



DHL GROUP

INFORMATION SECURITY CODE OF PRACTICE FOR PARTNERS

Document Owner: DHL Group CISO

Version: 4.0

Date issued: August 2025

Document classification: public

Table of Contents
Part 1: DHL Group: Introduction to Security Requirements
Part 2: Mandatory Minimum Security Requirements
Table A – Minimum Security Requirements
Table B – Right to Audit for DHL Group
Part 3: Enhanced Security Requirements
Table C – Enhanced Security Requirements
Table D – Conditions of Supplier Access to DHL Group Internal Information and DHL Group Systems
Part 4: Definitions

Part 1: DHL Group: Introduction to Security Requirements

- 1) DHL Group uses, creates and stores a significant amount of data in the course of its business and must ensure that the confidentiality, integrity and availability of data, Services and Processes are protected. This explicitly includes IT (information technology) and OT (operation technology) domains. All Suppliers engaged with DHL Group are required to implement and maintain appropriate and effective safeguards and controls to ensure the security of DHL Group Systems and information.
- 2) Capitalized terms used in the IS COP shall have the meaning assigned to those terms in the definitions section at Part 4 of the IS COP, unless the context requires otherwise. Where the IS COP forms part of any agreement between the Supplier and a member of DHL Group, the definitions provided within the IS COP shall prevail over any conflicting definitions in the remaining part of such agreement, but only with regards to the interpretation of the IS COP.
- 3) Part 2 of the IS COP sets out mandatory minimum security requirements with which DHL Group expects the Supplier to comply. If the Supplier is unable to comply with these minimum security requirements, it will not be able to enter into any agreement with DHL Group.
- 4) Part 3 of the IS COP sets out enhanced controls with which all Suppliers should seek to comply. Further, if the Supplier meets any of the following criteria, then it must comply with the enhanced controls in Part 3 of the IS COP:
 - a) the Supplier Processes DHL Group Data using Supplier systems outside DHL Group premises; and /or
 - b) the Supplier has access to DHL Group Systems.
- 5) Where the Supplier Processes Personal Data on behalf of DHL Group and/or the Supplier Processes Personal Data outside of the European Economic Area, additional requirements and expectations pursuant to Data Protection Legislation will be included in the relevant agreement between the Supplier and the relevant member of DHL Group. To the extent that those additional measures overlap or conflict with requirements set out in the IS COP, the more stringent requirements of the two shall apply to the Supplier.
- 6) Suppliers providing Information and Communication Technology Products or Services to DHL Group must disclose the geographical locations (regions, countries) where such Products or Services are provided, including those provided by agents, contractors or sub-contractors.
- 7) Where the Supplier provides Services or Processes to DHL which are considered important, essential or critical under the applicable national legislation (such as, but not limited to, NIS2 legislation), the Supplier shall comply with the more stringent legal provisions.

Part 2: Mandatory Minimum Security Requirements

- 1) In addition to the below mandatory minimum security requirements, the Supplier should manage information security in accordance with the practices described in ISO 27001 (not necessarily certified) or other equivalent international standards.
- 2) Where any part of the Services are not covered by the scope of a current ISO 27001 (or IEC62443 in the OT / product domain) certification, Suppliers must be prepared to demonstrate, upon request, that they have implemented controls equivalent to Industry Standard Practices, including, but not limited to, ISO/IEC

27001 and IEC62443 (for Operational Technology (OT) used for DHL Services and Processes), in its then-current version (or in the version in effect at the time).

- 3) DHL Group may, at its own discretion, conduct information security audits relating to the supply of Services by the Supplier. Details regarding DHL Group's right to audit are set out below.
- 4) The Supplier shall comply with the mandatory minimum security requirements listed in the following table A.
- 5) When the Supplier provides products with digital elements, the Supplier must inform DHL Group of the guaranteed Support Period, during which the product will be monitored for vulnerabilities and incidents, and security updates will be provided free of charge. This Support Period will be incorporated into the product description and serve as a binding contractual agreement. Furthermore, the Supplier must provide a self-declaration of conformity with applicable EU standards (e.g. CE mark).

Table A – Minimum Security Requirements

Requirement	Expectation
General	
A.1 Preservation of confidentiality, integrity and availability	The Supplier is accountable for preserving the confidentiality, integrity, and availability of DHL Group Data preventing corruption or loss of DHL Group Data and any unauthorized access to the infrastructure where such data is hosted. The Supplier shall ensure that it, including its agents, contractors or sub-contractors, implements appropriate controls and reasonable procedures required to guard against unauthorized and/or unlawful use of DHL Group Data.
A.2 System security	The Supplier shall ensure that any system on which the Supplier holds any DHL Group Data, including back-up data, is a secure system that complies with Part 3 of the ISOP, and in particular only enables access to DHL Group Data in electronic form to Supplier Personnel to the extent necessary to provide the Services.
Requirement	Expectation
Information and Cyber Security Protection	
A. 3 Protecting Information	The Supplier must protect DHL Group Data throughout its lifecycle and continuously manage their cybersecurity. The Supplier shall maintain an inventory of DHL Group Data in the Supplier's possession (and also in the possession of any sub-contractor). Upon request the Supplier must provide DHL Group with evidence to demonstrate that controls are in place to protect and manage DHL Group Data in accordance with its classification.
A.3.1 Security Monitoring	The Supplier must monitor all systems that are used to host DHL Data or Services for incidents. The Supplier shall establish a rule-based system for incident detection that is able to correlate events from different information sources.
A.4 Information Security Testing	Where the Supplier hosts a web site or externally facing application which stores, Processes or transmits DHL Group Data or displays DHL Group branding, or where a DHL Group internal address space is extended to the Supplier's network, the following requirements shall apply. To the extent that the Supplier has agreed to comply with DHL

Requirement	Expectation
	Group requirements which overlap or conflict with the requirements set out below, the more stringent requirements of the two shall apply to the Supplier: 1) that security testing, including penetration testing, is performed by qualified and skilled personnel prior to applications being connected to untrusted or public networks; 2) there is a regular security testing schedule of the web site, occurring at a frequency of at least annually. DHL Group is to be informed of the times and dates of the security testing; 3) DHL Group is provided with a summary of the results of the annual penetration testing of the software platform provided to DHL Group, together with a list of remedial actions for each finding including its risk rating, where each action has a delivery date; and 4) progress on remedial action is reported upon request to DHL Group.
A.4.1 Vulnerability Remediation	The Supplier must promptly and at no charge to DHL Group remediate Vulnerabilities in their systems and products. For products with digital elements provided to DHL Group, the Supplier must ensure that DHL Group is informed about Vulnerabilities as they are discovered, that security updates are provided in a timely manner and that these updates, where technically feasible, are separated from feature updates.
Requirement	Expectation
Information Security Incident Management	
A.5 Response Plan	The Supplier shall maintain a written Information Security Incident response plan. The Supplier shall remedy each Information Security Incident in a timely manner following its Information Security Incident response plan in accordance with Good Industry Practice.
A.6 Notification Requirements	The Supplier must notify DHL Group of any Information Security Incident impacting any DHL Group Data or DHL Group Systems managed or interfaced by the Supplier within the timeframe established by applicable laws or regulation but not later than 24 hours after becoming aware of the Information Security Incident. The Supplier is expected to use reasonable efforts to provide a comprehensive report of the Information Security Incident and the related response as well as ensuring they reconstruct any lost or destroyed information without any charge to DHL Group. In the event of an Information Security Incident or a Personal Data breach (as defined by relevant Data Protection Legislation) impacting DHL Group Data, the Supplier must report this to supplier-cybersecurity@dhl.com, its designated DHL Group business contact and upon request by DHL Group any other communication channels specified by DHL Group.
A.7 Cooperation with DHL Group's Investigations	The Supplier shall reasonably cooperate with DHL Group in handling an Information Security Incident, including, but not limited to, the following: 1) coordinating with DHL Group on the Supplier's response plan; 2) assisting with DHL Group's investigation of the Information Security Incident; 3) facilitating interviews with the Supplier Personnel and others involved in the Information Security Incident or response; and 4) making available all relevant information required for DHL Group to comply with applicable laws, regulations, or industry standards, or as otherwise required by DHL Group.

Requirement	Expectation
A.8 Third party notifications	The Supplier agrees that it shall not notify any third party (including any regulatory authority or customer) of any Information Security Incident on behalf of DHL Group without first obtaining DHL Group's prior written consent, unless this violates any existing law or regulation. Further, the Supplier agrees that DHL Group shall have the sole right to determine: 1) whether notice of the Information Security Incident is to be provided to any individuals, regulators, law enforcement agencies, or others; and 2) the form and contents of such notice.
Requirement	Expectation
Data Protection Legislation Requirements for the Supplier	
A.9 Legal compliance	1) The Supplier shall adhere to applicable Data Protection Legislation, including provisions concerning the security of Personal Data, and to relevant regulations, such as GDPR; 2) The Supplier shall comply with all said requirements when Personal Data, in particular that of customers, consumers, employees and shareholders, is collected, recorded, hosted, Processed, transmitted, used, and / or erased; and 3) The Supplier shall comply with any contractual requirements on data protection and information security and shall not disclose any information that is not known to the general public.
Requirement	Expectation
Contract Termination	
A.10 Contract Termination	Upon termination of the contractual relationship and / or after expiration of the agreed retention period with DHL Group, the Supplier must: 1) irreversibly destroy all data, data carriers and documents, including data backups, not returned to DHL Group in compliance with applicable laws and regulations, in particular - but not limited to - data protection and privacy laws, e.g. the GDPR. Should retention be mandated by law, the Supplier must ensure secure storage with restricted access and irreversible deletion once the legal retention period expires; and 2) provide evidence upon request that access to DHL Group's systems (for the avoidance of doubt: under the Suppliers responsibility) and facilities has been revoked or altered and that all accounts utilized to provide Services for DHL Group have been deactivated.

- 6) DHL Group shall have the following audit rights over the Supplier. To the extent that the Supplier has agreed to audit rights for DHL Group which overlap or conflict with the rights set out below, the more extensive audit rights for DHL Group of the two shall be exercisable by DHL Group:

Table B – Right to Audit for DHL Group

Requirement	Expectation
B.1 Audit Access	The Services and IT systems provided by the Supplier shall be subject to audit by DHL Group (or any external auditors as DHL Group may appoint) within reasonable written notice (including, but not limited to, data processing agreements concluded by the Supplier being compliant with Data Protection Legislation). Audit activities may include providing Supplier with questionnaires for Supplier-self assessment, reviewing documentation, conducting interviews, evidence collection and analysis of delivered reports and process documents, physical/ remote audit or certification, provided that these activities do not require any access to view production/confidential data of the Supplier and/or its customers.
B.2 Audit Findings	The Supplier shall mitigate all findings identified in the audit within a commonly agreed timeframe and provide evidence of successful mitigation to DHL Group.
B.3 Evidence of Compliance	Upon request by DHL Group (not more often than once every twelve months), the Supplier shall provide evidence of compliance for the provisioned Services and IT systems in the form of independent review from third party auditors or industry recognized security assurance standards. The evidence provided shall comprise: 1) A copy of its annual certification of compliance with ISO 27001 and/or SSAE SOC2 or any equivalent reports; and 2) A summary of its vulnerability assessment and / or penetration testing reports relating to systems and processes involved in the provision of the Services. Confidential and / or data whose sensitivity is derived from classification or legal requirements may be removed in the report to protect the confidentiality of the Supplier's systems. However, the total number and severity of the identified issues shall be provided including risk mitigation measures and implementation timeline.
B.4 Requests for Information	Upon request by DHL Group, the Supplier must provide answers and evidence to DHL Group contained in a 'Request for Information' (Rfi) regarding the Supplier's information security and data protection risk and compliance as well as with respect to publicly accessible network addresses used to provide services for DHL.

Part 3: Enhanced Security Requirements

- 1) These enhanced security requirements set out in summary the technical and organizational information security control requirements that the Supplier must adopt when:
 - a) the Supplier is Processing DHL Group Data using Supplier systems outside DHL Group premises; or
 - b) the Supplier has access to DHL Group Systems.
- 2) These enhanced security requirements shall apply in addition to any requirements relating to information security practices and data protection standards set out in any agreement between the Supplier and DHL Group.

Table C – Enhanced Security Requirements

ISO Chapter/Control	Requirements
C.6 Organization of Information Security	The Supplier must have a coordinated approach to information security. In particular, the Supplier's information security management system must consist of the following: 1) A set of regularly reviewed information security policies that must be defined and implemented; 2) All information security responsibilities must be defined and allocated; 3) Conflicting duties and areas of responsibilities must be segregated to reduce opportunities for unauthorized and unintentional modification or misuse of DHL Group's assets; 4) Appropriate contacts with relevant authorities, special interest groups or other specialist security forums and professional associations, which must be maintained; 5) Information security measures must be addressed in project management, regardless of the type of project; 6) Defined security measures / controls to manage the risks introduced by using mobile devices and remote working; and 7) The policies for information security must be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. 8) The Supplier must establish and publicly publish a Responsible Disclosure Policy detailing the process for handling vulnerability reports. 9) If requested by DHL, an information security management working group must be established. This is made up of representatives of the Supplier and DHL and meets on demand of one of the parties.
C.7 Human Resource Security	The Supplier must have established measures to mitigate people security risks prior to employment, during employment, and after termination of employment. In particular, the Supplier must: 1) Carry out background checks and screening on all Supplier Personnel candidates, where legally permitted; 2) Incorporate Supplier Personnel information security responsibilities into contractual agreements, policies and procedures; 3) Deliver information security awareness education and training at a regular and defined interval; and

ISO Chapter/Control	Requirements
	4) Have formal disciplinary measures for Supplier Personnel who breach information security policies.
C.8 Asset Management	The Supplier must implement measures to manage information security assets throughout their lifecycle. In particular, the Supplier must: 1) Identify assets associated with information and information processing facilities including Embedded Technology and draw up and maintain an inventory of these assets; 2) Ensure assets maintained in the inventory have a named business owner; 3) Ensure rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented; 4) Ensure all Supplier Personnel and external party users return all of the DHL Group and/or Supplier assets (as applicable) in their possession upon termination of their employment, contract or agreement; and 5) Classify, label and handle information assets in terms of legal requirements, value, criticality and sensitivity.
C.9 Access control	The Supplier must implement access control measures to protect information assets and resources including Embedded Technology. In particular, the Supplier must: 1) Establish and implement policies and procedures for access control (including onboarding, off-boarding and cross boarding users) and privileged access management; 2) Provide access based on principle of least privilege and segregation of duties; 3) Define and communicate user responsibilities in the use of secret authentication information; 4) Review user access rights at regular intervals; 5) Restrict the use of utility programs that may be capable of overriding system and application controls; and 6) Implement password policies and usage of multifactor authentication technologies in line with risk and best practice.
C.10 Cryptography	The Supplier must implement cryptographic controls in alignment with industry-accepted standards in their current version. In particular, the Supplier must: 1) Define and implement a policy to define mandatory encryption measures in alignment with information classifications; and 2) Develop and enforce a policy governing the use, adequate length, protection, and lifespan of cryptographic keys, ensuring compliance with Industry Best Practices regarding entropy and key space utilization.
C.11 Physical and Environmental Security	The Supplier must have measures to maintain security within physical sites and premises (e.g. offices, warehouses, data centers). In particular, the Supplier must define and implement security controls to protect: 1) Physical security perimeter and points of entry; 2) Offices, rooms, facilities, secure areas and delivery and loading areas; 3) Equipment (e.g. operational technology), supporting utilities, power and telecommunication cabling; 4) Procedures for working in secure areas, which shall be designed and applied; and

ISO Chapter/Control	Requirements
	5) Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises. Access points shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
C.12 Operations Security	The Supplier must implement controls to protect information assets and information processing facilities including Embedded Technology. In particular, the Supplier must: 1) Define and implement policies and procedures for change management, capacity management, and operations; 2) Segregate development, testing, and operational environments; 3) Implement controls to detect, prevent and respond to malware; 4) Create, maintain, and ensure successful restore of backups of information, software and system images at regular and defined intervals; 5) Maintain event logs of user activities and system administrator / operator activities, and secure logs against unauthorized access; 6) Synchronize all information processing system clocks to a single reference time source; 7) Control installation of software on operational systems; 8) Identify and remediate technical vulnerabilities in a timely manner; and 9) Carefully plan audit requirements and activities involving verification of operational systems and agree to minimize disruptions to business processes. 10) Upon DHL's request, provide an up-to-date list of software and firmware (in sense of Software Bill of Material, SBOM), which is used in its services or assets (e.g. software name, software version, device and where it is used). 11) Ensure that devices or IT systems are hardened (e.g. system default user accounts are disabled or default passwords changed, ensure only permissions absolutely necessary for their execution assigned, unused / unnecessary features, services, interfaces, ports, and protocols disabled or removed, insecure features, services, interfaces and protocols like TELNET, FTP, HTTP, etc. disabled or removed).
C.13 Communications Security	The Supplier must implement controls to maintain the security of information that is Processed and transferred through networks. In particular, the Supplier must ensure the following: 1) Networks should be managed and controlled to protect information in systems and applications. Security mechanisms, service levels and management requirements of all network services must be clearly defined and included in network services agreements, regardless of whether these services are provided in-house or outsourced. Segregation of information services, users and information systems on networks is essential. Formal transfer policies, procedures and controls should be established to protect information transfer across all communication channels; 2) Agreements should address the secure transfer of business information between the Supplier and external parties; 3) Information involved in electronic messaging should be appropriately protected; and

ISO Chapter/Control	Requirements
	4) Requirements for confidentiality agreements reflecting the Supplier's needs for the protection of information should be identified, regularly reviewed and documented.
C.14 System Acquisition, Development and Maintenance	The Supplier must integrate information security controls into all information systems and throughout the software development lifecycle. In particular, the Supplier must ensure the following: 1) Rules for the secure development of software and systems should be established and applied to developments within the Supplier; 2) When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on Supplier and/or DHL Group (as applicable) operations or security; 3) Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled; and 4) The Supplier should supervise and monitor the activity of outsourced system development.
C.15 Supplier Relationships	The Supplier must manage risks associated with contracting third-party Suppliers (i.e. fourth parties to DHL Group) that may access, Process, or store the Supplier's information assets. In particular, the Supplier must: 1) Have a third-party risk management policy that defines information security requirements to mitigate third party risks; 2) Establish and formally agree (i.e. within legally binding contracts) information security requirements with each third-party Supplier; 3) Regularly monitor, review and audit each third-party Supplier's service delivery; and 4) Manage changes to provision of services by third-party Suppliers through maintenance of information security policies, procedures and controls.
C.16 Information Security Incident Management	The Supplier must have an established and documented process for identifying, assessing and responding to Information Security Incidents. In particular, the Supplier must: 1) Define roles and responsibilities pertaining to Information Security Incident management, including identifying key dependencies and escalation points; 2) Establish and communicate channels for reporting information security events (whether or not they are Information Security Incidents) or identified vulnerabilities / weaknesses; 3) Implement a methodology for triaging and classifying Information Security Incidents; 4) Conduct post-incident analysis exercises to continuously improve the Information Security Incident management process; and 5) Document and preserve evidence pertaining to an Information Security Incident.
C.17 Information Security Aspects of Business Continuity Management	The Supplier must embed information security continuity and resilience measures within its business continuity management systems. In particular, the Supplier must: 1) Develop policies, processes and plans to ensure information security continuity and continuity of information security management in adverse situations;

ISO Chapter/Control	Requirements
	2) Conduct and document the results of testing of business continuity plans at regular and pre-defined intervals to ensure information security continuity controls are functioning as required; and 3) Implement redundancy measures to maintain availability of information processing facilities.
C.18 Compliance	The Supplier must ensure compliance with legal and contractual obligations and ensure internal compliance with information security policies and procedures. In particular, the Supplier must: 1) Define a governance cadence (i.e. required frequency of review) over the organization's approach to managing and implementing information security Good Industry Practice; and 2) Conduct reviews at regular and pre-defined intervals to assess compliance with information security policies, processes and standards.

3) Where the Supplier requires access to DHL Group internal information and systems the following apply:

Table D – Conditions of Supplier Access to DHL Group Internal Information and DHL Group Systems

Requirement	Expectation
D.1 Access on a need-to-know basis	The Supplier's access to any DHL Group Data shall only be granted to the Supplier when a need to know exists and when such a disclosure has been expressly authorized by a representative of DHL Group.
D.2 Legitimate and documented business need	Inbound access to DHL Group Systems shall only be granted to the Supplier where the relevant DHL Group System manager determines that the Supplier has a legitimate and documented business need for such access, and the systems of the Supplier provide no significant threat to any part of DHL Group infrastructure. The Supplier access shall only be enabled for specific individuals and only for the time period required to accomplish approved tasks.
D.3 Follow DHL Group network access onboarding procedures	The Supplier shall follow DHL Group System access onboarding procedures to obtain inbound access to DHL Group Systems. Such procedures include required information provision as part of network configurations including, but not limited, to IP addresses, network protocol, and network access implementation method (e.g. VPN setup).
D.4 Documentary evidence of an Information Security Management System	Before access can be issued to the Supplier for the period of engagement, documentary evidence of an information security management system or process compliant with ISO 27001 or other equivalent international standards shall be provided and the Supplier shall agree in writing to prevent unauthorized and improper use of DHL Group Systems made available to the Supplier.
D.5 Immediate termination	DHL Group also reserves the right to immediately terminate network connections with all Supplier systems if DHL Group believes either that the Supplier is not meeting these requirements, or if the Supplier is providing an opportunity for attack against DHL Group Systems.
D.6 Documented security architecture	The Supplier shall maintain documented security architecture of the networks managed by the Supplier in its operation of the Services provided to DHL Group. The Supplier shall review the network architecture, including measures designed

Requirement	Expectation
	to prevent unauthorized network connections to all systems, applications, and network devices on a regular basis (i.e. at least once a year).
D.7 Separation of DHL Group Systems and Supplier systems and infrastructure	When Supplier hosts DHL Group Systems or DHL Group information is stored or processed on Supplier's Systems, these Supplier Systems shall be strictly separated from the Supplier's internal systems and infrastructure.
D.8 Data logging	The Supplier shall collect all logging data relating to DHL Group (proof, evidence of actions) and shall provide this data to DHL Group upon request.

Part 4: Definitions

1) The definitions in this Part 4 apply to the IS COP.

"Affiliate"	(i) in relation to DHL Group, a legal entity which, presently or in the future, directly or indirectly, is Controlled by Deutsche Post AG or under common Control with Deutsche Post AG; and (ii) in relation to the Supplier, a legal entity which, presently or in the future, directly or indirectly, is Controlled by the Supplier or under common Control with the Supplier;
"Control" or "Controlled"	the controlling entity possessing, directly or indirectly, or jointly with a third party or parties, the power to direct management and policies of the controlled entity;
"Data Protection Legislation"	GDPR; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and, to the extent applicable, all other applicable laws and regulations of any other country relating to the Processing of Personal Data and privacy;
"DHL Group Data"	all data or records of whatever nature and in whatever form relating to the business, employees, customers, Suppliers or otherwise relating to the business of DHL Group;
"DHL Group"	Deutsche Post AG and any Affiliate of Deutsche Post AG from time to time and a reference to DHL Group in the IS COP shall be construed as a reference to all and any of them. It includes the relevant member of the DHL Group that is a party to any agreement with the Supplier to which the IS COP forms part of such agreement;
"DHL Group Systems"	the information technology and communication systems, including networks, hardware, software, middleware, virtual platforms, embedded technology (see definition below) and interfaces owned by or licensed to DHL Group or any of its or their agents, customers or contractors;
"Embedded Technology"	Embedded Technology Devices are physical objects used for monitoring and / or affecting the physical environment with sensors, data storage and / or processing ability, internal software, and / or the ability to exchange data with other devices and systems over an IT network.
"GDPR"	Regulation (EU) 2016/679 (the General Data Protection Regulation), including any amendments and updates in force from time to time;

“Good Industry Practice”, “Industry Best Practices” and “Industry Standard Practice”	in respect of any activity, performing that activity effectively, reliably and professionally using the degree of skill, care, diligence, prudence, foresight and judgement which would reasonably be expected from a skilled and experienced operator of similar standing engaged in the provision of similar services;
“Information Security Incident”	1) any actual compromise of the confidentiality, integrity or availability of DHL Group Data; 2) any actual compromise of, or unauthorized access to, any system that Processes DHL Group Data that presents a risk to the confidentiality, integrity or availability of DHL Group Data; or 3) receipt of a complaint, report, or other information regarding the potential compromise or exposure of DHL Group Data Processed by Supplier;
“Internet”	the global network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols;
“ISCOP”	DHL Group’s Information Security Code of Practice for Partners;
“Partner”	Suppliers, including subcontractors, i.e. all companies who do business with any company or division of DHL Group;
“Process” or “Processing” or “Processes”	any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
“Personal Data”	any personal data (as such term is defined in Data Protection Legislation) which is subject to the applicable Data Protection Legislation;
“Services”	any or all of the services provided by the Supplier;
“Supplier”	the counterparty to any agreement with DHL Group to which the ISCOP forms part of such agreement;
“Supplier Personnel”	the employees, contractors and other individuals who are engaged by the Supplier, its Affiliates or their subcontractors from time to time to meet the Supplier’s obligations; and
“Web based applications”	A web-based application is a computer program that utilizes web browsers and / or web technologies (HTML, API and others) to perform tasks over a computer network.