[附件_____]

数据处理和转让协议

本数据处理和传输协议（"DPTA"）作为_____（"协议"）的一部分，由柯林斯宇航（统称为"柯林斯"）的一部分_____，与_____及其子公司和关联公司（统称为"供应商"）之间签订。

1. 本《DPTA》特此纳入协议并构成协议的一部分。本《DPTA》中大写的术语应具有第2条（或本《DPTA》中的其他位置）赋予这些术语的含义。如果没有其他定义，应具有其普通和习惯的含义。本《DPTA》将取代双方之前就本协议主题达成的任何协议，包括柯林斯和供应商之前根据《中华人民共和国个人信息保护法》签订的所有数据传输协议。

2. 以下定义适用于本节：

(a) "数据隐私法"是指与数据隐私、个人信息或数据的保护以及个人信息或数据的跨境转移有关且适用的国家、联邦、州和省法律，包括但不限于中华人民共和国《个人信息保护法》（"PIPL"）规定的隐私和安全法律和法规。

(b) "柯林斯个人信息"应指提供给供应商或其代理人、代表或分包商的与协议以及协议项下的交易有关的、与任何已识别或可识别的自然

[Exhibit ___]

DATA PROCESSING AND TRANSFER AGREEMENT

This Data Processing and Transfer Agreement ("DPTA") is made a part of the _____ (the "Agreement") by and between _____, a part of Collins Aerospace (collectively, "Collins"), and _____ and its subsidiaries and affiliates (collectively, "Supplier").

1.This DPTA is hereby incorporated into and forms a part of the Agreement. Capitalized terms in this DPTA shall have the meanings ascribed to such terms under Section 2 (or in other locations throughout this DPTA), and, if not otherwise defined, shall have their ordinary and customary meanings. This DPTA will supersede any previous agreements between the Parties as to the subject matter herein, including all prior data transfer agreements entered into between Collins and Supplier pursuant to the People's Republic of China Personal Information Protection Law.

2. The following definitions are applicable to this section:

(a)"Data Privacy Laws" shall mean applicable national, federal, state and provincial laws relating to data privacy, the protection of personal information or data, and the cross-border transfer of personal information or data, including, without limitation, the privacy and security laws and regulations of the People's Republic of China under the Personal Information Protection Law ("PIPL").

(b)"Collins Personal Data" shall mean any information or data provided to Supplier or its agents, representatives, or subcontractors in connection with the Agreement, and the transactions thereunder that relate to any identified or identifiable natural person, or, to the extent of a conflict with applicable law,

人有**关的任何信息或数**据，或者在与**适用法律**相冲突的情况下，受任何数据隐私法的约束。

that is subject to any Data Privacy Laws.

3. 供应商应：

3.Supplier shall:

(a) 遵守所有**适用的数据**隐私法，如果供应商认为收集或处理柯林斯个人信息违反了数据隐私法，应及时书面通知柯林斯。

(a)comply with all applicable Data Privacy Laws and promptly notify Collins in writing if Supplier believes that collecting or processing Collins Personal Data violates Data Privacy Laws;

(b) 仅为履行协议项下的义务，遵照柯林斯的指示或遵守法律义务之目的，才会按照附件1（附于本DPTA并成为本DPTA的一部分）所述的方式收集、访问、使用或分享柯林斯个人信息，或将柯林斯个人信息转让给经授权的第三方。供应商不会对柯林斯个人信息进行任何二次使用或其他使用（例如用于数据**挖掘**），**除非**（i）得到柯林斯的明**确**书面授权，（ii）遵守法律要求。

(b)only collect, access, use, or share Collins Personal Data, or transfer Collins Personal Data to authorized third parties, in performance of its obligations under the Agreement, in the manner as described in Exhibit 1 (attached hereto and made a part of this DPTA), in conformance with Collins's instructions, or to comply with legal obligations. Supplier will not make any secondary or other use (e.g., for the purpose of data mining) of Collins Personal Data except (i) as expressly authorized in writing by Collins , (ii) as required by law;

(c) 不与任何第三方分享、转让、披露或提供对柯林斯个人信息的访问，除非根据协议提供服务或遵守法律规定。如果供应商确实与第三方分享、转让、披露或提供对柯林斯个人信息的访问，则应：

(c)not share, transfer, disclose or provide access to Collins Personal Data to any third party except to provide services under the Agreement or as required by law. If Supplier does share, transfer, disclose or provide access to Collins Personal Data to a third party, it shall:

(i) 对任何分包商或其他此类第三方的作为和疏忽负

(i)be responsible for the acts and omissions of any subcontractor or other such third party, that processes (within the meaning of the applicable Data Privacy Laws) Collins Personal Data on Supplier's behalf in the same

责，这些分包商或第三方代表供应商处理（基于**适用的数据**隐私法界定的含义）柯林斯个人信息，其方式和程度与供应商对其自身与此类柯林斯个人信息有**关的**作为和疏忽负责的方式和程度相同。

manner and to the same extent as it is responsible for its own acts and omissions with respect to such Collins Personal Data;

(ii) **确保**该第三方受到书面协议的约束，该协议包含与本节规定的相同或相当的义务和保护措施；以及

(ii)ensure such third party is bound by a written agreement that contains the same or equivalent obligations and protections as those set forth in this Section; and

(iii) 只有在符合**适用**的数据隐私法的情况下，才与第三方分享、转让、披露或提供访问。

(iii)only share, transfer, disclose or provide access to a third party to the extent that such conduct is compliant with applicable Data Privacy Laws;

(d) 采取商业上合理的步骤，**确保能接触到柯林斯**个人信息的供应商的雇员、代理人、代表、分包商、分包商雇员或供应商使用的任何其他人员（统称为"供应商人员"）的可靠性，并**确保供**应商人员有义务对柯林斯个人信息进行保密，例如通过签订保密协议或适用相关法律或规定。

(d)take commercially reasonable steps to ensure the reliability of Supplier's employees, agents, representatives, subcontractors, subcontractor employees, or any other person used by Supplier (collectively, "Supplier Personnel") who have access to the Collins Personal Data and and ensure that Supplier Personnel are obligated to maintain the confidentiality of Collins Personal Data, such as through a confidentiality agreement or by application of relevant law or regulation;

(e) 提供柯林斯可能不时合理要求的信息、协助和

(e)provide such information, assistance and cooperation as Collins may reasonably require from time to time to establish Supplier's

	合作，以**确定供**应商对数据隐私法的遵守。	compliance with Data Privacy Laws;
(f)	根据柯林斯的要求，允许柯林斯聘请第三方外部审计人员，以核实供应商和第三方对其在本协议下义务的遵守情况。此外，应柯林斯的要求，供应商应向柯林斯提供任何根据ISO 27001、ISO 29100、SSAE 16（或SAS 70）、SSAE 18、SOC 2或ISAE 3402发布的涉及柯林斯个人信息的审计报告。	(f)upon Collins's request, permit Collins to hire third party external auditors to verify Supplier and third party compliance with their obligations hereunder. Additionally, upon request, Supplier shall provide Collins with any audit reports issued under ISO 27001, ISO 29100, SSAE 16 (or SAS 70), SSAE 18, SOC 2, OR ISAE 3402 that covers Collins Personal Data;
(g)	将保持合理和**适当的技**术、物理和管理措施，以本协议附件2（附后并成为本协议的一部分）中所述的方式保护柯林斯个人信息。这些措施将包括合理地限制对包含柯林斯个人信息的任何地点的物理访问，如将这些记录储存在上锁的设施、储存区或容器中。供应商必须定期重新评估所采取的措施，以**确保其保持合理和适**当。	(g)will maintain reasonable and appropriate technical, physical, and administrative safeguards intended to protect Collins Personal Data in the manner as described in Exhibit 2 of this Agreement (attached hereto and made a part hereof). These measures will include reasonable restrictions upon physical access to any locations containing Collins Personal Data, such as the storage of such records in locked facilities, storage areas, or containers. Supplier must periodically re-evaluate the measures adopted to ensure that they remain reasonable and appropriate;
(h)	向柯林斯提供商业上合理的协助，以便：	(h)provide Collins with commercially reasonable assistance in:
	(i) 应个人或法律代表的要求，删除柯林斯个人信息；以及	(i)deleting Collins Personal Data in response to a request by an individual or legal representative; and
	(ii) 根据柯林斯的书面指示，使个人能够选择退出。	(ii)enabling individuals to opt-out, pursuant to Collins's written instructions;

(i) 向与供应商有直接联系的个人提供隐私通知，除非供应商和柯林斯书面同意，隐私通知的义务完全由柯林斯负责。

(i)provide a privacy notice to individuals with whom the Supplier has direct contact unless Supplier and Collins agree in writing that the privacy notice obligation is solely Collins's responsibility;

(j) 根据柯林斯的书面指示，向柯林斯提供清除超过一年或双方书面同意的其他时间段的柯林斯个人信息的能力，除非**适用法律要求保留**这些资料；以及

(j)pursuant to Collins's written instructions, provide Collins with the ability to purge Collins Personal Data older than one year or such other time period agreed upon in writing by the parties, unless otherwise required to retain the data by applicable law; and

(k) 如果收到或获悉任何下列情况，立即书面通知柯林斯 (i) 针对柯林斯个人信息的投诉或指控表明违反了数据隐私法；(ii)一个或多个个人要求访问、纠正或删除柯林斯个人信息；(iii)一个或多个个人对收集、处理、使用或转让柯林斯个人信息进行查询或投诉；以及(iv)监管部门要求、传票、搜查令或其他法律、监管、行政或政府程序寻求柯林斯个人信息（统称"数据隐私事项"）。如果供应商得知任何数据隐私事项，供应商应向柯林斯提供协助，与柯林斯充分合作调查该事项，包括但不限于向柯林斯提供相**关信息**，**准**备回应，实施补救措施，和/或在进行任何索赔、法院或法定程序时进行合作和抗辩。柯林斯应负责就其柯林斯个人数据与个人进行沟通，除非柯林斯授权供应商代

(k)immediately advise Collins in writing if it receives or learns of any: (i) complaint or allegation indicating a violation of Data Privacy Laws regarding Collins Personal Data; (ii) request from one or more individuals seeking to access, correct, or delete Collins Personal Data; (iii) inquiry or complaint from one or more individuals relating to the collection, processing, use, or transfer of Collins Personal Data; and (iv) regulatory request for, subpoena, search warrant, or other legal, regulatory, administrative, or governmental process seeking Collins Personal Data (collectively, "Data Privacy Matters"). If Supplier learns of any Data Privacy Matters, Supplier shall provide assistance to Collins, fully cooperate with Collins in investigating the matter, including but not limited to, providing the relevant information to Collins, preparing a response, implementing a remedy, and/or cooperating in the conduct of and defending against any claim, court or regulatory proceedings. Collins shall be responsible for communicating with individuals regarding their Collins Personal Data in connection with such Data Privacy Matters unless Collins authorizes Supplier to do so on its behalf. Supplier shall use commercially and legally reasonable efforts to limit the nature and scope of the required disclosure to the minimum amount of Collins Personal Data required to comply with applicable law. Unless prevented by applicable law, Supplier shall provide Collins with advance written notice of any such Data Privacy Matters sufficient to allow Collins to contest legal, regulatory, administrative, or other governmental

表其这样做。供应商应在商业上和法律上做出合理的努力，将所需披露的性质和范围限制在遵守**适用法律所需的、**最低数量的柯林斯个人数据。除非**适用法律不**允许，否则供应商应提前向柯林斯提供任何此类数据隐私事项的书面通知，以使柯林斯能够对法律、法定、行政或其他政府程序提出**异**议。

processes.

4. 供应商应尽快向柯林斯提供书面通知，并尽可能在四十八（48）小时内将其了解到的任何实际或合理怀疑的意外或非法破坏或意外损失、更改、未经授权或意外披露或访问柯林斯个人信息的事件（"安全漏洞"）。如果供应商无法在四十八（48）小时内发出通知，供应商应向柯林斯提供**关于延**迟的解释，柯林斯将将此有权与监管机**构分享。供**应商应采取一切合理措施，尽可能控制和补救安全漏洞；向柯林斯提供有**关安**全漏洞的调查和补救的信息，除非受到法律限制。除非法律或法院命令要求，否则在未得到柯林斯对安全漏洞通知（如有）的内容、媒体和时间的事先书面同意和事先书面批准的情况下，不得进行任何通知、公告或发布或以其他方式授权播放任何有**关安全漏洞的通知**或信息（"漏洞通知"）；即使在法律或法院命令要求的情况下，在提供任何漏洞通知之前，应尽一切合理努力与柯林斯协调。如果安全漏洞(a)**涉及供**应商网络或系统上的数据或(b)是供应商的过错，那么供应商将

4.Supplier shall provide written notice to Collins as soon as possible and, whenever possible, in forty-eight (48) hours, of any actual or reasonably suspected incident of accidental or unlawful destruction or accidental loss, alteration, unauthorized or accidental disclosure of or access to Collins Personal Data of which it becomes aware (a "Security Breach"). If Supplier is unable to provide notice within forty-eight (48) hours, Supplier shall provide Collins with an explanation for the delay that Collins will be entitled to share with regulators. Supplier shall take all reasonable measures to contain and remedy the Security Breach, wherever possible; provide Collins with information regarding the investigation and remediation of the Security Breach, unless restricted by law; not make any notification, announcement or publish or otherwise authorize any broadcast of any notice or information about a Security Breach (a "Breach Notice") without the prior written consent of and prior written approval by Collins of the content, media and timing of the Breach Notice (if any), unless required to do so by law or court order; and even where required to do so by law or court order, make all reasonable efforts to coordinate with Collins prior to providing any Breach Notice. Where the Security Breach (a) involves data on the Supplier's networks or systems or (b) is the fault of the Supplier, then Supplier will, at the request of Collins, pay for the costs of remediation, notification (including, where reasonably necessary, a call center), and, if the Security Breach involves data elements that could lead to identity theft, provide the

应柯林斯的要求，支付补救、通知（包括在合理必要的情况下，呼叫中心）的费用，如果安全漏洞**涉及可能**导致身份盗用的数据元素，则向受影响的个人提供信用监测或其他商业上合理的身**份盗用**风险降低服务，为期一年或法律或政府监管机**构要求的更**长时间。

affected individuals with credit monitoring or other commercially-reasonable identity theft mitigation service for one year or such longer period as required by law or a government regulator.

5. 如果供应商应向柯林斯提供受数据隐私法保护的个人信息，供应商应确保这些个人信息的提供符合**适用法律的**规定，包括在需要时获得同意或提供通知。

5.In the event Supplier shall provide to Collins personal information protected by Data Privacy Laws, Supplier shall ensure that such personal information is provided consistent with applicable law, including, where required, obtaining consent or providing notice.

6. 供应商获得的所有柯林斯个人信息应被退回或销毁（由柯林斯选择），除非并在此范围内：(i)供应商需要此类柯林斯个人信息来履行其在本协议项下或**适用法律**项下的义务；或(ii)**适用法律禁止**归还或销毁。如果没有相反的指示，除非法律禁止，供应商在工作说明终止或完成后经等待30天柯林斯未要求归还柯林斯个人信息的，供应商应立即销毁所有柯林斯个人信息。

6.All Collins Personal Data acquired by Supplier shall be returned or destroyed (at the option of Collins), unless and to the extent that: (i) such Collins Personal Data is required by Supplier to discharge its obligations hereunder or under applicable law; or (ii) return or destruction is prohibited by applicable law. Absent contrary instructions and except as prohibited by law, Supplier shall immediately destroy all Collins Personal Data after termination or completion of the statement of work after waiting 30 days to allow Collins to request return of Collins Personal Data.

7. 数据转移。如果协议和/或订单**涉及供**应商将把居住在中国境内个人的柯林斯个人信息转移到中国境外的服务，那么柯林斯特此同意：(a)**确保其具有向**供应商提供柯林斯个人信息的合法权利；(b)通知或以其他方式获得数据主体对处理柯林斯个人信息的同意（在必要范围内）；以及(c)根据数据保护法的要求，获得数据主体的单独同意（在必要范围内）。

7.Data Transfers. If the Agreement and/or Order involves the provision of services where the Supplier will transfer Collins Personal Information of individuals that reside in the PRC to locations outside of the PRC, then Collins hereby agrees: (a) to ensure that it has the legal right to provide the Collins Personal Data to the Supplier; (b) to notify or otherwise obtain the consent (to the extent necessary) from the Data Subjects for the Processing of the Collins Personal Information; and (c) to obtain separate consents from the Data Subjects (to the extent necessary) as may be required under the Data Protection Laws.

签名见下页

有鉴于此，双方于文首所载的日期签署本《DPTA》。

[*插入柯林斯实体的名称*]，柯林斯宇航的一个组成部分
姓名（全名）：
标题：
签名：

SIGNATURES APPEAR IMMEDIATELY BELOW

IN WITNESS WHEROF, the Parties have caused this DPTA to be executed as of the date and year first written above.

[*insert name of Collins entity*], a part of Collins Aerospace
Name (written out in full):
Title:
Signature:

附件1：处理过程的描述

1.处理的目的

柯林斯正在向供应商采购服务。在接受服务的过程中，柯林斯将需要分享本文所述的个人信息。供应商将只为提供这些服务的目的处理个人信息。所提供服务的性质在协议和任何根据协议执行的工作说明或根据协议发出的订单中有所规定。

2.处理期

供应商应在协议期间及之后的合理时间按照其法律义务处理个人信息，以便核对任何剩余的合同后活动、付款核对、工作交接，。

3.处理方法

个人信息的处理方法应按照协议和/或根据协议执行的任何工作说明或根据协议发出的订单中的描述。

4.处理的柯林斯个人信息类型

Exhibit 1: Description of Processing

1. Purpose of the Processing

Collins is procuring services from the Supplier and, in the course of receiving the services, Collins will need to share personal data as set forth herein. The Supplier will only process personal data for the purpose of providing those services. The nature of the services being provided are set forth in the Agreement and any Statement of Work executed pursuant to, or Order issued under, the Agreement.

2. Processing Period

The Supplier shall process the personal data during the term of the Agreement and for a reasonable period of time thereafter in order to reconcile any remaining post-contractual activities, payment reconciliation, work transition, and in accordance with its legal obligations.

3. Method of Processing

The method of processing of the personal data shall be in as described in the Agreement and/or any Statement of Work executed pursuant to, or Order issued under, the Agreement.

所处理的个人信息涉及以下类别的数据主体。
为使供应商履行协议中规定的服务所需的任何个人信息，包括（但不限于）。

- 柯林斯的员工、承包商、客户、终端用户、求职者和投资者
- 柯林斯的商业伙伴的人员，如供应商、供货商和客户等
- 柯林斯因法律原因可能拥有其个人数据的第三方，如诉讼中的当事人

5.安全措施
至少，供应商应实施并遵循《DPTA》附件2中描述的技术和组织安全措施。

6.权利和义务
双方特此同意遵守《DPTA》中规定的权利和义务。

7.数据保留；删除
个人信息应仅保留在履行协议和/或根据协议执行的任何工作说明或根据协议发出的订单所需的时间内，以及此后的合理时间内，以便根据其法律义务核对任何剩余的合同后活动、付款核对、工作过渡。

8.分包商
向次级处理人的任何转让将符合标准合同条款、条款和条件中题为
"数据隐私
"的部分以及本附件1的条款。

附件2：确保数据安全的技术和组织措施

供应商承诺建立和维护物理、技术和组织安全措施，以维护和保护在本协议中创建、收集、接收或以其他方式获得的个人信息以及据此提供的处理

4. Type of Collins Personal Data Processed
The personal data processed concerns the following categories of data subjects:
Any personal data required to allow Supplier to perform the services as set forth in the Agreement, including (without limitation):

- Collins employees, contractors, customers, end users, job applicants, and investors
- Personnel of Collins's business partners, such as vendors, suppliers, and customers
- Third parties whose personal data Collins may have for legal reasons, such as parties in litigation

5. Security Measures
At a minimum, the Supplier shall implement and follow the technical and organisational security measures described in Exhibit 2 of the DPTA.

6. Rights and Obligations
The Parties hereby agree to abide by the rights and obligations set forth in the DPTA.

7. Data Retention; Deletion
Personal data shall be retained only so long as required to perform the services under the Agreement and/or any Statement of Work executed pursuant to, or Order issued under, the Agreement and for a reasonable period of time thereafter in order to reconcile any remaining post-contractual activities, payment reconciliation, work transition, and in accordance with its legal obligations.

8. Subcontractors
Any transfers to sub-processors will be consistent with the terms of the Standard Contractual Clauses, the Section of the Terms and Conditions entitled "Data Privacy", and this Exhibit 1.

Exhibit 2: Technical and Organizational Measures to Ensure the Security of the Data

The Supplier undertakes to institute and maintain physical, technical, and organizational security measures in order to maintain and to protect the security of personal data created, collected, received, or

业务的安全，这些措施是根据相关数据保护法处理个人信息所需的。

供应商的技术和组织安全措施应至少包括以下内容（可随时更新）。

内部控制和系统

供应商应遵守符合ISO 27001和ISO 20000准则的严格内部控制。供应商将以强制性政策和程序的形式对接触柯林斯个人数据的员工和所有分包商或代理人实施安全规则。这些政策和程序包括：

- 措施、标准、程序、规则和规范以达到**适当的安全水平。**

- 个人信息的含义和重要性，以及对其进行保护、保密和仅在需要了解的基础上访问的必要性。

- 工作人员的职能、义务和访问权。

- 报告、管理和应对个人信息安全事件的程序；以及

- 制作备份副本和恢复个人信息的程序。

安全问题

供应商对个人信息的访问是通过柯林斯规定的访问和程序进行的。

以下总结了主要的安全义务（在出现争议或不一致的情况下，应以商定的更全面的安全义务为准）。

otherwise obtained in connection with the Agreement, and the processing operations provided thereunder, which measures are required for the processing of personal data in accordance with the relevant Data Protection Laws.

The technical and organisational security measures of the Supplier shall include, as a minimum, the following (as may be updated from time to time).

Internal Controls and systems

The Supplier shall comply with strict internal controls in line with ISO 27001 and ISO 20000 guidelines. The Supplier will implement security rules in the form of mandatory policies and procedures for staff and all subcontractors or agents who have access to Collins group personal data. These policies and procedures cover:

- measures, standards, procedures, rules and norms to address the appropriate level of security;

- the meaning and importance of personal data and the need to keep it secure, confidential and accessed on a need to know basis only;

- staff functions, obligations and access rights;

- the procedures for reporting, managing and responding to personal data security incidents; and

- the procedures for making backup copies and recovering personal data.

Security

Access to personal data by the Supplier is provided through access and procedures governed by Collins.

The following summarizes key security obligations (and in the event of dispute or inconsistency, the fuller security obligations agreed shall prevail):

工作人员在数据文件方面的职能和义务：

必须以书面形式在安全文件中明确规定**每个能**够访问个人信息和信息系统的用户或用户档案的职能和义务。

事件的记录：

应有一个通知和管理影响个人信息的事件的程序，并建立一个登记册，以记录事件的类型，它发生的时间或在**适当的情况下**，**被**发现的时间，发出通知的人，它被传达的对象，它所产生的影**响和所采取的**纠正措施。

识别和核实：

供应商应采取措施保证用户的正确识别和核实。供应商应建立一种机制，允许对试图访问信息系统的任何用户进行明确和个性化的识别，并对其授权进行核实。安全文件应规定密码的更换频率，在任何情况下都不得少于**每年一次。在有效期内**，**密**码应以不可理解的方式储存。

备份副本和恢复：

安全文件应要求且供应商应确保(1)至少**每周**创建一次备份；(2)实施数据恢**复程序**，**在技**术上可行的情况下，能够将其重建到损失或破坏发生时的原始状态。

安保人员：

安全文件应指定一名或数名安全官员，负责执行和监测安全文件要求的遵守情况。这一任命可以是针对所有的档案系统或个人信息处理的一般任命

Functions and obligations of staff with regards to data files:

The functions and obligations of each of the users or profiles of users with access to the personal data and to the information systems must be clearly defined in writing in a security document.

Record of incidents:

There shall be a procedure for notification and management of incidents that affect personal data and a register established for recording the type of incident, the moment it occurred, or if appropriate, was detected, the person making the notification, to whom it was communicated, the effect arising from it and the corrective measures applied.

Identification and Authentication:

The Supplier shall take the measures that guarantee the correct identification and authentication of the users. The Supplier shall establish a mechanism that permits the unequivocal and personalized identification of any user who tries to access the information system and the verification of his authorization. The security document shall establish the frequency, which under no circumstances shall be less than yearly, with which the passwords shall be changed. While in force, passwords shall be stored in an unintelligible way.

Backup Copies and Recovery:

The security document shall require and the Supplier shall ensure that: (1) backups are created at least weekly; and (2) data recovery procedures are implemented that enable their reconstruction to the original state at the moment the loss or destruction occurred, to the extent technically feasible.

Security Officer:

The security document shall appoint one or several security officers responsible for implementing and monitoring compliance with the requirements of the security document. This appointment may be general for all the filing systems or processing of

，也可以是根据所使用的信息系统的具体任命，这些都应在安全文件中明确记录。

审计：

安全文件应要求且供应商应确保至少**每两年**进行一次内部或外部审计，以核实对安全文件中所载安全措施的遵守情况。

媒体和文件的管理：

安全文件应要求且供应商应确保建立一个登记或清点系统，用于录入含有个人信息的媒体，允许直接或间接识别文件或媒体的类型，以及日期和时间、发行者、传输中包含的文件或媒体的数量、它们所包含的信息类型、传输方法和负责接收的人。

识别和核实：

安全文件应要求且供应商应建立一种机制，以限制对个人信息的未经授权的访问，包括根据新的或新识别的风险更新安全文件。

物理访问控制：

安全文件应要求且供应商应确保只有经授权的人员才能进入存放支持信息系统的物理设备的场所。

事件的记录：

登记册应提供恢复数据的程序，说明执行该程序的人、恢复的数据，并酌情说明哪些数据在恢复过程中必须手工记录。

personal data or specific depending on the information systems used, which shall be clearly recorded in the security document.

Audit:

The security document shall require and the Supplier shall ensure that, at least every two years, an internal or external audit is conducted that verifies compliance with the security measures contained in the security document.

Management of media and documents:

The security document shall require and the Supplier shall ensure that a registration or inventory system for the entry of media containing personal data shall be established permitting, directly or indirectly, identification of the type of document or media, as well as the date and time, the issuer, the number of documents or media included in the transmission, the type of information they contain, the method of transmission and the person responsible for receipt.

Identification and authentication:

The security document shall require and the Supplier shall establish a mechanism to limit unauthorized access to the personal data, including updating the security document based on new or newly identified risks.

Physical access control:

The security document shall require and the Supplier shall ensure that only the personnel authorized have access to the places housing the physical equipment that supports the information systems.

Record of incidents:

The register shall provide the procedures for the recovery of data, indicating the person who executed the process, the data restored and, if appropriate, which data have had to be manually recorded in the recovery process.