数据安全与隐私原则

IBM 云服务

KUP12494-CNZH-01

目录

概述

IBM 云服务包括基础架构、平台和软件服务产品。IBM 根据服务架构、预期用途和服务类型，按照 IBM 策略，为所提供的每项云服务实施技术和组织安全与隐私保护措施。图 1 显示了每类服务的常规责任划分情况。

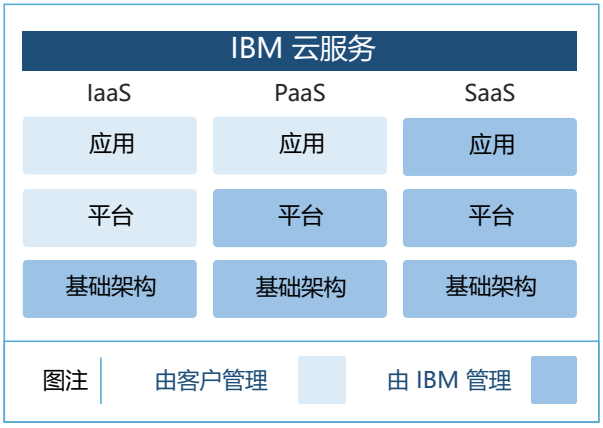

图 1：IBM 云服务产品类型

IBM 基础架构即服务 (IaaS) 产品提供计算资源，以便客户部署和操作软件，如操作系统、运行时、中间件及其所选择的应用。IaaS 客户负责其在 IaaS 解决方案上部署的应用、内容、运行时、中间件和操作系统，包括实施和管理非物理性的数据安全和隐私保护措施。

IBM 平台即服务 (PaaS) 产品允许客户使用系统、网络、存储、运行时框架、库以及集成和管理工具（可能作为服务的一部分包含其中）来创建、部署和管理云应用。PaaS 客户负责管理其在 PaaS 解决方案上部署的应用和内容，包括对其应用和数据实施并管理数据安全和隐私保护措施。

IBM 软件即服务 (SaaS) 产品提供来自云环境的标准化应用，IBM 负责此类应用的部署、管理、运行、维护和安全，包括底层中间件、平台和基础架构。SaaS 客户继续负责管理其最终用户账户、对 IBM SaaS 产品的适当使用，以及根据云服务协议条款而处理的数据。SaaS 客户负责根据自身需求来评估 IBM 实施的标准数据安全和隐私保护措施的适当性。

IBM 针对每项云服务（无论类型）的具体管理职责都将在相关产品协议进行规定。除此之外，数据安全和隐私措施旨在保护 IBM 云服务免受意外丢失、未经授权访问以及未经授权使用客户数据等风险，这些措施在各项服务描述中进行规定或并入其中，包括任何可用的可配置选项和服务。

本“数据安全和隐私原则”文档描述了通过引用而并入每项服务描述中的总体 IBM 策略和实践。

监管

IBM 的 IT 安全策略（通过特定公司指令获得权限）由 IBM CIO 组织制定和管理，并且是 IBM 业务不可或缺的一部分 。相关人员必须遵守 IBM 的内部 IT 策略，且必须接受审计。

安全策略

IBM 至少每年对 IBM 信息安全策略进行一次审查，并根据需要做出调整优化，从而与当今威胁保持同步并与广泛接受的国际标准（例如 ISO/IEC 27001 和 27002）更新一致。

IBM 对所有新员工（包括替补员工）强制执行一系列雇佣证明要求。这些标准还适用于 IBM 全资子公司及合资公司。这些要求（可能进行更改）包括但不限于犯罪背景调查、身份证明验证，以及针对曾为政府机构工作的求职者的其他调查。每个 IBM 公司负责在当地法律适用和允许的范围内在招聘流程中实施上述要求。

IBM 员工每年都必须完成安全和隐私培训，且每年都必须保证他们将遵守 IBM 商业行为准则中规定的 IBM 道德与商业行为准则、保密和安全要求。

IBM 将根据 IBM 事件管理和响应策略、结合适用法律规定的数据泄密通知要求来处理安全事件。

IBM 计算机安全事件响应团队 (CSIRT) 负责开展执行主要的 IBM 全球网络安全事件管理活动。CSIRT 由 IBM 首席信息安全官负责管理，团队成员包括全球事件经理和取证分析师。美国商务部直属国家标准与技术研究所 (NIST) 颁发的计算机安全事件处理指南是 IBM 全球事件管理流程制定的基础。

CSIRT 与 IBM 的其他内部职能部门协调工作，调查可疑事件，并在必要时制定并执行适当的响应计划。一旦确定发生安全事件，IBM 将根据情况及时通知受影响的云服务客户。

访问、干预、传输和分离控制

IBM 云服务架构确保对客户数据实施逻辑分离。内部规则和措施会基于合同目的将各项数据处理工作分离开来，如数据插入、修改、删除和传输等。只有授权人员才能根据职责分离原则访问客户数据（包括任何个人数据），且数据访问将基于身份和访问管理策略得到严格控制，并根据 IBM 内部特权用户监控和审查程序接受严格监控。

IBM 将基于具体角色授予个别员工访问特权，并会对该等权限实施定期验证。客户数据访问仅限于提供客户服务和支持所需的级别（即，所需的最低权限）。

IBM 网络内的数据传输使用有线基础架构，在防火墙之后进行，不使用无线网络。

在接到请求或在服务终止后，我们将根据云服务协议条款，按照 NIST 介质清理准则，以不可恢复的形式呈现客户数据。

服务完整性和可用性控制

IBM 云服务在正式发布之前会接受渗透测试和漏洞扫描。此外，IBM 和授权的独立第三方还会定期开展渗透测试、漏洞扫描和道德黑客行动。

对操作系统资源和应用软件的修改需遵循 IBM 变更管理策略。 对网络设备和防火墙规则的更改也受变更管理策略的约束，并在实施前需由安全人员单独审核。

IBM 的数据中心服务支持 HTTPS、SFTP 和 FTPS 等各种信息传递协议，实现通过公共网络来传输数据。IBM 会 24x7 全天候系统地监控生产数据中心资源。授权管理员将定期开展内外部漏洞扫描，以帮助检测和消除潜在风险。

每项 IBM 云服务都具有根据“ISO 27002 信息安全控制实践规则”而制定、维护、验证和测试的业务连续性和灾难恢复计划。IBM 会根据云服务的架构和预期用途，为每项云服务制定恢复点和恢复时间目标，并将其列入服务描述或其他交易文档中。用于场外存储的备份数据（如有）将在传输之前先行加密。

IBM 会定期开展并审查安全配置和补丁管理活动。IBM 基础架构遵循灾难恢复和固态磁盘镜像等应急规划概念。IBM 会记录并定期重新验证面向其基础架构的业务连续性计划。

活动日志记录和输入控制

IBM 会根据公司策略悉数记录并监控其云服务计算环境中所有的管理性访问和活动，并根据 IBM 全球记录管理计划对这些日志进行归档和保留。IBM 将根据变更管理策略记录和管理生产型云服务所发生的任何变更。

物理安全和进入控制

IBM 贯彻落实物理安全标准，以便限制对数据中心资源的未经授权的物理访问。IBM 数据中心的入口受门禁卡器限制和控制，并由监控摄像头进行监控。只有授权人员才能进入。

未经授权人员进入场所的收发区和装卸台均会受到严格控制。收发需预先安排并经授权人员批准。非操作人员、设施内部人员或保安人员在进入场所时需先行登记，在场所中需由授权人员陪同。

权限期限终止的员工会从访问列表中删除，并要求交还门禁卡。门禁卡的使用将记入日志。

订单控制

IBM 将根据服务协议执行数据处理活动，IBM 在协议中描述了云服务产品的期限、功能、支持和维护条款以及为确保客户数据的保密性、完整性和可用性而应该采取的措施。

合规性

IBM 云服务信息安全标准和管理实践符合 ISO/IEC 27001 信息安全管理标准，并遵守 ISO/IEC 27002 信息安全管理控制实践规则。IBM 将定期开展评估和审计，以跟踪其信息安全标准的遵守情况。此外，所有的 IBM 生产数据中心每年都将接受独立第三方开展的业界标准审计。

第三方子处理机构

IBM 云服务可能需要第三方子处理机构访问客户数据才能正常履行其合同义务。如果此类第三方子处理机构参与云服务交付活动，那么，IBM 会在客户请求时提供此类子处理机构及其角色。IBM 要求所有这些子处理机构保持与 IBM 所提供的整体安全和隐私保护级别相同的标准、实践和策略。

其他资源

IBM 云服务协议

http://www.ibm.com/support/operations/files/pdf/csa_us.pdf

IBM 安全工程门户

http://www.ibm.com/security/secure-engineering/

IBM 安全漏洞管理

http://www.ibm.com/security/secure-engineering/process.html

IBM 商业行为准则

http://www.ibm.com/investor/governance/business-conduct-guidelines.html

有关政府访问数据的致客户函

http://asmarterplanet.com/blog/2014/03/open-letter-data.html

IBM SaaS 数据处理位置

http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&htmlfid=KUJ12409USEN&attachment=KUJ12409USEN.PDF

IBM Corporation

Route 100

Somers, NY

10589

美国出品

2016 年 4 月

本文档为自最初公布日期起的最新版本，IBM 可能会随时对其进行更改。

IBM 产品根据其提供时所依据协议条款和条件获得保证。

请回收利用