or disposal of specific substances, as specified in the Environmental Annex to the Supply and Purchase Agreement.

The supplier shall obtain, maintain and comply with all environmental permits, licenses and registrations necessary for its operations. The supplier shall monitor, control, minimize and appropriately treat emissions and pollutants (to air, soil and water) and other waste generated from its operations. The supplier shall strive to continuously reduce the carbon footprint of its operations through actions such as improving energy efficiency, sourcing renewable energy and eliminating, reducing and recycling waste.

The supplier shall have an appropriate, structured and systematic approach to managing its environmental responsibilities that includes, if applicable, establishing a suitable environmental management system.

7. IPR AND PUBLICITY

The supplier shall comply with all applicable laws and international treaties on intellectual property rights. The supplier shall not infringe KONE's or any third party's intellectual property rights.

Unless otherwise agreed, the supplier is not entitled to publicize its cooperation with KONE or utilize KONE trademarks without the express prior written consent of KONE.

8. MONITORING AND REPORTING

The supplier shall regularly monitor its compliance with the Code.

The supplier shall upon request provide KONE access to all relevant information and documents needed to verify the supplier's compliance with the Code. Should KONE have a reason to believe that the supplier may be in breach of the Code

(e.g. based on media reports), KONE may itself or through a third-party auditor survey the supplier's relevant premises to validate the supplier's compliance with the Code.

Should the supplier have, in the reasonable opinion of KONE, materially violated the Code, KONE is entitled to terminate the business relationship with the supplier with immediate effect.

If the supplier becomes aware of a breach of any of the requirements of the Code by its own employees or KONE employees, the Supplier shall inform KONE as soon as possible. If the supplier is unable to discuss the matter with KONE Sourcing, reports can be sent to compliance@KONE.com or made (anonymously where permitted by local law) via the KONE Compliance Line reporting channel:

<https://www.speakupfeedback.eu/web/konesuppliers/>.

9. APPLICABILITY

By agreeing to work with KONE the supplier confirms that it and its affiliates comply with the Code. An "affiliate" refers in this Code to a company that is controlled by the supplier, controls the supplier or is under common control with the supplier.

The supplier shall ensure that its suppliers, sub-contractors, consultants and partners comply with the principles of the Code.

Acknowledged and approved

Place _____ Date _____

Company name _____

Signature _____

Company registration number _____

1. GENERAL

- 1.1 This Annex is in addition to, and not in lieu of, other requirements of the Agreement. The Supplier shall ensure that all Products and Services provided to KONE comply with the requirements set out in this Annex. (*Products* and *Services* are used in this document to refer to any service, product or deliverable provided by the Supplier)
- 1.2 The Supplier shall comply with applicable laws and regulations for information security and privacy. The Supplier shall design and deliver the Products and Services in a manner consistent with good industry practices such as ISO 27001/27002, SOC 2 Type 2 for service organizations and ISO 22301 for business continuity management and disaster recovery.
- 1.3 Within 3 days from a request by KONE, the Supplier shall provide evidence of its compliance with the requirements of this Annex.
- 1.4 In addition to any other remedies that KONE may have, if any non-compliance is observed with the requirements of this Annex, the Supplier shall implement appropriate remediations at its own cost and without delay.
- 1.5 The Supplier shall document any identified security risks related to the provision of Products and Services and to KONE's information, which show the nature and extent of the risks, and progress in mitigating them.
- 1.6 If the Supplier performs services at KONE premises, the Supplier shall comply with all KONE safety, security and confidentiality instructions. If the Supplier's devices are used, the Supplier shall ensure devices are operated and configured securely to protect KONE data. If the Supplier uses KONE's devices, the Supplier shall follow all KONE policies and instructions relating to secure use.

2. GOVERNANCE

- 2.1 Supplier shall implement an internal information security policy across the Supplier's organization, which aligns with common industry good practices and standards for information security (e.g., ISO27001, NIST CSF, ISF Standard of Good Practice), and shall regularly review and keep the policy up to date.
- 2.2 Supplier shall provide KONE a point of contact for security related matters.

3. ASSET MANAGEMENT

- 3.1 The Supplier shall maintain an up-to-date asset inventory of all IT systems that are used to process or store KONE information and systems that are otherwise related to the Products and Services, and ensure that all assets have a designated owner.
- 3.2 The Supplier shall ensure that KONE information and assets are not used for any purposes other than those set out in the Agreement, unless KONE has provided a prior written consent.

4. IDENTITY AND ACCESS MANAGEMENT

- 4.1 The Supplier shall use industry good practices for identity and access management and have security controls in place to ensure only authorized people can access KONE information and systems used in the provision of the Products and Services.
- 4.2 The Supplier shall: (i) maintain system logon activity for systems that are used to access KONE information; (ii) ensure access rights are reviewed no less regularly than on a monthly basis; (iii) ensure an audit trail is logged and retained for a minimum of 180 days.
- 4.3 The Supplier shall provide access to KONE information for the Supplier's own personnel only on a need-to-know basis and timely remove the access when it is no longer needed.
- 4.4 The Supplier shall ensure that multi-factor authentication (MFA) configured according to good practices is used when remotely accessing KONE information and systems.

5. SECURE CONFIGURATION

- 5.1 The Supplier shall ensure all configurations (including security configurations) of hardware, software, Services, and networks are established, documented, implemented, monitored and reviewed.
- 5.2 The Supplier shall ensure that its hardware, software, services, and network configurations are hardened according to good security practices (for example using the Center of Internet Security's (CIS) benchmarks).

6. SYSTEM AND NETWORK SECURITY

- 6.1 The Supplier shall ensure its networks and network devices relevant to the Products and Services are secured and managed according to a formal process.
- 6.2 The Supplier shall ensure use of utility programs capable of overriding system and application controls is tightly restricted and controlled.
- 6.3 The Supplier shall ensure that any changes to the Supplier's information processing facilities and information systems related to the Products and Services are subject to formal change management procedures.
- 6.4 The Supplier shall implement security measures for when personnel are working remotely, and shall protect KONE information accessed, processed or stored outside the organization's premises.
- 6.5 The Supplier shall ensure that any endpoints (e.g., laptops, mobile devices, servers) that are used to process, store or access KONE information are secured.
- 6.6 The Supplier shall apply malware protection to all systems processing, storing or accessing KONE information.

7. THREAT AND VULNERABILITY MANAGEMENT

- 7.1 The Supplier shall prevent exploitation of technical vulnerabilities by implementing a process to evaluate exposure to technical vulnerabilities and take appropriate measures to mitigate them. The Supplier shall notify KONE of any critical vulnerabilities that require actions from KONE.

- 7.2 The Supplier shall regularly update its systems according to a formalized patch management procedure.
- 7.3 If there are integrations from systems fully managed by the Supplier to KONE managed systems, the Supplier must immediately notify security@kone.com of any vulnerabilities that might have an impact on KONE systems.
- 7.4 If requested by KONE, Supplier shall evaluate presence of any specific critical security vulnerabilities in the Supplier systems and remediate them without undue delay.

8. INFORMATION PROTECTION

- 8.1 The Supplier shall clearly identify all KONE Information, treat all KONE Information as confidential unless agreed otherwise, and limit access to authorized personnel.
- 8.2 The Supplier shall use current industry-standard strong encryption when processing, transmitting and/or storing KONE's personal data, customer data or other confidential KONE information. The Supplier shall define and implement rules for effective use of cryptography, including key management.
- 8.3 The Supplier shall not share KONE data with other third parties unless provided for in the Agreement, or KONE has provided prior written consent to do so.
- 8.4 If the Supplier uses cloud services as part of the Services provided to KONE, the Supplier shall ensure that KONE information, including personal information, is protected from unauthorized access, use, disclosure, alteration, or destruction.

9. INCIDENT MANAGEMENT

- 9.1 The Supplier shall have a formal process in place, along with clear and communicated responsibilities, to prepare for and timely respond to security incidents.
- 9.2 The Supplier shall immediately notify KONE of any breach or suspected breach of security or privacy (such as compromise of KONE's material or Information, or an incident affecting a Services and Products provided by the Supplier), by email to security@kone.com. The Supplier shall also provide KONE with regular updates on handling the incidents.
- 9.3 The Supplier shall deliver a report of the security incident investigation for incidents adversely affecting KONE as well as the root cause analysis with suggestions for corrective actions to be taken to remediate the situation.

10. SECURITY EVENT MANAGEMENT

- 10.1 The Supplier shall monitor all networks and systems related to the Products and Services for anomalous behavior and take appropriate actions to react to and evaluate potential security incidents.
- 10.2 The Supplier shall produce, store, protect and analyze all logs that record activities, exceptions, faults and other relevant events for systems that process or store KONE information or are used in the provision of Products and Services to KONE.

11. HUMAN RESOURCE SECURITY

- 11.1 The Supplier shall ensure that individuals with access to KONE information and systems (including subcontractors) are trustworthy and meet established security criteria for those positions.
- 11.2 The Supplier shall provide Information security and privacy awareness training to all Supplier personnel (including subcontractors) as relevant to their role in providing the Products and Services (in particular individuals that work with KONE's confidential and secret information (e.g., R&D data, customer data, financial data)).

12. PHYSICAL SECURITY

- 12.1 The Supplier shall ensure that only authorized persons have access to the Supplier's locations where KONE information or other KONE assets are managed.
- 12.2 The Supplier shall identify all physical and environmental threats, and design relevant controls to prevent potential consequences of such disruptions to the Supplier premises.
- 12.3 When handling unpublished KONE products or other sensitive material or information, the Supplier shall arrange visibility limitations (window shades, frosted glass, etc.), and shall ensure there is no unauthorized exposure.

13. LEGAL AND COMPLIANCE

- 13.1 If the Supplier operates in China, or stores or processes personal data of Chinese personnel, the Supplier shall ensure that it complies with the PIPL (The China Personal Information Protection Law).

14. CONTINUITY

- 14.1 The Supplier shall maintain business continuity management and disaster recovery plans and processes covering their overall operations related to the Products and Services, and ensure agreed SLAs (Service Level Agreements) are met. The Supplier shall test, update and exercise the plans regularly. Plans must at minimum address:
 - how business operations are restored within a reasonable time-period (based on SLAs) following an interruption to or failure to processes related to Service delivery, how operations are restored within an agreed time period, and how information security will be maintained during the disruption
 - Arrangements to engage relevant KONE personnel when executing them
- 14.2 The Supplier shall conduct business impact analysis, identify business continuity risks, and take necessary actions to control and mitigate such risks related to the Products and Services.
- 14.3 The Supplier shall make data backups and store them in a secured storage, and shall ensure the capability to fulfill KONE business continuity requirements during emergency situations.
- 14.4 The Supplier shall have the capability and resources to provide support for any of their legacy systems, platforms, and applications that KONE is using. This includes also support for managing technical vulnerabilities.

15. INFORMATION SECURITY ASSURANCE

- 15.1 The Supplier shall implement a process to monitor and review compliance with the Supplier's information security policy.

16. SECURE DEVELOPMENT

- 16.1 If the Supplier provides KONE any software solutions, the Supplier must have a formal and comprehensive Secure Development Lifecycle (SDLC) process in place that is designed to identify and mitigate security risks throughout the software development process and the Supplier must be able to provide documentation of the process upon request by KONE
- 16.2 The Supplier shall separate development, testing, and production environments, and shall protect any production environments and data from being compromised. If the Supplier uses any sensitive data (such as Personally Identifiable Information (PII)) in development or test environments, the Supplier shall use data masking to protect and hide the sensitive data.

SERVICE SPECIFIC ADDITIONAL REQUIREMENTS

17. CLOUD SECURITY

- 17.1 The Supplier shall ensure that KONE's data is logically segregated in multi-tenant cloud environments and ensure KONE data is only accessible to authorized personnel.
- 17.2 The Supplier shall provide user registration and deregistration functions, and specifications for the use of these functions to KONE.
- 17.3 The Supplier shall provide access controls that allow KONE to restrict access to its cloud services, its cloud service functions, and KONE information maintained in the service.
- 17.4 The Supplier shall provide secure authentication techniques, such as Multi-Factor Authentication (MFA), for authenticating KONE cloud service administrators to the administrative capabilities of the cloud service.
- 17.5 The Supplier shall ensure that any of its utility programs which are capable of bypassing normal operating or security procedures is only used by authorized personnel, and that the use of such programs is reviewed and audited regularly
- 17.6 The Supplier shall ensure that all resources (e.g.: equipment, data storage, files, memory) which are no longer needed are securely disposed or reused.
- 17.7 The Supplier shall ensure that KONE data is stored and processed only in locations that have been approved by KONE and that comply with all relevant data protection laws.
- 17.8 The Supplier shall ensure that its Applications Programming Interfaces (APIs) are designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications). The Supplier shall ensure both its internal and external APIs can only be accessed by an authentication method.
- 17.9 The Supplier shall provide the specifications of its cloud backup capabilities to KONE upon request. The specifications shall include the following information, as appropriate:
- scope and schedule of backups

- retention periods for backup data
- procedures for verifying integrity of backup data
- procedures and timescales involved in restoring data from backup
- procedures to test the backup capabilities
- storage location of backups

18. SECURE DEVELOPMENT – CUSTOMIZED SOLUTIONS

- 18.1 KONE may review applied cryptography controls for KONE dedicated solutions developed by the Supplier.
- 18.2 The Supplier shall ensure read and write access to source code, development tools, and software libraries are appropriately managed, shall prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes, and shall maintain the confidentiality of KONE intellectual property.
- 18.3 The Supplier shall perform security testing on a regular basis, identify and mitigate any identified security vulnerabilities, and provide test results to KONE upon request.
- 18.4 The Supplier shall allow KONE or its designated security auditing partners to perform ad-hoc testing and application security reviews before any products developed for KONE are deployed to production. The Supplier shall bear the cost of correcting any deficiencies to be compliant with the Agreement and these security requirements.
- 18.5 The Supplier shall design, develop, deploy, and test all interfaces in accordance with good industry standards (e.g., OWASP Top 10 for Web Applications and OWASP Application Security Verification Standard).
- 18.6 If the Supplier is developing elevator or escalator control systems components or IoT components connected to control systems, the supplier shall follow a secure development process compliant with IEC 62443-4-1. Upon request from KONE, the Supplier shall provide evidence of following the process.