CSA GCR cloud security alliance GREATER CHINA REGION ®

公认隐私原则 中文版

Generally Accepted Privacy Principles

2021.08

致谢

中文版翻译说明

由云安全联盟大中华区(CSA GCR)数据安全工作组负责组织翻译公认隐私原则(Generally Accepted Privacy Principles)。

翻译审校工作专家：

组长：高巍

组员：薛琨，张明敏，廖聪城，王贵宗

在此感谢以上参与该文档的翻译审校工作的专家及工作人员。如译文有不妥当之处，敬请读者联系 CSA 数据安全工作组给与雅正!

联系邮箱：info@c-csa.cn；
云安全联盟大中华区
2021 年 8 月 8 日
云安全联盟 CSA 公众号

前言

美国注册会计师协会(AICPA) 和加拿大特许会计师协会(CICA)坚信，隐私是一个商业问题。考虑到各组织在试图解决隐私事务时所面临的问题，我们很快得出结论，企业没有一个全面的框架来有效管理其隐私风险。这两个协会决定，他们可以通过开发一个隐私框架来做出重大贡献，该框架可以解决受隐私要求或期望影响的所有各方的需求。因此，这两个机构制定了一个名为 《AICPA 和 CICA 公认隐私原则》的隐私框架。这两个机构将这些原则和标准广泛提供给对解决隐私问题感兴趣的所有各方。

这些原则和标准是由志愿者开发和更新的，他们考虑了当前的国际隐私监管要求和最佳实践。这些原则和标准是按照两个研究所的适当程序发布的，其中包括公开征求公众意见。采用这些原则和标准是自愿的。

这些原则的一个基本前提是，良好的隐私即能保障良好的商业。良好的隐私实践是公司治理和问责制的一个关键组成部分。当今的关键商业要务之一是保护一个组织所收集和持有的个人信息的隐私。随着业务系统和流程变得越来越复杂精细化，越来越多的个人信息被收集。由于更多的数据被收集和持有，而且通常是以电子格式，个人信息可能面临各种脆弱性的风险，包括丢失、滥用、未经授权的访问和未经授权的披露。这些风险引起了组织、政府、个人和公众的关注。

对于在多个司法管辖区环境中运作的组织，管理隐私风险可能是一个更加重大的挑战。遵守普遍接受的隐私原则并不能保证符合一个组织所要遵守的所有法律和法规。组织需要了解其开展业务的所有管辖区的重要隐私要求。虽然本框架提供了关于隐私的一般指导，但各组织应咨询自己的法律顾问，以获得更多关于管辖本组织具体情况的特定法律和法规的建议和指导。

考虑到这些问题，AICPA 和 CICA 制定了《公认隐私原则》，作为一个操作框架，帮助管理层以考虑到许多地方、国家或国际要求的方式来处理隐私问题。主要目标是促进隐私合规和有效的隐私管理。次要目标是提供适当的标准，以便可以进行隐私验证工作(通常称为隐私审计)。

公认隐私原则代表了 AICPA 和 CICA 的贡献，即帮助组织保持对隐私风险的有效管理，确保组织的需求，并反映公共利益。有关发展的其他历史和其他隐私资源可在网上找到：www.aicpa.org/privacy 和 www.cica.ca/privacy。《公认隐私原则》可从 AICPA 和 CICA 的网站下载，分别为 www.aicpa.org/privacy 和 www.cica.ca/privacy。

由于隐私环境不断变化，《公认隐私原则》将需要不时地进行修订。因此，请将有关本文件的任何意见通过电子邮件发送给美国注册会计师协会(GAPP@aicpa.org)或加拿大特许会计师协会(mailto:privacy@cica.ca)。

AICPA CICA

美国注册会计师协会和加拿大特许会计师协会隐私工作组

主席

Everett C. Johnson, CPA

德勤会计师事务所 (退休)

副主席

Kenneth D. Askelson, CPA, CITP, CIA

彭尼公司(退休)

Eric Federing

毕马威会计师事务所

Philip M. Juravel, CPA

Juravel & Company, LLC

Sagi Leizerov, Ph.D., CIPP

安永会计师事务所

Rena Mears, CPA, CITP, CISSP, CISA, CIPP

德勤会计师事务所

Robert Parker, FCA, CA CISA, CMC

德勤会计师事务所 (退休)

Marilyn Prosch, Ph.D., CIPP

亚利桑那州立大学

Doron M. Rotman, CPA (Israel), CISA, CIA, CISM, CIPP

毕马威会计师事务所

Kerry Shackelford, CPA

KLS Consulting LLC

Donald E. Sheehy, CA CISA, CIPP/C

德勤会计师事务所

工作人员联系方式:

Nicholas F. Cheung, CA, CIPP/C

CICA

负责人，保障服务开发部

Bryan Walker, CA

CICA

总监，从业人员支持

Nancy A. Cohen, CPA, CITP, CIPP

AICPA

高级技术经理。

专业社区和实践管理

James C. Metzler, CPA, CITP

AICPA

副总裁，小型机构权益部

AICPA 保障服务部

执行委员会于 2009 年 8 月批准了《公认隐私原则》。

目录

隐私—公认隐私原则概述 8

介绍 8

为什么隐私是一个商业问题 9

国际隐私考虑因素 9

外包和隐私 10

什么是隐私？ 11

隐私定义 11

个人信息 11

隐私还是保密？ 12

公认隐私原则简介 13

整体隐私目标 13

公认隐私原则 13

应用 GAPP 15

公认隐私原则和标准的展示 17

公认隐私原则和标准 18

管理 18

声明 29

选择和同意 33

收集 37

使用，留存和处置 40

访问 43

向第三方披露 48

隐私安全 52

质量 60

监督与执行 62

附录 A-词汇表 68

隐私—公认隐私原则概述

介绍

许多组织发现了需要在地区、国家或国际基础上管理隐私[1]的挑战。大多数组织都面临着许多不同的隐私法律和法规，需要将其要求付诸实施。

公认隐私原则(GAPP)是从商业角度制定的，参考了一些(但绝不是所有)重要的地方、国家和国际隐私法规。GAPP 将复杂的隐私要求定义成一个单一的隐私目标，由十项隐私原则支持。每项原则都有客观、可衡量的标准支持，这些标准构成了有效管理组织内隐私风险和合规性的基础。为支持这些标准，GAPP 提供了说明性的政策要求、沟通、控制，也包括监测控制。

任何组织都可以使用 GAPP 作为其隐私管理体系的一部分。GAPP 的开发是为了帮助管理层创建一个有效的隐私管理体系，以应对隐私风险和义务，以及商业机会。它也可以作为管理者和其他监督管理角色的有用工具。本章内容包括隐私的定义和解释为什么隐私是一个商业问题，而不仅仅是一个合规问题。此外，还说明了这些原则如何适用于外包方案，以及为了组织及其客户的利益可以采取的潜在隐私举措类型。

本章内容和接下来的一套隐私原则与相关标准对从事以下工作的人员有帮助：

- 监督和监测隐私和安全计划。
- 在一个组织中实施和管理隐私。
- 在一个组织中实施和管理安全。
- 监督和管理组织中的风险和合规性。
- 评估合规性并审计隐私和安全计划。
- 隐私监管。

[1] 附录 A-词汇表中包含的每个词的第一次出现都有下划线，并超链接到其在导言部分的词汇表和公认隐私原则及相关标准表中的定义。

为什么隐私是一个商业问题

执行良好的隐私保护意味着具备良好的商业基础。良好的隐私保护实践是公司治理和问责制的一个关键部分。当今的关键商业要务之一是维护个人信息的隐私。随着业务系统和流程变得越来越复杂和精细化，企业正在收集越来越多的个人信息。因此个人信息容易受到各种风险的影响，包括丢失、滥用、未经授权的访问和未经授权的披露。这些风险已经引起了组织、政府和公众的关注。

各个组织正试图在适当的收集和使用用户个人信息之间取得平衡。政府正试图保护公共利益，同时管理他们从公民那里收集的个人信息的缓存。消费者对他们的个人信息非常关注，许多人认为他们已经失去了对信息的控制。此外，公众对身份盗用和不当获取个人信息，特别是财务和医疗记录，以及有关儿童的信息非常关注。

用户个人希望他们的隐私能得到尊重，他们的个人信息能得到与其有业务往来组织的保护。他们不希望一个组织未能保护他们的隐私。因此，所有企业都需要将隐私作为一个风险管理问题来有效解决。以下是不当的隐私政策和规程带来的具体风险：

- 对组织的声誉、品牌或业务关系造成损害
- 受到法律责任和行业或法规制裁
- 被指控为具有欺骗性的商业行为
- 客户或员工的不信任
- 个人拒绝同意将其个人信息用于商业目的
- 业务损失以及随之而来的收入和市场份额的减少
- 国际业务活动的中断
- 因个人身份被盗用而产生的法律责任

国际隐私考虑因素

对于在一个以上国家运营的组织来说，管理其隐私风险可能是一个重大挑战。

例如，互联网和商业的全球性质意味着一个国家的监管行动可能会影响世界各地的个人用户和客户的权利与义务。许多国家都有监管跨境数据流动的法律(包括欧盟 EU 关于数据保护和隐私的指令)，如果一个组织想在这些国家开展业务，就必须遵守这些指令，

因此组织需要遵守世界各地不断变化的隐私要求。此外不同的司法管辖区有不同的隐私理念，使国际合规成为一项复杂的任务。一些国家认为个人信息属于个人，并认为企业在收集和维护这些信息时具有类似信托的关系。另外，还有一些国家认为个人信息属于收集信息的企业。

此外，企业面临的挑战是努力跟上他们业务所在的每个国家的最新要求。通过遵守一个高的全球标准，如本文件中规定的标准，将有助于遵守许多法规。

即使是国际业务有限的组织也经常面临遵守其他国家的隐私要求的问题。这些组织中的许多人不确定如何处理通常更严格的海外法规。这增加了组织因为无意中的违规行为而被所在国当作负面案例公布的一个风险。

此外，许多司法管辖地区(如州或省)和某些行业，如医疗或银行，都有与隐私有关的具体要求。

外包和隐私

外包增加了处理隐私问题的复杂性。一个组织可以将其业务流程的一部分外包出去，并随之将一些隐私责任外包出去；但是，该组织不能将其业务流程中的隐私的最终责任外包出去。当执行外包服务的组织在不同的国家，并可能受制于不同的隐私法律或可能根本没有隐私要求时，复杂性会增加。在这种情况下，将业务流程外包的组织需要确保其妥善管理隐私责任。

GAPP 及其支持标准可协助组织完成对提供外包服务的第三方的隐私政策、程序和措施的评估(包括独立审查)。

这些原则和标准在全球范围内适用，这可以让外包商感到放心，因为隐私评估可以使用基于国际上已知的公平信息惯例的一致衡量标准来进行。

什么是隐私?

隐私定义

在《公认隐私原则》中，隐私被定义为 "个人和组织在收集、使用、留存、披露和处理个人信息方面的权利和义务"。

个人信息

个人信息(有时被称为个人可识别信息)是关于(或与之相关的) 可识别个人的信息。它包括任何可与个人相联系或用于直接或间接识别个人的信息。就这一目的而言，个人包括潜在的、当前的和以前的用户、雇员，以及与该组织有关系的其他人。一个组织收集的关于个人的大多数信息，如果可定位到一个已识别的个人，就可能被认为是个人信息。个人信息的一些例子如下：

- 姓名
- 家庭或电子邮件地址
- 身份证号码(又如，社保账号)。
- 身体特征
- 消费者的购买历史

有些个人信息被认为是敏感信息。一些法律和法规将以下内容定义为敏感个人信息：

- 关于医疗或健康状况的信息
- 财务信息
- 种族或民族血统
- 政治观点
- 宗教或哲学信仰
- 工会会员资格
- 性取向
- 与犯罪行为或刑事定罪有关的信息

敏感的个人信息通常需要额外的保护和更高的关注职责。例如，一些司法管辖区可能要求对敏感信息的收集和使用给予明确的同意，而不是默认同意。

一些关于人的信息或与人有关的信息无法与具体个人联系起来。此类信息被称为非个人信息。这包括统计或汇总的个人信息，这些信息的个人身份是未知的，或者与个人的关联已被删除。在这种情况下，个人的身份无法从剩下的信息中确定，因为这些信息已被去标识化或匿名化。非个人信息通常不受隐私保护影响，因为它不能与个人相联系。然而，由于其他法规和协议(例如，临床研究和市场研究)，一些组织可能对非个人信息仍有义务。

隐私还是保密?

与通常由法律或法规定义的个人信息不同，保密信息不存在被广泛认可的单一定义。在沟通和交易过程中，合作伙伴经常交换信息或数据，其中一方或另一方要求在 "需知 "的基础上进行维护。可能受到保密性要求的信息种类的例子包括以下内容：

- 交易细节
- 工程图纸
- 业务计划
- 有关企业的银行信息
- 存货供应
- 买入或卖出价格
- 价格表
- 法律文件
- 按客户和行业划分的收入

此外，与个人信息不同的是，为确保机密信息的准确性和完整性，对其进行访问的权利并没有明确的规定。因此，对什么是机密信息的解释在不同的组织之间会有很大的不同，在大多数情况下，是由合同约定所决定的。关于保密性标准的更多信息，请参考 AICPA 和 CICA 信任服务原则、标准和安全、可用性、处理完整性、保密性和隐私的说明(见 www.aicpa.org/TrustServices 或 www.webtrust.org)。

公认隐私原则简介

GAPP 旨在协助管理层创建一个有效的隐私管理体系，应对他们的隐私义务、风险和商业机会。

隐私原则和标准是建立在重要的区域、国家和国际隐私法律、法规、指南[2]和良好商业惯例的关键概念之上。通过使用 GAPP，各组织可以从商业角度出发，积极主动地应对他们在建立和管理其隐私计划和风险方面所面临的重大挑战。GAPP 还有助于在多司法管辖区的基础上管理隐私风险。

整体隐私目标

隐私原则和标准是建立在以下的隐私目标之上：

个人信息的收集、使用、留存、披露和处理都符合组织的隐私声明中的承诺以及美国注册会计师协会和加拿大注册会计师协会发布的《公认隐私原则》中规定的标准。

公认隐私原则

隐私原则对正确保护和管理个人信息至关重要。它们的基础是国际知名的公平信息实践，包括在世界各地不同司法管辖区的许多隐私法律和法规以及公认的良好隐私实践。

以下是 10 条普遍接受的隐私原则：

1. 管理。组织对其隐私政策和规程进行定义、记录、沟通和分配责任。

[2] 例如，经合组织（Organisation for Economic Co-operation and Development）已经发布了《关于保护隐私和跨境流动的准则》。欧盟发布了《数据隐私指令》（Directive 95/46/EC）。此外，美国还颁布了《格雷姆-里奇-比利雷法案》、《健康保险可携性和责任法案》以及《儿童在线隐私保护法案》。加拿大颁布了《个人信息保护和电子文件法》，澳大利亚颁布了 1988 年的《澳大利亚隐私法》，并在 2001 年进行了修订。将这些国际隐私概念与普遍接受的隐私原则进行比较的图表可以在网上找到：www.aicpa.org/privacy。遵守这套普遍接受的隐私原则和标准不一定就能遵守适用的隐私法律和法规，组织应就遵守任何法律和法规寻求适当的法律咨询。

2. 声明。该组织提供有关其隐私政策和规程的声明，并确定收集、使用、留存和披露个人信息的目的。

3. 选择和同意。该组织说明个人可做出的选择，并在收集、使用和披露个人信息方面获得默许或明确的同意。

4. 收集。该组织只针对通知中明确的目的收集个人信息。

5. 使用、留存和处置。该组织将个人信息的使用限制在通知中明确的目的，以及个人已提供默许或明确同意的目的。该组织仅在为实现所述目的或法律法规要求的必要时间内留存个人信息，并在此之后适当地处理这些信息。

6. 访问。该组织向个人提供访问其个人信息的方式，以便审查和更新。

7. 向第三方披露。该组织仅出于通知中明确的目的，并在个人的默许或明示同意下，向第三方披露个人信息。

8. 隐私安全。该组织保护个人信息免受未经授权的访问(包括物理和逻辑访问)。

9. 质量。该组织为通知中确认的目的，确保相关个人信息的准备、完整性。

10. 监督和执行。该组织监测其隐私政策和规程的遵守情况，并有规程来处理与隐私有关的投诉和纠纷。

对于 10 条隐私原则中的每一条，都规定了相关的、客观的、完整的和可衡量的标准，以指导组织的隐私政策、沟通、规程和控制措施的发展和评估。隐私政策是传达管理层的意图、目标、要求、责任和标准的书面声明。沟通是指组织向个人、内部人员和第三方传达其隐私声明和其中的承诺以及其他相关信息。规程和控制措施是组织为实现标准所采取的其他行动。

应用 GAPP

GAPP 可被各组织用于以下方面：

- 设计、实施和沟通隐私政策
- 建立和管理隐私管理体系
- 监测和审计隐私管理体系
- 衡量绩效和基准

建立和管理隐私计划涉及以下活动：

- 制定战略。执行隐私战略和业务规划。
- 诊断。执行隐私差距和风险分析。
- 实施。制定、记录、引入和 使该计划的行动计划制度化，包括建立对个人信息的控制。
- 维持和管理。监测隐私计划的活动。
- 审计。内部或外部审计人员评估组织的隐私计划。

下表总结并说明了一个组织如何使用 GAPP 来处理这些业务活动。

活动	一般性讨论	公认隐私原则的潜在用途
制定战略	**愿景。**一个组织的战略涉及到它的长期方向和繁荣。愿景确定了组织的文化，并有助于塑造和确定组织如何与外部环境互动，包括客户、竞争对手以及法律、社会和道德问题。 **战略规划。**这是一个组织的总体规划，包含了其战略方向。其目的是确保该组织的工作都朝着一个共同的方向发展。战略计划确定了组织的长期目标和实现隐私合规的主要问题。	**愿景。**在一个组织的隐私工作中，建立愿景有助于该组织整合风险偏好和优先考虑目标。 **战略规划。**在一个组织的隐私工作中，公认隐私原则(GAPP)可用于协助 组织确定需要处理的重要组成部分。

活动	一般性讨论	公认隐私原则的潜在用途
	资源分配。这一步骤确定了为实现战略计划或商业计划中规定的目标和目的而分配的人力、财政和其他资源。	**资源分配。**利用 GAPP，该组织将确定从事和负责的领域，可能包括系统管理、隐私和安全问题，并规定其活动的资源配置。 **总体战略。**战略文件描述了预期或打算的未来发展。GAPP 可以帮助一个组织澄清所考虑的系统或企业的隐私目标的计划。该计划确定了实现目标和里程碑的过程。它还提供了一个机制来沟通关键实施要素，包括服务、预算、开发成本、推广和隐私广告的细节。
诊断	这个阶段通常被称为评估阶段，包括对组织环境的彻底分析，确定存在弱点、漏洞和威胁的可能。对一个组织来说，最常见的初始项目是诊断性评估。这种评估的目的是根据其隐私目标和目的对组织进行评估，并确定该组织在何种程度上实现了这些目标和目的。	GAPP 可以协助组织了解其高层次的风险、机会、需求、隐私政策和实践、竞争压力以及组织所遵守的相关法律和法规的要求。 GAPP 提供了一个立法中立的基准，使该组织能够根据期望的状态评估当前的隐私状况。
实施	一个行动计划被推动，或一个诊断建议被付诸实施，或两者都是。实施包括制定和记录隐私计划和行动计划，以及执行所有计划的和其他必要的任务，以使行动计划得以实施。它包括定义谁将执行什么任务，分配责任，并建立时间表和里程碑。这涉及到计划和 一系列计划项目的规划和实施，以便为组织在制定其倡议时提供指导、方向、方法和工具。	GAPP 可以协助该组织实现其实施目标。在实施阶段结束时，该组织应制定以下可交付成果： • 解决隐私要求的系统、程序和流程 • 更新的符合隐私要求的表格、手册和合同 • 内部和外部的隐私意识计划
维持和管理	维持和管理包括监测工作，及时发现进展与行动计划的差异，以启动纠正措施。 监测是指相关的管理政策、流程和支持技术，以确保遵守组织的隐私政策和规程，并	该组织可以使用 GAPP 来制定适当的报告标准，以监测对信息的请求、用于汇总信息的来源和实际披露的信息。它还可用于确定验证程序，以确保信息披露对象有权

活动	一般性讨论	公认隐私原则的潜在用途
	能够表现出应有的谨慎。	获得该信息。
内部隐私审计	内部审计师提供客观的保证和咨询服务，旨在增加价值和改善一个组织的运作。他们帮助一个组织实现其目标，采用系统的、规范的方法来评估和改善风险管理，以及控制和治理过程的有效性。	内部审计师可以使用 GAPP 作为基准来评估一个组织的隐私计划和控制措施，并向管理层提供有用的信息和报告。
外部隐私审计	外部审计师，特别是注册会计师(CPA)和特许会计师(CA)，可以进行鉴证和保证服务。一般来说，这些服务，无论是对财务和非财务信息的执行，都能为个人、管理层、客户、业务伙伴和其他用户建立信任和提供信心。	外部审计师可以根据 GAPP 评估一个组织的隐私计划和控制措施，并提供对个人、管理层、客户、业务伙伴和其他用户有用的报告。

公认隐私原则和标准的展示

在每个原则下，标准以三栏的形式呈现。第一栏包含衡量标准。第二栏包含说明性的控制措施和操作规程，旨在提供例子并加强对如何应用这些标准的理解。这些说明并不全面，也不要求一个组织达到标准的任何说明。第三栏包含额外的考虑因素，包括补充信息，如良好的隐私惯例、可能与某一行业或国家有关的特定法律、和法规的指定要求。

一些标准可能不适合直接用于某些组织或流程。当某项标准被认为不适用时，该组织应考虑说明该决定的理由，以支持今后的评估。

这些原则和标准为设计、实施、维护、评估和审计隐私项目以满足一个组织的需要提供了基础。

公认隐私原则和标准

管理

参考	管理标准	控制措施和规程的说明	其他考虑因素
1.0	**该组织对其隐私政策和程序进行定义、记录、沟通并分配责任。**		
1.1	**政策与沟通**		
1.1.0	**隐私政策** 该组织定义并记录其在以下方面的隐私政策： *a.* 通知 (见 2.1.0) *b.* 选择和同意 (见 3.1.0) *c.* 收集 (见 4.1.0) *d.* 使用、留存和处置 (见 5.1.0) *e.* 访问 (见 6.1.0) *f.* 披露给第三方 (见 7.1.0) *g.* 保护隐私的安全 (见 8.1.0) *h.* 质量 (见 9.1.0) *i.* 监视和执行 (见 10.1.0)	隐私政策以书面形式记录下来，并对有需要的内部人员和第三方随时可用。	

参考	管理标准	控制措施和规程的说明	其他考虑因素
1.1.1	**与内部人员的沟通** 至少每年一次向负责收集、使用、留存和披露个人信息的组织内部人员传达隐私政策和违反这些政策的后果。隐私政策的变化在批准后不久就会传达给这些人员。	该组织 • 定期向内部人员(例如在网络或网站上)传达有关该组织隐私政策的相关信息。尽快传达批准的隐私政策变更内容。 • 要求内部人员(初期和阶段性)确认他们对该组织隐私政策的理解且他们同意遵守这些政策。	本文所指的隐私政策包括与保护个人信息有关的安全政策。
1.1.2	**用于政策的职责与责任** 将职责与责任分配给一个人或团队，以制定、记录、实施、执行、监测和更新组织的隐私政策。将这些人或团队的名字和他们的职责告知内部员工。	该组织将隐私政策的职责分配给一个指定的人，如公司隐私官员(被指定负责隐私政策的人可能与被指定负责其他政策的人不同，例如安全)。 指定人员或团队的职责、权力和责任都有明确的记录。职责包括以下内容： • 与管理层一起建立用于对个人信息的敏感性进行分类并确定所需保护级别的标准 • 制定和维护组织的隐私政策 • 监测和更新组织的隐私政策 • 授权执行该组织的隐私政策 • 监测遵守的程度，并发起行动以改善对政策和实践的培训或澄清	被确定为对隐私最终负责的个人应来自组织内部。

参考	管理标准	控制措施和规程的说明	其他考虑因素
		董事会的一个委员会将隐私问题定期纳入公司整体治理的定期审查中。	
1.2	**规程和控制措施**		
1.2.1	**审查和批准** 隐私政策和规程，以及对其的修改，被管理层审查和批准。	隐私政策和规程被： • 高级管理层或管理委员会审查和批准。 • 至少每年审查一次，并根据需要进行更新。	
1.2.2	**隐私政策和规程与法律法规的一致性** 至少每年一次和当适用的法律和法规变化时对政策和规程进行审查，将其与适用的法律和法规要求进行比较。对隐私政策和规程进行修订，以符合适用的法律和法规的要求。	公司法律顾问或法务部门： • 确定哪些隐私法律和法规适用于该组织运营所在的司法管辖区。 • 确定适用于该组织的其他标准。 • 审查该组织的隐私政策和规程，以确保它们符合适用的法律、法规和相应的标准。	除了法律和监管要求外，一些组织可能会选择遵守某些标准，如国际标准化组织(ISO)公布的标准；也有可能被要求遵守某些标准，如支付卡行业公布的标准，作为开展业务的条件。各组织可将此类标准作为这一过程的一部分。
1.2.3	**个人信息的识别和分类** 个人信息和敏感个人信息的类型以及处理这些信息所涉及的相关规程、系统和第三方都已识别。且此类信息包含在该组织的隐私和相关安全政策和规程中。	该组织有一个信息分类政策和流程，其中包括以下内容： • 分类流程，该流程识别并将信息分为以下一个或多个类别： › 商业机密	

参考	管理标准	控制措施和规程的说明	其他考虑因素
		› 个人信息(敏感信息和其他个人信息) › 一般性商业信息 › 公开信息 • 识别处理个人信息的流程、系统和第三方 • 适用于每一类信息的具体安全和隐私政策和规程	
1.2.4	**风险评估** 风险评估过程被用来建立一个风险基线，并至少每年确定新的或变化的个人信息风险，并制定和更新对这些风险的应对。	实施流程来定期识别组织的个人信息风险。这种风险可能是外部的(如供应商丢失信息或未能遵守监管要求)，或内部的(如通过电子邮件发送未受保护的敏感信息)。当发现新的或变化的风险时，要更新隐私风险评估和应对策略。 该过程考虑了一些因素，如隐私事件管理的经验、投诉和争端解决过程以及监测活动。	理想情况下，隐私风险评估应与安全风险评估相结合，并成为该组织的整体企业风险管理计划的一部分。董事会或董事会的一个委员会应提供对隐私风险评估的监督和审查。
1.2.5	**承诺与隐私政策和规程的一致性** 内部人员或顾问审查合同是否与隐私政策和规程一致，并处理任何不一致的地方。	管理层和法务部门都会审查所有合同和服务级别协议，以确保与组织的隐私政策和规程保持一致。	
1.2.6	**基础设施和系统管理** 在实施涉及个人信息的新流程时，以及在对	以下是用于处理隐私影响的方法： • 管理层评估新的和重大改变的产品、服	一些司法管辖区禁止将个人信息用于测试和开发目的，除非它已被匿名化或以其他方式

参考	管理标准	控制措施和规程的说明	其他考虑因素
	此类流程(包括外包给第三方或劳务派遣人员的任何此类活动)进行更改时，对潜在的隐私影响进行评估，并根据隐私政策继续保护个人信息。为此，涉及个人信息的流程包括以下方面的设计、获取、开发、实施、配置、修改和管理。 • 基础设施 • 系统 • 应用系统 • 网站 • 程序 • 产品和服务 • 数据库和信息库 • 移动计算和其他类似的电子设备 • 设备 禁止在流程和系统测试开发中使用个人信息，除非这些信息被匿名化或按照组织的隐私政策和规程受到保护。	务、业务流程和基础设施对隐私的影响。 • 该组织对所有用于收集、使用、留存、披露和销毁个人信息的信息系统和相关技术(包括手动程序、应用程序、技术基础设施、组织结构以及用户和系统人员的责任)使用记录在案的系统开发和变更管理流程。 • 该组织评估计划的新系统和变更对隐私的潜在影响。 • 对系统组件的变化进行测试，以最小化对个人信息保护任何不利影响的风险。所有测试数据都是匿名的。一个受控的测试数据库被维护以进行全面的回归测试，以确保对一个程序的变更不会对其他处理个人信息的程序产生不利影响。 • 有程序确保在从旧系统迁移到新系统或变更系统的过程中保持对个人信息的完整性维护和保护。 • 在实施对处理个人信息的系统和程序的变更之前，包括那些可能影响安全的变更，都需要有文档化记录和隐私官、安全官、业务部门主管和 IT 管理层的批	保护达到政策要求的生产信息保护的相同水平。

参考	管理标准	控制措施和规程的说明	其他考虑因素
		准。但是，为保持对个人信息的相同保护水平，需要进行的紧急变更；可以在事后进行记录和批准。 信息技术部门保持一份所有处理个人信息的软件以及各自的级别、版本和已经应用的补丁的清单。 有程序规定，只有经过授权、测试和记录的变更才能在系统上应用。 在涉及计算机系统的地方，遵循适当的程序，如使用单独的开发、测试和生产库，以确保对个人信息的访问受到适当的限制。 负责启动或实施新系统和变更的人员，以及新的或修订的程序和应用程序的用户，都得到与隐私有关的培训和认识课程。与隐私有关的具体角色和责任得到分配。	
1.2.7	**隐私事件和违规管理** 已经实施了一个成文的隐私事件和违规管理计划，包括但不限于以下内容： • 识别、管理和解决隐私事件和违规行为的规程 • 明确的职责	已经实施了一项正式的、全面的隐私事件和违规管理计划，其中规定了以下内容： • 事件和违规行为会报告给违规小组的成员，该成员会评估事件是否与隐私或安全有关，或两者都有，对事件的严重程度进行分类，启动必要的行动，并确定隐私和安全负责人的参与。	一些组织可能会采用违规通知政策，以便在其运营的所有司法管辖区统一使用。根据需要，这样的政策至少要基于任何此类管辖区的最全面的法律要求。

参考	管理标准	控制措施和规程的说明	其他考虑因素
	• 识别事件严重性并确定所需行动和升级程序的流程 • 遵守违规法律和法规的流程，包括需要时，利益相关者违规通知 • 对事件或违规行为负责的员工或第三方的问责流程，并酌情进行补救、惩罚或惩戒 • 基于下列情况，对具体事件的定期审查(至少每年一次)流程，以确定必要的计划更新： › 事件模式和根本原因 › 内部控制环境或外部要求(法规或立法)的变化 • 流程的定期测试或演练(至少每年一次)，并根据需要对相关计划执行补救措施	• 首席隐私官(CPO)对该项目负有全面责任，并得到隐私和安全指导委员会的支持和违规团队的协助。不涉及个人信息的事件和违规行为是首席安全官的职责。 • 该组织有一个隐私违规通知政策，并得到以下支持： (a) 识别受违规事件影响数据主体的通知以及相关司法管辖区其他要求的流程 (b) 如果有法律法规或政策要求，评估利益相关者违规通知必要性的流程，以及 (c) 及时提供通知的流程。该组织与第三方签订协议，以管理通知流程，必要的话为个人提供信用监测服务。 • 该计划包括明确的升级路径，根据事件的类型或严重程度，或两者兼而有之，升级至执行管理层、法律顾问和董事会。 • 该项目规定了必要时与执法部门、监管	

参考	管理标准	控制措施和规程的说明	其他考虑因素
		部门或其他机构联系的流程。 • 每年，或在该计划发生重大变化时，以及在任何重大事件发生后，都会对新员工和团队成员进行该计划的培训，并对普通员工进行意识培训。 隐私事件和违规事件管理计划还规定了以下内容： • 在任何重大隐私事件发生后，由内部审计或外部顾问进行正式的事件评估。 • 每季度对实际事件进行一次审查，并根据以下情况确定所需的项目更新。 › 事件的根本原因 › 事件模式 › 内部控制环境和立法的变化 • 季度审查的结果报告给隐私指导委员会，每年报告给审计委员会。 • 每季度定义、跟踪并向高级管理层报告关键指标。 • 该计划至少每六个月测试一次，并在实施重大系统或规程变更后尽快进行测	

参考	管理标准	控制措施和规程的说明	其他考虑因素
		试。	
1.2.8	**支持资源** 资源由组织提供，以实施和支持其隐私政策。	管理层每年审查其隐私管理计划的人员分配、预算和其他资源的分配情况。	
1.2.9	**内部人员的资质** 该组织规定了负责保护个人信息隐私和安全的人员资格，并且只将这种责任分配给那些符合这些资格要求并接受过必要培训的人员。	负责保护个人信息隐私和安全的内部人员的资格由以下规程来保证： • 正式的岗位描述(包括职责、教育和专业要求，以及关键隐私管理职位的组织汇报关系)。 • 招聘流程(包括全面筛选证书、背景调查和推荐人调查)和正式的雇用和保密协议 • 绩效评估(由主管执行，包括对专业培养活动的评估)	
1.2.10	**隐私意识和培训** 提供关于组织的隐私政策和相关事项的隐私意识项目，以及根据其角色和责任针对选定的人员的具体培训。	所有员工每年都必须参加互动式在线隐私和安全意识课程。新员工、劳务派遣人员和其他人员必须在上岗后的第一个月内完成该课程，以留存其访问权限。 组织提供深入的培训，包括隐私和相关的安全政策与规程、法律与监管考虑、事件响应及其他相关主题。这种培训是：	

参考	管理标准	控制措施和规程的说明	其他考虑因素
		• 对所有能接触到个人信息或负责保护个人信息的员工，每年都必须进行。 • 针对员工的工作职责进行了裁剪。 • 通过外部培训和会议加以补充。 对组织的隐私培训和意识课程的出席情况进行监视。 对培训和意识课程进行审查和更新，以反映当前的立法、监管、行业以及组织政策和规程要求。	
1.2.11	**监管和业务要求的变化** 对于组织业务运营所在的每个司法管辖区，确定并处理以下因素的变化对隐私要求的影响： • 法律和监管 • 合同，包括服务级别协议 • 行业要求 • 业务运营和流程 • 人员、角色和职责 • 技术	该组织有一个持续的流程，以监测、评估和处理以下变化对隐私要求的影响： • 法律和监管环境 • 行业要求(如直销协会的要求) • 合同，包括与第三方的服务等级协议(改变合同中的隐私和安全相关条款的变化，在执行前由隐私官或法律顾问审查和批准 • 业务运营和流程 • 被指派负责隐私和安全事务的人员 • 技术(在实施之前)	理想情况下，这些规程将与风险评估过程相协同。 该组织还应该考虑新出现的良好实践，如在没有明确要求的司法管辖区内执行违规通知。

参考	管理标准	控制措施和规程的说明	其他考虑因素
	更新隐私政策和规程以响应变化的要求。		

声明

参考	声明标准	控制措施和规程的说明	其他考虑因素
2.0	**该组织提供有关其隐私政策和规程的声明，并确定收集、使用、留存和披露个人信息的目的。**		
2.1	**政策与沟通**		
2.1.0	**隐私政策** 该组织的隐私政策涉及向个人提供声明。		
2.1.1	**与个人沟通** 就以下隐私政策向个人提供声明。 *a.* 收集个人信息的目的 *b.* 选择和同意（见 3.1.1） *c.* 收集(见 4.1.1) *d.* 使用、留存和处置（见 5.1.1） *e.* 访问(见 6.1.1) *f.* 披露给第三方(见 7.1.1) *g.* 保护隐私的安全 (见 8.1.1) *h.* 质量(见 9.1.1) *i.* 监督和执行(见 10.1.1) 如果个人信息是从个人以外的来源收集的，这些来源要在声明中说明。	该组织的隐私声明 • 描述所收集的个人信息，这些信息的来源，以及收集信息的目的。 • 说明收集敏感个人信息的目的，以及这种目的是否是法律要求的一部分。 • 说明不提供所需信息的后果(如果有的话)。 • 说明可能会分析出关于个人的某些信息，如购买模式。 • 可以通过各种方式提供(例如：面谈，打电话，填写申请表或问卷，或电子方式)然而，书面声明是首选方法。	声明还可能描述将披露个人信息的情况，如以下情况： • 为公共安全或国防目的进行的某些处理活动 • 为公共卫生或人身安全的目进行某些处理活动 • 法律允许或要求时 声明中所描述的目的应以个人能够合理地理解该目的以及该个人信息如何被使用的方式来说明。这种目的应与该组织的商业目的相一致，不应过于宽泛。 应考虑提供一个摘要级别的声明，并与政策中更详细的部分相链接。

参考	声明标准	控制措施和规程的说明	其他考虑因素
2.2	**规程和控制措施**		
2.2.1	**提供声明** 向个人提供关于该组织的隐私政策和规程的声明： (a) 在收集个人信息时或之前，或收集后尽快提供， (b) 在该组织改变其隐私政策和规程时或之前，或此后尽快，或 (c) 在个人信息被用于先前未确定的新目的之前。	隐私声明 • 在首次向个人收集个人信息时，可随时查阅并提供。 • 及时提供(即在收集个人信息之时或之前，或之后尽快提供)，使个人能够决定是否向该组织提交个人信息。 • 明确的日期，使个人能够确定自他们上次阅读该通知或自他们上次向该组织提交个人信息以来，该声明是否有变化。 此外，该组织： • 记录该组织的隐私政策和规程的历史版本。 • 告知个人对此前传达的隐私通知的更改，例如通过在组织的网站上发布通知，通过信件发送书面通知，或发送电子邮件。 • 记录隐私政策和规程的变化，并将其传达给个人。	见 3.2.2，"对新目的和用途的同意"。 一些法规要求表明，应定期提供隐私声明，例如，在《格雷姆-里奇-比利雷法案》(GLBA)中要求每年提供一次。
2.2.2	**涵盖的组织和活动**	该隐私声明描述了所涵盖的具体组织、业务	

参考	声明标准	控制措施和规程的说明	其他考虑因素
	在组织的隐私声明中，对隐私政策和规程所涵盖的组织和活动进行了客观描述。	部门、地点和信息类型，例如： • 业务运营所在的司法管辖区(法律和政治) • 业务部门和关联公司 • 业务范围 • 第三方的类型(例如，送货公司和其他类型的服务提供商)。 • 信息的类型(例如，关于客户和潜在客户的信息) • 信息的来源(例如邮购或网上)。 当个人可能认为他们受该组织的隐私政策保护，但事实上不受保护时，组织应告知他们(例如，链接到与该组织类似的另一个网站，或在该组织的场所使用由第三方提供的服务)。	
2.2.3	**清晰和醒目** 该组织的隐私声明是醒目的，并使用清晰的语言。	隐私声明 • 使用简单明了的语言。 • 有适当的标签，容易看到，而且不是用异常小的字体。 • 在数据收集点链接到或显示在网站上。	如果一个组织的不同子公司或部门使用多个声明，鼓励使用类似的格式，以避免消费者混淆，并使消费者能够识别任何差异。 一些法规可能包含声明必须包含的具体信息。 对于某些行业和特定的收集、使用、留存和

参考	声明标准	控制措施和规程的说明	其他考虑因素
		• 网站使用国家官方语言或法律要求的语言。	披露的类型，通常有说明性的声明。

选择和同意

参考	选择和同意标准	控制措施和规程的说明	其他考虑因素
3.0	**该组织描述了个人可作出的选择，并在收集、使用和披露个人信息方面获得了隐含或明确的同意。**		
3.1	**政策与沟通**		
3.1.0	**隐私政策** 该组织的隐私政策涉及到个人可选择的内容和组织要获得的同意。		
3.1.1	**与个人沟通** 个人被告知： (a) 在收集、使用和披露个人信息方面，他们可以做出选择，以及 (b) 收集、使用和披露个人信息所需要的隐含或明确的同意，除非法律或法规特别要求或允许。	该组织的隐私声明以清晰和简洁的方式描述了以下内容： • 个人在收集、使用和披露个人信息方面可以做出的选择 • 个人在行使这些选择时应遵循的流程(例如，选择退出框以拒绝接收营销材料) • 个人改变联系偏好的能力和流程 • 未能提供交易或服务所需的个人信息的后果是什么？ 个人被告知以下事项： • 不需要提供与隐私声明中确定的目的不相关的个人信息。	一些法律和法规(如 1988 年澳大利亚《隐私法》第 1 条第 11 项原则"对个人信息披露的限制")规定了组织无需获得个人同意的具体豁免情况。这种情况的例子包括如下： • 记录保存者根据合理的理由认为，为其他目的使用信息是必要的，以防止或减少对有关个人或其他人的生命或健康的严重和紧迫的威胁。 • 为其他目的使用信息是法律要求或授权的。

参考	选择和同意标准	控制措施和规程的说明	其他考虑因素
		• 在法律或合同限制和合理通知的情况下，可以改变偏好，并在以后的时间里撤回同意。 所需的同意类型取决于个人信息的性质和收集方法(例如，订阅通讯的个人默认同意接受该组织的通知)。	
3.1.2	**拒绝或撤消同意的后果** 在收集个人信息时，个人会被告知拒绝提供个人信息或拒绝同意或撤回同意为声明中确定的目的使用个人信息的后果。	在收集的时候，该组织告知个人以下内容。 • 关于拒绝提供个人信息的后果(例如，交易可能不被处理) • 关于拒绝同意或撤回同意的后果(例如，选择不接收产品和服务信息可能会导致不知道有促销活动) • 关于未能提供超过最低要求的个人信息将如何影响或不影响他们(例如，仍将提供服务或产品)。	
3.2	**规程和控制措施**		
3.2.1	**默认或明确同意** 在收集个人信息之时或之前，或之后尽快，都会获得个人的默认或明示同意。个人在其同意中所表达的偏好将得到确认和执行。	该组织 • 及时获得并记录个人的同意(即在收集个人信息之时或之前或之后尽快)。 • 确认个人的偏好(以书面或电子方式)。	

参考	选择和同意标准	控制措施和规程的说明	其他考虑因素
		• 记录并管理对个人偏好的更改。 • 确保个人的偏好得到及时的执行。 • 通过为用户提供一个告知和质疑供应商对其联系偏好解释的流程，解决有关个人偏好记录中的冲突。 • 确保整个组织和第三方对个人信息的使用符合个人的偏好。	
3.2.2	**对新的目的和用途的同意** 如果以前收集的信息将被用于隐私声明中未指明的目的，则应记录新的目的，通知个人，并在这种新的使用或用于新的目的之前获得隐含或明确的同意。	当个人信息将被用于一个先前未指定的目的时，该组织应： • 通知个人并记录新的目的。 • 获得并记录将个人信息用于新目的的同意或撤销同意。 • 确保个人信息的使用符合新的目的，或者，如果同意被撤销，则不使用。	
3.2.3	**敏感信息的明确同意** 在收集、使用或披露敏感个人信息时，应直接获得个人的明确同意，除非法律或法规另有明确要求。	只有在个人提供明确同意的情况下，该组织才会收集敏感信息。明确同意要求个人通过某种行动肯定地同意使用或披露敏感信息。明确同意是直接从个人那里获得的，并且有记录，例如，要求个人勾选一个方框或签署一份表格。这有时被称为选择加入。	加拿大的《个人信息保护和电子文档法》(PIPEDA)附表 1 第 4.3.6 条规定，当信息可能被认为是敏感信息时，一个组织一般应寻求明确的同意。 许多司法管辖区禁止收集敏感数据，除非特殊许可。例如，在欧盟成员国希腊，希腊的《个人数据处理方面的个人保护法》

参考	选择和同意标准	控制措施和规程的说明	其他考虑因素
			第 7 条规定，"禁止收集和处理敏感数据"。然而，可以通过获得许可的方式收集和处理敏感数据。 一些司法管辖区认为，政府颁发的个人标识符，例如社会安全号码或社会保险号码，是敏感信息。
3.2.4	**同意向/从个人计算机或其他类似电子设备传输在线数据** 在将个人信息转移到个人电脑或其他类似设备或从其转移出去之前，必须获得同意。	该组织要求客户允许在客户的计算机或其他类似的电子设备中存储、更改或复制个人信息(除 cookies 外)。 如果客户向组织表示不需要 cookies，组织有控制措施确保 cookies 不存储在客户的电脑或其他类似的电子设备中。 组织不会在未获得许可的情况下下载会传输个人信息的软件。	应考虑防止或检测引入用于从计算机或其他类似电子设备中挖掘或提取信息的软件，因为这些软件可能被用来提取个人信息，例如间谍软件。

收集

参考	收集标准	控制措施和规程的说明	其他考虑因素
4.0	**该组织只为通知中确定的目的收集个人信息。**		
4.1	**政策与沟通**		
4.1.0	**隐私政策** 该组织的隐私政策涉及个人信息的收集。		一些司法管辖区，如欧洲的一些国家，要求收集个人信息的组织向其监管机构登记。
4.1.1	**与个人的沟通** 个人被告知，个人信息的收集仅用于声明中确定的目的。	该组织的隐私声明披露了所收集的个人信息的类型，用于收集个人信息的来源和方法，以及是否开发或获得关于个人的信息，如购买模式。	
4.1.2	**收集的个人信息的类型和收集的方法** 收集的个人信息的类型和收集方法，包括使用 cookies 或其他跟踪技术，在隐私声明中都有记录和描述。	收集的个人信息类型包括以下内容： • 财务(例如：财务账户信息) • 健康(例如：关于身体或精神状态或历史的信息) • 人口统计学(例如：年龄、收入范围、社会地理代码)。 个人信息的收集方法和第三方来源包括以下内容： • 信用报告机构 • 通过电话 • 通过互联网使用表单、cookies 或网络	一些司法管辖区，如欧盟的司法管辖区，要求个人有机会拒绝使用 cookies。

参考	收集标准	控制措施和规程的说明	其他考虑因素
		信标 该组织的隐私声明披露其是否使用 cookies 和网络信标以及如何使用。该通知还描述了如果拒绝使用 cookie 的后果。	
4.2	**规程和控制措施**		
4.2.1	**收集仅限于确定的目的** 个人信息的收集仅限于声明中限定的目的。	系统和规程已经准备就绪，以 • 指定对声明中所列目的必要的个人信息，并将其与可选个人信息区分开。 • 定期审查组织的计划或服务对个人信息的需求(例如，每五年一次或在计划或服务发生变化时)。 • 在收集敏感个人信息时获得明确的同意(见 3.2.3，"敏感信息的明确同意")。 • 监督对个人信息的收集仅限于隐私声明中所列目的必要信息，以及所有可选数据都被确定为可选数据。	
4.2.2	**通过公平和合法的手段收集** 收集个人信息的方法在实施之前由管理层进行审查，以确认个人信息的获得： (a) 公平，没有恐吓或欺骗； (b) 合法，遵守所有与收集个人信息有关的	该组织的管理层、隐私官和法律顾问，审查收集的方法和对其的任何改变。	以下情况可能被认为是欺骗性做法： • 在组织的网站上使用工具，如 cookies 和网络信标，收集个人信息，而不向个人提供声明 • 在未告知个人的情况下，收集其访问网站所产生信息，并与其他来源的个人信

参考	收集标准	控制措施和规程的说明	其他考虑因素
	法律规则，无论是来自法规还是普通法。		息进行关联。 • 利用第三方来收集信息，以避免向个人提供声明 各组织应考虑其业务所在辖区以外的法律和监管要求(例如，在加拿大的组织收集欧洲人的个人信息可能要遵守某些欧洲法律要求)。 对投诉的审查可能有助于确定是否存在不公平或非法的做法。
4.2.3	**从第三方收集信息** 管理部门确认，从其收集个人信息的第三方(即个人以外的来源)是可靠的来源，可以公平和合法地收集信息。	该组织 • 在与第三方数据提供者建立关系之前进行尽职调查。 • -在接受第三方数据来源的个人信息之前，审查第三方的隐私政策、收集方法和同意类型。	合同中包括要求公平、合法地收集个人信息并从可靠来源收集的条款。
4.2.4	**开发的关于个人的信息** 如果该组织开发或获得有关他们的额外信息供其使用，将通知个人。	该组织的隐私声明表明，如果适用，它可能利用第三方来源、浏览、信用和购买历史等开发和获得有关个人的信息。	

使用，留存和处置

参考	使用，留存和处置标准	控制措施和规程的说明	其他考虑因素
5.0	**该组织将个人信息的使用限制在声明中所明确的，以及个人已提供隐含或明确同意的目的范围。该组织仅在为实现所述目的法律法规要求的情况下留存个人信息，此后将适当地处理这些信息。**		
5.1	**政策与沟通**		
5.1.0	**隐私政策** 该组织的隐私政策涉及个人信息的使用、留存和处理。		
5.1.1	**与个人的沟通** 个人被告知，其个人信息： (a) 仅用于声明中确定的目的，并且仅在个人提供隐含或明确同意的情况下使用，除非法律法规另有规定； (b) 留存时间不超过实现所述目的的必要时间，或法律或法规特别要求的时间；以及 (c) 以防止丢失、盗窃、滥用或未经授权访问的方式进行处置。	该组织的隐私声明描述了个人信息的以下用途，例如： • 处理商业交易，如索赔和担保、工资、税收、福利、股票期权、奖金或其他补偿计划 • 处理有关产品或服务的询问或投诉，或在推广产品或服务期间进行互动 • 产品设计和开发，或购买产品或服务 • 参与科学或医学研究活动、营销、调查或市场分析 • 网站的个性化设计或下载软件	

参考	使用，留存和处置标准	控制措施和规程的说明	其他考虑因素
		• 法律要求 • 直接营销 该组织的隐私声明解释，个人信息将只留存到完成所述目的时，或法律或法规特别要求的时间，此后将被安全地处理或成为匿名信息，以避免关联到任何个人。	
5.2	**规程和控制措施**		
5.2.1	**个人信息的使用** 个人信息仅用于声明中确定的目的，并且仅在个人提供默认或明确同意的情况下使用，除非法律或法规另有明确规定。	系统和规程已准备就绪，以确保个人信息的使用： • 符合该组织的隐私声明中确定的目的。 • 符合从个人获得的同意。 • 遵守适用的法律和法规。	一些法规对个人信息的使用有具体规定。例如，《美国政府法案》、《健康保险可携性和责任法》(HIPAA)，以及《儿童在线隐私保护法》(COPPA)。
5.2.2	**个人资料的留存** 个人资料的留存时间不超过实现所述目的的必要时间，除非法律或法规另有规定。	该组织 • 记录其留存政策和处置规程。 • 根据其留存政策，留存、储存和处理记录的存档和备份副本。 • 确保个人信息的留存时间不超过标准的留存时间，除非有合理的商业或法律理由这样做。 在信息留存的实践中要考虑合同要求，这可	一些法律规定了个人信息的留存期限。例如，HIPAA 对个人健康信息披露的核算有留存要求–电子健康记录留存 3 年，非电子健康记录留存 6 年。 其他法定的记录留存要求也可能存在；例如，某些数据可能需要为税收目的或根据就业法而留存。

参考	使用，留存和处置标准	控制措施和规程的说明	其他考虑因素
		能是常规政策的例外情况。	
5.2.3	**个人资料的处理、销毁和再加工** 不再留存的个人信息将被匿名化、处置或销毁，以防止丢失、被盗、滥用或未经授权的访问。	该组织 • 根据留存政策，删除或销毁记录，无论储存方法如何(例如，电子、光学媒体或基于纸张)。 • 根据其销毁政策处理原始的、存档的、备份的和临时的或个人的记录副本。 • 记录个人信息的处理情况。 • 在技术范围内，找到并删除或按要求删改关于个人的特定信息，例如，在交易完成后删除信用卡号码。 • 定期和系统地销毁、清除或使不再需要的个人信息成为匿名信息，以实现已确定的目的或按照法律法规的要求。 如果合同要求可能导致组织的常规政策出现例外，则在制定处置、销毁和编辑做法时要考虑这些要求。	应该考虑使用专业公司提供的安全销毁个人信息服务。这其中的某些公司会在需要时提供销毁证书。 某些归档技术，如 DVD、CD、微缩胶片或微缩平片，可能无法在不销毁这些介质上整个数据库的情况下删除个别记录。

访问

参考	访问标准	控制措施和规程的说明	其他考虑因素
6.0	**该组织为个人提供了审查和更新其个人信息的途径。**		
6.1	**政策与沟通**		
6.1.0	**隐私政策** 该组织的隐私政策涉及向个人提供对其个人信息的访问。		
6.1.1	**与个人的沟通** 个人被告知如何获得他们的个人信息以审查、更新和纠正该信息。	该组织的隐私声明 • 解释个人如何获得对他们个人信息的访问以及与这种访问有关的任何费用。 • 概述了个人可以更新和纠正其个人信息的方式(例如，通过书面、电话、电子邮件或使用该组织的网站)。 • 解释如何解决与个人信息有关的分歧。	
6.2	**规程和控制措施**		
6.2.1	**个人对其个人信息的访问** 个人能够确定该组织是否保存有关于他们的个人信息，并且在提出要求后，可以访问他们的个人信息。	已制定规程以 • 确定该组织是否持有或控制关于个人的信息。 • 告知获取个人信息所需的步骤。	一些法律和法规规定了以下内容： • 提供访问个人信息的规定和要求(例如，HIPAA)。 • 要求以书面形式提交访问个人信息的请求

参考	访问标准	控制措施和规程的说明	其他考虑因素
		• 及时回应个人的请求。 • 根据要求，以个人和组织都方便的打印或电子形式，提供个人信息的副本。 • 记录访问请求和采取的行动，包括拒绝访问和未解决的投诉和争议。	
6.2.2	**对个人身份的确认** 要求访问信息的个人，在其获得信息前，应对其身份进行验证。	雇员接受了充分的培训，以便在批准下列事项之前验证个人的身份： • 访问他们的个人信息 • 更改敏感信息或其他个人信息的请求(例如，更新地址或银行资料等信息)。 该组织： • 不使用政府颁发的身份识别资料(例如：社会安全号码或社会保险号码)进行认证。 • 只向记录地址邮寄有关变更请求的信息，或者在地址变更的情况下，同时向新旧地址邮寄。 • 要求使用独特的用户识别和密码(或同等的)来在线访问用户账户信息。	认证的程度取决于所提供的个人信息的类型和敏感性。对于不同的渠道可以考虑采用不同的技术，例如： • 网络 • 交互式语音应答系统 • 呼叫中心 • 亲临现场
6.2.3	**可理解的个人信息、时间范围和费用**	该组织：	各组织可以免费或以最低成本向个人提供对其个人信息的访问，因为这对商业和客户关

参考	访问标准	控制措施和规程的说明	其他考虑因素
	以可理解的形式，在合理的时间范围内，以合理的费用(如有)向个人提供个人信息。	• 以可理解的格式(例如，不是以代码、一系列数字、过于技术性的语言或其他行话)，并以方便个人和组织的形式，向个人提供个人信息。 • 付出合理的努力来找到所要求的个人信息，如果无法找到个人信息，则留存足够的记录以证明已经进行了合理的检索。 • 采取合理的预防措施，确保所发布的个人信息不会直接或间接地识别另一个人。 • 对个人信息访问请求的响应时间范围应与该组织在其常规业务交易的正常响应时间相似，或根据法律允许或要求的情形。 • 提供对存档或备份系统以及介质中个人信息的访问。 • 在提出访问要求时或在此后尽快告知个人获取信息的费用。 • 向个人收取的费用(如有任何费用的话)其数额不超过该组织提供信息的成本。 • 提供适当的物理空间来检查个人信息。	系有潜在的好处，也有机会提高信息的质量。

参考	访问标准	控制措施和规程的说明	其他考虑因素
6.2.4	**拒绝访问** 在法律或法规特别允许或要求的情况下，个人将被书面告知访问其个人信息的请求被拒绝的原因，组织拒绝该请求的法律权利来源(如果适用)，以及当个人质疑这种拒绝访问时，法律法规所赋予或要求的权利(如果有)。	该组织 • 概述可能被拒绝获取个人信息的原因。 • 记录所有拒绝访问的情况和未解决的投诉和争议。 • 在有理由拒绝个人获取其部分个人信息的情况下，为个人提供部分访问权。 • 向个人提供书面解释，说明拒绝获取个人信息的原因。 • 如果对个人信息的访问被拒绝，提供一个正式的升级(上诉)程序。 • 传达组织的法律权利和个人的质疑权利(如适用)。	一些法律和法规(例如，1988 年澳大利亚隐私法第 2 点，第 5 项原则，"与记录者保存的记录有关的信息"，以及 PIPEDA 第 8.(4)、8.(5)、8.(7)、9、10 和 28 条)规定了可以拒绝访问的情况，应遵循的程序(例如在 30 天内书面通知客户拒绝访问)，以及对违反行为的潜在惩罚或制裁。
6.2.5	**更新或更正个人信息** 个人能够更新或更正组织所持有的个人信息。如果实践和经济上可行的话，该组织应将该更新或更正信息发送给此前接收过该个人信息的第三方。	该组织 • 说明个人更新或更正个人信息记录必须遵循的流程(例如，通过书面、电话、电子邮件或使用该组织的网站)。 • 核实个人更新或更正的个人信息的准确性和完整性(例如，通过编辑和验证控制措施，以及强制填写必填项)。 • 如果组织的雇员代表个人进行更改，则	在一些司法管辖区(例如，PIPEDA，附表 1，第 4.5.2 和 4.5.3 条)，个人信息不能被删除，但组织有义务停止进一步处理。

参考	访问标准	控制措施和规程的说明	其他考虑因素
		记录日期、时间和该雇员的身份。 • 在可能和合理的情况下，将个人信息的修改、删除或屏蔽通知给被披露的第三方。	
6.2.6	**分歧的声明** 以书面形式告知个人，更正个人信息的请求被拒绝的原因，以及他们可以如何上诉。	如果个人和组织对个人信息是否完整和准确有分歧，个人可以要求组织接受声称个人信息不完整和准确的声明。 该组织 • 记录个人和该组织对个人信息是否完整和准确有异议的情况。 • 以书面形式通知个人更正个人信息的请求被拒绝的原因，并列出个人的上诉权利。 • 当要求访问个人信息或实际提供访问时通知个人，不同意的声明可以包括有关个人寻求更改的性质以及实体拒绝更改的原因的信息。 • 在适当的情况下，通知先前已获得个人信息的第三方存在分歧以及分歧的性质。。	见 10.1.1，"与个人的沟通"，10.2.1，"询问、投诉和争议程序"，以及 10.2.2，"争议解决和追索"。 一些法规(例如，HIPAA)对拒绝请求和处理个人的分歧有具体要求。 如果分歧的解决没有让个人满意，在适当的时候，这种异议的存在会被告知有机会接触有关信息的第三方。

向第三方披露

参考	披露给第三方标准	控制措施和规程的说明	其他考虑因素
7.0	**该组织仅出于声明中确定的目的，并在征得个人默示或明确同意的情况下，向第三方披露个人信息。**		
7.1	**政策与沟通**		
7.1.0	**隐私政策** 该组织的隐私政策涉及向第三方披露个人信息的问题。		
7.1.1	**与个人的沟通** 个人被告知，除非法律或法规特别允许或要求，否则个人信息只为声明中明确的目的而向第三方披露，并且个人已经提供了隐含或明确的同意。	该组织的隐私声明 • 说明与第三方共享个人信息(如果有的话)的相关实践以及信息共享的原因。 • 确定向其披露个人信息的第三方或第三方的类别。 • 告知个人，向第三方披露个人信息仅用于 (a) 声明中确定的目的，以及 (b) 个人已提供隐含或明确同意的目的，或法律或法规特别允许或要求的目的。	该组织的隐私声明可以披露以下内容： • 用于保证已披露给第三方的个人信息的隐私和安全的流程 • 如何保持与第三方共享的个人信息是最新的，以便在个人改变其信息的情况下，与第三方共享的过时或不正确的信息会被更改

参考	披露给第三方标准	控制措施和规程的说明	其他考虑因素
7.1.2	**与第三方的沟通** 处理个人信息的隐私政策或其他具体指示或要求会传达给被披露个人信息的第三方。	在与第三方共享个人信息之前，该组织将其隐私政策或处理个人信息的其他具体指示或要求传达给第三方，并获得第三方的书面同意，即其对所披露的个人信息的隐私做法符合这些政策或要求。	
7.2	**规程和控制措施**		
7.2.1	**个人信息的披露** 除非法律或法规特别要求或允许，否则个人信息只为声明中描述的目的，以及个人已提供隐含或明确同意的目的而向第三方披露。	系统和规程已准备就绪，以 • 防止向第三方披露个人信息，除非个人已默示或明确同意披露。 • 记录向第三方披露的个人信息的性质和范围。 • 测试向第三方的披露是否符合该组织的隐私政策和规程，或法律法规特别允许或要求的披露。 • 记录任何因法律原因向第三方的披露。	个人信息可能会通过各种法律程序向执法机构或监管机构披露。 一些法律和法规对个人信息的披露有具体规定。有些允许在未经同意的情况下披露个人信息，而有些则需要可核实的同意。
7.2.2	**个人信息的保护** 个人信息只披露给与该组织有协议的第三方，以符合该组织隐私政策的相关方面或其他具体指示或要求的方式保护个人信息。该组织有相应的规程来评估第三方是否具备有效的控制措施来满足协	在向第三方提供个人信息时，该组织签订的合同要求对个人信息的保护水平与该组织的保护水平相当。在这样做时，该组织 • 将第三方对个人信息的使用限制在履行合同所必需的目的范围内。 • 将个人的偏好传达给第三方。	该组织对其拥有或保管的个人信息负责，包括已转移给第三方的信息。 一些法规(例如，来自美国联邦金融监管机构)要求组织采取合理步骤，通过在选择服务提供商时进行适当的尽职调查来监督适当的服务提供商。

参考	披露给第三方标准	控制措施和规程的说明	其他考虑因素
	议、指示或要求的条款。	• 将任何关于组织转让的个人信息的访问请求或投诉提交给指定的隐私负责人，如企业隐私官。 • 规定第三方如何以及何时处置或归还该组织提供的任何个人信息。 该组织使用以下一种或多种方法评估对此类合同的遵守情况，以根据其风险评估获得越增强的保证水平： • 第三方对有关其做法的调查问卷作出答复。 • 第三方根据内部审计报告或其他程序，自我证明其做法符合该组织的要求。 • 该组织对第三方进行现场评估。 • 该组织收到独立审计师提供的审计或类似报告。	一些司法管辖区，包括欧洲的一些国家，要求转移个人信息的组织在转移之前向其监管机构登记。 PIPEDA 要求在个人信息被第三方处理时提供类似的保护水平。 欧盟指令第 25 条规定，只有在第三方确保足够的保护水平的情况下，才可以进行这种转移。
7.2.3	**新的目的和用途** 只有在个人事先默示或明确同意的情况下，才会将个人信息披露给第三方用于新的目的或用途。	系统和程序已经到位，以便 • 在向第三方披露个人信息以达到隐私声明中未指明的目的之前，通知个人并获得其同意。 • 记录该组织是否已通知个人并获得个人的同意。	其他类型的转移包括转移至下列第三方，即 • 子公司或关联公司。 • 提供个人要求的服务。 • 执法机构或监管机构。 • 在另一个国家，并可能受到其他要求的

参考	披露给第三方标准	控制措施和规程的说明	其他考虑因素
		• 监督个人信息是否仅被提供给第三方用于隐私声明中规定的用途。	影响。
7.2.4	**第三方对个人信息的滥用** 该组织采取补救措施，以应对该组织传输给第三方的个人信息被滥用的情况。	该组织 • 审查投诉，以确定任何第三方滥用个人信息的迹象。 • 对任何有关第三方违反组织的隐私政策和规程或合同安排而使用或披露个人信息的情况做出反应。 • 在可行的范围内，减轻因第三方违反组织的隐私政策和规程使用或披露个人信息而造成的任何损害(例如，通知受影响的个人，尝试恢复披露给他人的信息，取消受影响的号码并重新发放新号码)。 • 在第三方滥用个人信息的情况下采取补救措施(例如，合同条款涉及滥用个人信息的后果)。	

隐私安全

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
8.0	**该组织保护个人信息免受未经授权的访问(包括物理和逻辑)。**		
8.1	**政策与沟通**		
8.1.0	**隐私政策** 该组织的隐私政策(包括任何相关的安全政策)，解决个人信息安全问题。	隐私政策充分应对安全措施，以保障个人信息的隐私，无论是电子、纸张还是其他形式。安全措施与个人信息的敏感程度相一致。	在由组织或被认为将由组织控制下的任何位置的个人信息必须得到保护。
8.1.1	**与个人的沟通** 个人被告知将采取预防措施来保护个人信息。	该组织的隐私声明描述了用于保护个人信息的常规类型安全措施，例如： • 雇员被授权根据工作职责访问个人信息。 • 使用认证来防止未经授权访问以电子方式存储的个人信息。 • 对以硬拷贝形式存储的个人信息保持物理安全，并使用加密技术来防止未经授权访问通过互联网发送的个人信息。 • 对敏感信息采取额外的安全保障措施。	用户、管理层、供应商和其他各方应努力制定和采用良好的隐私实践，并促进认识到安全需求和尊重他人合法利益的行为。 应考虑在隐私声明中披露个人的安全义务，如对用户 ID 和密码保密和报告安全漏洞。 应考虑限制对详细安全规程的披露，以避免损害内部安全。
8.2	**规程和控制措施**		
8.2.1	**信息安全计划** 已经制定、记录、批准和实施了一项安全计	该组织的安全计划涉及以下与保护个人信息有关的事项：	所采用的保障措施可以考虑数据的性质和敏感程度，以及该组织业务的规模和复杂性。例如，该组织对个人信息和其他敏感信息的

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
	划，其中包括管理、技术和物理保障措施，以保护个人信息免遭丢失、滥用、未经授权的访问、披露、更改和破坏。该安全计划应涉及，但不限于以下领域[3]，只要它们与个人信息安全有关： *a.* 风险评估和处理[第 1.2.4 节] *b.* 安全政策[第 8.1.0 节] *c.* 信息安全组织[第 1、7 和 10 节]。 *d.* 资产管理[第 1 节] *e.* 人力资源安全[第 1 节] *f.* 物理和环境安全[第 8.2.3 和 8.2.4 节]。 *g.* 通信和业务管理[第 1、7 和 10 节] *h.* 访问控制[第 1、8.2 和 10 节]。 *i.* 信息系统的获取、开发和维护[第 1.2.6 节] *j.* 信息安全事件管理[第 1.2.7 节]。	• 定期的风险评估 • 确定所有类型的个人信息和相关流程、系统以及参与处理这些信息的第三方 • 确定和记录授权用户的安全要求 • 允许访问，该访问的性质，以及谁授权这种访问 • 通过使用有效的物理和逻辑访问控制，防止未经授权的访问 • 增加新的用户，修改现有用户的访问级别，以及删除不再需要访问的用户的程序。 • 分配安全的责任和义务 • 分配系统更改和维护的责任和义务 • 保护操作系统和网络软件及系统文件 • 保护加密工具和信息 • 实施系统软件的升级和补丁在实施前测	保护程度可能高于其对其他信息的保护程度。 一些法规(例如，HIPAA)对需要考虑和实施的具体安全措施提供了更多的细节和指导。 一些安全规则(例如，与 GLBA 有关的保护信息的规则)要求如下。 • 董事会(或董事会任命的委员会或个人)批准和监督组织的信息安全计划。 • 一个组织应采取合理措施，通过以下方式监督适当的服务提供商 › 在选择服务提供者时进行适当的尽职调查。 › 通过合同要求服务提供商对有问题的个人信息实施并保持适当的保护措施。 支付卡行业已经为某些品牌的持卡人信息制定了具体的安全和隐私要求。

[3] 这些领域来自于 ISO/IEC 27002:2005，信息技术-安全技术-信息安全管理实践准则。美国国家标准协会（ANSI）代表国际标准化组织（ISO）给予许可。ISO/IEC 27002 的副本在美国可以从 ANSI 购买，网址是 http://webstore.ansi.org/，在加拿大可以从加拿大标准委员会购买，网址是 www.standardsstore.ca/eSpecs/index.jsp。不一定要满足 ISO/IEC 27002:2005 的所有标准才能满足公认隐私原则的标准 8.2.1。与每个领域相关的参考资料表明与此目的最相关的《公认隐私原则》标准。

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
	k. 业务连续性管理[第 8.2 节] *l.* 合规[第 1 和第 10 节]	试、评估和授权系统组件 • 处理如何解决与安全问题有关的投诉和请求 • 处理错误和遗漏、安全漏洞和其他事件 • 检测实际和企图的攻击或入侵系统的规程，并主动测试安全规程(例如，渗透测试) • 分配培训和其他资源以支持其安全政策 • 在系统处理安全和相关系统安全策略时未明确的例外情况做出规定 • 业务连续性管理和灾难恢复计划及相关测试 • 规定识别适用的法律和法规、确定的承诺、服务级别协议和其他合同，并与之保持一致 • 要求用户、管理层和第三方确认(初始阶段和每年)他们理解并同意遵守该组织与个人信息安全有关的隐私政策和规程 • 取消访问权限的程序，并确保在人员被解雇时归还用于访问或存储个人信息的计算机和其他设备	

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
		该组织的安全计划防止访问该组织不再活跃的计算机、存储介质和纸质信息中的个人信息(例如，储存、出售或以其他方式处理的计算机、存储介质和纸质信息)。	
8.2.2	**逻辑访问控制** 对个人信息的逻辑访问是通过处理以下事项的规程来限制的。 *a.* 对内部人员和个人进行授权和登记 *b.* 识别和验证内部人员和个人的身份 *c.* 进行更改和更新访问配置文件 *d.* 授予访问 IT 基础设施组件和个人信息的特权和权限 *e.* 防止个人访问他们自己个人或敏感信息以外的任何东西 *f.* 限制对个人信息的访问，只允许经授权的内部人员根据其分配的角色和责任访问。 *g.* 仅将输出内容分发给经授权的内部人员 *h.* 限制对离线存储、备份数据、系统和介质的逻辑访问	系统和规程已准备就绪，以 • 根据数据的敏感性和用户访问个人信息的合法业务需要，确定将向用户提供的访问级别和性质。 • 在允许访问处理个人信息的系统之前，对用户进行认证，例如，通过用户名和密码、证书、外部令牌或生物识别技术。 • 要求加强远程访问的安全措施，如额外的或动态的密码、回调程序、数字证书、安全的 ID 卡、虚拟私人网络(VPN)，或适当配置的防火墙。 • 实施入侵检测和监控系统。	用户授权过程考虑以下几点： • 数据如何被访问(内部或外部网络)，以及存储的介质和技术平台 • 访问含有个人信息的纸质和备份介质 • 在没有其他方法来验证实际个人的情况下，拒绝访问联合账户 一些司法管辖区要求对存储的数据(静态)进行加密或以其他方式进行混淆。

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
	i. 限制对系统配置、超级用户功能、主密码、强力工具和安全设备(例如，防火墙)的访问 *j.* 防止引入病毒、恶意代码和未经授权的软件		
8.2.3	**物理访问控制** 对任何形式的个人信息(包括组织系统中包含或保护个人信息的组件)的物理访问都受到限制。	系统和规程已准备就绪，以 • 管理对个人信息的逻辑和物理访问，包括硬拷贝、归档和备份拷贝。 • 记录并监控对个人信息的访问。 • 防止未经授权或意外地破坏或丢失个人信息。 • 调查违规行为和试图获得未经授权的访问。 • 将调查结果传达给适当的指定隐私主管。 • 对含有个人信息的报告的分发保持实际物理控制。 • 安全地处理含有机密信息的废物(例如，粉碎)。	物理保障措施可包括使用上锁的文件柜、卡片访问系统、物理钥匙、签到记录和其他技术来控制对办公室、数据中心和其他处理或存储个人信息的地点的访问。
8.2.4	**环境保障措施**	管理层根据其风险评估，保持对环境因素(例如，火灾、水灾、灰尘、停电、过热和潮湿)	一些法规，如欧盟指令中的法规，还要求保护个人信息免遭非法破坏、意外损失、自然

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
	所有形式的个人信息都受到保护，防止因自然灾害和环境危害而意外泄露。	的保护措施。该组织的控制区使用烟雾探测器和灭火系统进行防火保护。 此外，该组织还保持着物理和其他保障措施，以防止在发生环境事件时意外泄露个人信息。	灾害和环境危害，以及意外披露。
8.2.5	**传输个人信息** 个人信息在通过邮件或其他物理方式传输时受到保护。通过互联网、公共网络和其他不安全的网络以及无线网络收集和传输的个人信息，将通过部署行业标准的加密技术来传输和接收个人信息。	系统和规程已准备就绪，以 • 定义最低级别的加密和控制。 • 采用行业标准的加密技术，例如，128 位传输层安全(TLS)，通过 VPN 传输和接收个人信息。 • 批准外部网络连接。 • 保护通过邮件、信使或其他物理方式发送的硬拷贝和电子形式的个人信息。 • 对以无线方式收集和传输的个人信息进行加密，并保护无线网络免受未经授权的访问。	一些法规(例如，HIPAA)对健康信息记录(即与标准交易相关)的电子传输和签名认证有具体规定。 一些信用卡供应商发布了保护持卡人数据的最低要求，包括要求在传输和存储中对信用卡和交易相关数据使用加密技术。 随着技术、市场和监管条件的发展，可能需要采取新的措施来满足可接受的保护水平(例如，128 位安全 TLS，包括用户 ID 和密码)。 从无线设备(例如，手机)传输的个人信息的语音可能不会被加密。
8.2.6	**移动介质上的个人信息** 存储在移动介质或设备上的个人信息受到保护，不会被未经授权的访问。	政策和规程禁止在移动介质或设备上存储个人信息，除非存在业务需要并且这种存储得到管理层的批准。 系统、系统和规程已准备就绪，以保护以诸如使用以下方式访问或存储的个人信息：	应考虑到向监管机构和审计师等提供的任何个人信息所需的保护。

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
		• 笔记本电脑、PDA、智能手机和类似设备 • 员工在旅行和在家工作时使用的计算机和其他设备，例如 • USB 驱动器、CD 和 DVD、磁带或其他便携式媒体 这些信息是加密的，有密码保护，有物理保护，并受组织的访问、留存和销毁政策约束。 对用于备份和恢复的包含个人信息介质的创建、转移、存储和处置有控制措施。 有规程报告含有个人信息介质的遗失或潜在的滥用。 在雇员或承包商被解雇时，规程规定归还或销毁用于访问和存储个人信息的移动介质和设备，以及此类信息的印刷品和其他副本。	
8.2.7	**测试安全保障措施** 至少每年对保护个人信息的主要管理、技术和物理保障措施的有效性进行测试。	系统和规程已准备就绪，以 • 定期测试保护个人信息的主要管理、技术和物理保障措施的有效性。 • 定期使用内部或外部审计员对安全控制进行独立审计。	安全保障措施的测试频率和性质将随组织的规模和复杂性、其活动的性质和范围以及个人信息的敏感性而变化。 一些安全法规(例如，与 GLBA 有关的保护信息的规则)要求一个组织

参考	隐私安全标准	控制措施和规程的说明	其他考虑因素
		• 至少每年对系统和其他物理安全装置进行测试。 • 至少每年记录并测试灾难恢复和应急计划，以确保其可行性。 • 定期进行威胁和脆弱性测试，包括安全渗透和网络脆弱性和复原力。 • 定期对安全政策和规程进行适当的修正，同时考虑到所进行的测试结果以及新的和不断变化的威胁和漏洞。 • 定期向管理层报告安全测试的结果。	• 由独立的第三方或独立于开发或维护安全的工作人员对关键控制、系统和程序进行定期测试(或至少让这些独立方审查测试的结果)。 • 至少每年评估并可能调整其信息安全。

质量

参考	质量标准	控制措施和规程的说明	其他考虑因素
9.0	**该组织为声明中确定的目的维护准确、完整和相关的个人信息。**		
9.1	**政策与沟通**		
9.1.0	**隐私政策** 该组织的隐私政策涉及个人信息的质量问题。		
9.1.1	**与个人的沟通** 个人被告知，他们有责任向该组织提供准确和完整的个人信息，并在需要更正这些信息时与该组织联系。	该组织的隐私声明解释说，只有当个人与该组织有持续关系时，才需要保持个人信息的准确性和完整性。	
9.2	**规程和控制措施**		
9.2.1	**个人信息的准确性和完整性** 就使用目的而言，个人信息是准确和完整的。	系统和规程已准备就绪，以 • 在收集、创建、维护和更新个人信息时，对其进行编辑和验证。 • 记录获得或更新个人信息的日期。 • 规定个人信息何时不再有效。 • 规定何时和如何更新个人信息以及更新的来源(例如，每年重新确认所持有的信息和个人主动更新个人信息的方法)。	

参考	质量标准	控制措施和规程的说明	其他考虑因素
		• 说明如何核实直接从个人获得的、从第三方收到的(见 4.2.3，"从第三方收集")或披露给第三方的个人信息的准确性和完整性(见 7.2.2，"个人信息的保护")。 • 确保持续使用的个人信息足够准确和完整，以便做出决定，除非对准确性的需求有明确的限制。 • 确保个人信息不被例行更新，除非这一过程对于实现其使用目的是必要的。 该组织进行定期评估，以检查个人信息记录的准确性，并在必要时进行纠正，以实现所述目的。	
9.2.2	**个人信息的相关性** 个人信息与使用目的相关。	系统和规程已准备就绪，以 • 确保个人信息与使用目的充分相关，并尽量减少不适当的信息被用于对个人进行商业决策的可能性。 • 定期评估个人信息记录的相关性，并在必要时予以纠正，以尽量减少使用不适当的数据进行决策的现象。	

监督与执行

参考	监督与执行标准	控制措施和规程的说明	其他考虑因素
10.0	**该组织监测其隐私政策和规程的遵守情况，并有程序处理与隐私有关的查询、投诉和争议。**		
10.1	**政策与沟通**		
10.1.0	**隐私政策** 该组织的隐私政策涉及隐私政策和规程的监督和执行。		
10.1.1	**与个人的沟通** 个人被告知如何联系组织的查询、投诉和争议。	该组织的隐私声明 • 描述个人如何联系该组织进行投诉(例如，通过电子邮件链接到该组织的网站或电话号码)。 • 提供个人可以直接投诉的相关联系信息(例如，负责处理投诉的个人或办公室的姓名、电话号码、邮寄地址和电子邮件地址)。	
10.2	**规程和控制措施**		
10.2.1	**查询、投诉和争议程序** 有一个处理查询、投诉和纠纷的程序。	公司隐私官或其他指定人员被授权处理与隐私有关的投诉、争议和其他问题。 系统和程序已经到位，允许 • 在沟通和解决有关该组织的投诉时应遵循的程序。	

参考	监督与执行标准	控制措施和规程的说明	其他考虑因素
		• 对有争议的信息将采取的行动，直到投诉得到满意的解决。 • 在发生个人信息泄露的情况下可采取的补救措施，以及如何将这些信息传达给个人。 • 补救措施和正式的升级程序要到位，以审查和批准向个人提供的任何补救措施。 • 与任何指定的第三方争端解决或类似服务(如果提供)的联系信息和程序。	
10.2.2	**争议解决和追索** 每项投诉都会得到处理，解决方案会被记录在案并传达给个人。	该组织有一个正式记录的程序，以 • 对负责处理个人投诉和争议的员工进行有关解决和升级程序的培训。 • 及时记录并回应所有投诉。 • 定期审查未解决的纠纷和投诉，以确保它们得到及时解决。 • 将未解决的投诉和争议上报给管理层审查。 • 确定趋势和改变组织的隐私政策和规程的潜在需要。 • 当个人对组织提出的解决方案不满意	一些法规(例如 HIPAA 和 COPPA)有具体的规程和要求。 一些法律(例如 PIPEDA)允许通过法院系统升级，直至最高级法院。

参考	监督与执行标准	控制措施和规程的说明	其他考虑因素
		时，使用指定的独立第三方争议解决服务或监管机构规定的其他程序，同时由此类第三方承诺处理此类资源。 如果该组织为无法直接与该组织解决的投诉提供第三方争议解决程序，则提供关于个人如何使用该程序的解释。	
10.2.3	**合规性审查** 对隐私政策和规程、承诺和适用的法律、法规、服务级别协议和其他合同的遵守情况进行审查和记录，并向管理层报告此类审查的结果。如果发现问题，将制定和实施补救计划。	系统和规程已准备就绪，以 • 每年审查隐私政策和规程、承诺和适用的法律、法规、服务级别协议、组织采用的标准和其他合同的合规性。记录定期审查，例如，内部审计计划、审计报告、合规性检查表和管理层签字。 • 向管理层报告合规性审查的结果和改进建议，并实施补救计划。 • 监测合规性审查中发现的问题和漏洞的解决情况，以确保及时采取适当的纠正措施(即，必要时修订隐私政策和规程)。	除了法律、法规和合同要求外，一些组织可能会选择遵守某些标准，如 ISO 发布的标准，或被要求遵守某些标准，如支付卡行业发布的标准，作为开展业务的一个条件。
10.2.4	**违规事例** 对不遵守隐私政策和规程的情况进行记录和报告，如有需要，及时采取纠正和纪律措	系统和规程已准备就绪，以 • 通知员工及时报告隐私违规和安全漏洞的必要性。	

参考	监督与执行标准	控制措施和规程的说明	其他考虑因素
	施。	• 告知员工报告安全漏洞和隐私泄露的适当渠道。 • 记录违反隐私政策和规程的情况。 • 监测安全漏洞和隐私泄露的解决情况，以确保及时采取适当的纠正措施。 • 酌情对造成隐私事件或泄露的雇员和其他人进行惩戒。 • 在可行的范围内，减轻因第三方违反组织的隐私政策和规程使用或披露个人信息而造成的任何伤害(例如，通知受影响的个人，尝试恢复披露给他人的信息，取消受影响的账户号码并重新发放新号码)。 • 确定可能需要对隐私政策和规程进行修订的趋势。	
10.2.5	**持续监控** 根据风险评估[见 1.2.4]，执行持续的规程来监测对个人信息控制的有效性，并在必要时及时采取纠正措施。	该组织采用了以下方式： • 控制报告 • 趋势分析 • 培训出席率和评估	《内部控制体系监控指南》，由 COSO 发布 (特雷德韦委员会赞助组织委员会)发布的《监测内部控制系统指南》，为监测控制的有效性提供了有益的指导。

参考	监督与执行标准	控制措施和规程的说明	其他考虑因素
		• 投诉决议 • 定期内部审查 • 内部审计报告 • 涉及服务组织控制的独立审计报告 • 其他关于控制有效性的证据 要监视的控制措施的选择和监视的频率是基于信息的敏感性和信息可能暴露的风险。 此类控制措施的例子如下： • 政策要求所有雇员在受雇后 30 天内接受初步的隐私培训。持续的监控活动将包括审查选定员工的人力资源档案，以确定他们包含完成课程的适当证据。 • 政策要求，每当雇员改变工作职责或被解雇时，应在 24 小时内(或在雇员被解雇的情况下立即)审查并适当修改或终止该雇员对个人信息的访问。这是由人力资源系统内的一个自动程序控制的，该程序产生一份关于雇员状态变化的报告，这需要主管采取行动以避免自动终止访问。这是由安全小组监控的，该小组收到这些报告的副	

参考	监督与执行标准	控制措施和规程的说明	其他考虑因素
		本和相关的主管行动。 • 政策规定，在 72 小时内向投诉人提供与隐私有关的投诉确认，如果在 10 个工作日内没有得到解决，那么问题就会升级到首席检察官。控制措施是用来记录隐私投诉的日志，包括投诉日期和随后的活动，直至解决。监测活动是每月对此类日志进行审查，以确保与本政策的一致性。	

附录 A-词汇表

关联公司。一个控制、被控制或与另一组织共同控制的组织。

匿名化。去除任何可用于识别特定个人的与人有关的信息。

保密性。保护非个人信息和数据不被擅自披露。

同意。个人同意该组织按照隐私声明收集、使用和披露个人信息。这种同意可以是明确的或默认的。明确同意是以口头、电子或书面形式作出的，是明确的，不需要寻求同意的组织方面作出任何推断。默认同意可以从个人的行动与否中合理地推断出来，如没有选”选择退出”，或提供信用卡信息以完成交易。(见选择加入和选择退出)。

Cookies。Cookies 是由网络服务器生成的信息，并存储在用户的计算机中，以备将来使用。然后，这些信息可用于在返回网站时识别用户，使网站内容个性化，并根据以前的购买习惯推荐可能感兴趣的项目。某些广告商使用跟踪方法，包括 cookies，来分析网站的模式和路径。

加密。改变信息的过程，使其无法被任何人阅读，除非拥有特殊的密钥(解密)。

组织。一个收集、使用、留存和披露个人信息的团体。

个人。被收集个人信息的人(有时被称为数据主体)。

内部人员。雇员、劳务派遣人员、代理商和其他代表该组织及其附属机构的人。

选择加入。未经个人明确同意，该组织不得收集、使用、留存和披露个人信息。

选择退出。除非个人明确拒绝许可，否则组织在收集、使用、留存和披露个人信息方面存在默认同意。

外包。由为该组织履行业务职能的第三方使用和处理个人信息。

个人信息。关于或可能是关于可识别的个人或与之相关的信息。

个人信息周期。个人信息的收集、使用、留存、披露、处置或匿名化。

政策。传达管理层的意图、目标、要求、责任和标准的书面声明。

隐私。个人和组织在收集、使用、留存、披露和销毁个人信息方面的权利和义务。

隐私违规。当个人信息的收集、留存、访问、使用或披露方式不符合企业政策的规定、适用的隐私法律或法规时，就会发生隐私违规。

隐私管理体系。根据业务和合规风险及要求，为管理和保护个人信息而制定的政策、沟通、规程和控制措施。

目的。该组织收集个人信息的原因。

删改。从文件或档案中删除或涂黑个人信息。

敏感个人信息。需要额外保护和更高注意义务的个人信息，例如，关于医疗或健康状况的信息、某些财务信息、种族或民族血统、政治观点、宗教或哲学信仰、工会会员资格、性偏好，或与犯罪或刑事定罪有关的信息。

第三方。与收集个人信息的组织无关联的组织，或不在该组织的隐私声明范围内的任何关联组织。

网络信标。网络信标，也被称为网络虫子，是一串小的代码，提供了一种在网页上或电子邮件中传递图形图像的方法，以达到传输数据的目的。企业将网络信标用于许多目的，包括网站流量报告、唯一访客计数、广告和电子邮件审计和报告，以及个性化。例如，网络信标可以收集用户的 IP 地址，收集推荐人，并跟踪用户访问的网站。