安全措施

主讲人：	**ADP——全球安全组织**
版本：	**2.0**
发布日期：	**2019 年 9 月**

目录

术语和定义

以下术语可能在整个文档中出现：

使用的术语或缩写	定义
GETS	全球企业技术与解决方案
GSO	全球安全组织
CAB	变更咨询委员会
DRP	灾难恢复计划
CIRC	GSO 的紧急事件响应中心
SIEM	安全信息和事件管理
IDS	入侵检测系统
DNS	域名系统
NTP	网络时间协议
SOC	服务组织控制
TPSI	可信平台安全基础设施

概述

ADP 维护着一个包含行政、技术和物理防护措施的正式信息安全计划，以保护客户信息的安全性、保密性和完整性。该计划合理设计旨在 (i) 保护客户信息的安全性和机密性，(ii) 防范对信息安全或完整性预期的威胁或危害，以及 (iii) 防止未经授权的访问或使用信息。

本文件包含截至发布之日的 ADP 信息安全措施和实践的概述，但可能会随 ADP 的更改而有所调整。这些要求和实践旨在与 ISO/IEC 27001:2013 信息安全标准保持一致。ADP 定期评估其安全政策和标准。我们的目标是帮助确保安全计划有效且高效地运作，以保护客户及其员工委托给我们的所有信息。

第 1 部分——信息安全政策

信息安全功能的独立性

ADP 的首席安全官负责监督 ADP 的全球安全组织 (GSO) 并向总法律顾问 (GC) 汇报，而不是向首席信息官汇报，这使得 GSO 在 IT 方面具备必要的独立性。GSO 是一支跨部门的综合安全团队，采用多学科的方法来应对网络和信息安全与合规、运营风险管理、客户安全管理、员工保护和业务韧性。GSO 高级管理层在我们的首席安全官的领导下负责管理安全政策、程序和指南。

信息安全政策的正式定义

ADP 已制定并记录正式的信息安全政策，其中规定了 ADP 管理信息安全的方法。该政策涵盖的具体领域包括但不限于：

- **安全管理政策——**概述全球安全组织 (GSO) 和首席安全官 (CSO) 的职责，包括信息安全责任以及从安全角度对招聘流程的控制。
- **全球隐私政策——**讨论个人信息的收集、访问、准确性、披露以及对客户的隐私声明。
- **员工可接受的电子通讯使用和数据保护政策——**描述可接受的使用、各类电子通讯、加密和密钥管理。
- **信息处理政策——**为 ADP 信息的分类提供要求并建立保护控制措施。
- **实体安全政策——**定义 ADP 设施以及随后在此工作的员工和访客的安全要求。
- **安全操作管理政策——**为维护系统补丁提供最低限度的控制措施，有效应对恶意软件的威胁，并维护备份和数据库安全控制。
- **安全监控政策——**为入侵检测系统 (IDS)、日志和数据丢失防护 (DLP) 提供控制。
- **调查和事件管理政策——**定义事件响应、电子发现、员工保护和访问员工电子存储信息的标准。
- **访问和认证政策——**概述身份验证（例如用户 ID 和密码）、远程访问和无线访问的要求。
- **网络安全政策——**路由器、防火墙、活动目录 (AD)、域名系统 (DNS)、电子邮件服务器、隔离区 (DMZ)、云服务、网络设备、Web 代理和交换网络技术组成的安全架构。
- **全球第三方风险和并购政策——**定义聘请任何第三方协助 ADP 实现其业务目标的最低安全控制措施。
- **应用管理策略政策——**在系统开发生命周期的每个阶段建立适当的安全控制措施。
- **业务弹性政策——**通过建立文档、实施、维护和持续改进业务弹性项目的最低要求来管理 ADP 的保护、完整性和保存。
- **融合安全风险管理政策——**确认、监控、响应、分析、治理和新业务举措。

各项政策已在 ADP 内部网发布，所有员工和承包商均可通过 ADP 网络访问。

信息安全政策审查

ADP 每年至少审查一次其信息安全政策，或在影响 ADP 信息系统功能的重大变更发生时进行审查。

第 2 部分——信息安全组织

信息安全角色和职责

GSO 由跨部门的安全团队组成，采用多学科的方法来遵守网络和信息安全标准、运营风险管理、客户安全管理、员工保护和业务弹性。已为 GSO 所有成员正式定义了角色和职责。GSO 负责根据公司政策设计、实施和监督我们的信息安全计划。GSO 的活动由执行安全委员会监督，该委员会的成员包括 ADP 的首席安全官、首席执行官、首席财务官、首席战略官、首席人力资源官和总法律顾问。

移动计算和远程办公政策

ADP 要求对移动设备上的所有机密信息进行加密，以防止因计算机/设备被盗或丢失而造成的数据泄露。远程访问公司网络时，还需要高级端点保护和通过 VPN 的双因素身份验证。所有远程设备都需要密码保护。ADP 员工必须通过安全事件报告流程，立即报告丢失或被盗的远程计算设备。

作为 ADP 的就业条件，所有员工和承包商都必须遵守可接受的电子通讯使用和数据保护政策以及其他相关政策。

第 3 部分——人力资源保障

背景调查

根据个人所在司法管辖区适用的法律要求，ADP 将根据其员工、承包商和第三方的职责和责任进行适当的背景调查。在聘用或雇用此类人员之前，这些检查可确认候选人是否适合处理客户信息。

背景筛查可能包括以下内容：

- 身份/就业资格验证
- 工作经历
- 教育背景和专业资格
- 犯罪记录（经法律授权并取决于当地国家法规）

与员工和承包商签订的保密协议

ADP 雇佣合同和与承包商签订的合同，包含表明他们将有权访问的客户信息相关义务和责任的条款。所有 ADP 员工和承包商均受保密义务的约束。

信息安全培训计划

作为入职培训计划的一部分，所有员工都必须完成信息安全培训。此外，ADP 每年都会举办安全培训，提醒员工在履行日常职责时应履行的责任。

员工责任和纪律处分程序

ADP 发布了一项所有 ADP 员工均必须遵守的安全政策。违反安全政策可能会导致撤销访问权限和/或纪律处分，直至终止咨询合同或雇佣关系。

终止雇佣责任

在终止雇佣关系时的责任已正式记录，至少包括：

- 归还所有由相关员工持有的 ADP 信息和资产，无论其存储在何种介质上
- 终止访问 ADP 设施、信息和系统的权限
- 更改剩余活跃共享账户的密码（如适用）
- 知识转移（如适用）

第 4 部分——资产管理

资产的可接受使用方式

资产的可接受使用方式在若干项政策中进行了说明，这些政策适用于 ADP 员工和承包商，以帮助确保 ADP 及其客户的信息不会因使用这些资产而暴泄露。这些政策中描述的领域示例包括：电子通讯的使用、电子设备的使用以及信息资产的使用。

信息分类

由 ADP 或代表 ADP 获取、创建或维护的信息按以下适用情况指定安全分类：

- 公共 - 示例：营销手册、已发布的年度报告
- 仅限 ADP 内部使用 - 示例：办公室间沟通、操作程序
- ADP 机密 - 示例：个人及敏感个人信息
- ADP 限制 - 示例：财务预测、战略规划信息

处理信息的要求与信息安全分类直接相关。个人信息和敏感个人信息始终被视为 ADP 机密。所有客户信息均被列为机密。

ADP 员工有责任根据其安全分类级别保护并处理信息资产，该级别为每个分类级别提供信息保护和适用的处理要求。ADP 机密性分类适用于由第三方存储、传输或处理的所有信息。

设备和介质处置

当 ADP 设备、文档、文件和媒体被处置或重新使用时，将采取适当措施防止随后检索原始存储在其中的客户信息。所有计算机或电子存储介质上的信息，无论其分类如何，在被发布到 ADP 设施外或被重新利用之前，都会被安全处理，除非该介质被物理销毁。对存储在设备、文件、档案和媒体上的 ADP 信息进行安全销毁/擦除的程序已正式记录。

传输中的实体介质

已实施组织保障措施，以保护包含客户信息的印刷材料免受盗窃、丢失和/或未经授权的访问/修改：(i) 在运输过程中，例如使用密封信封、容器和亲自交付给授权用户；以及 (ii) 在审查、修订或其他处理过程中，从安全存储中移除时。

第 5 部分——访问控制

访问控制的业务需求

ADP 的访问控制策略基于业务定义的要求。政策和控制标准被阐述为访问控制，这些访问控制在所提供服务的所有组件中强制执行，并基于“最小权限”和“需要知道”的原则。

访问基础设施 - 访问控制管理

访问请求（包括移动、添加、创建和删除）会被记录、批准并定期审查。

每年至少进行一次正式审核，以确认个人用户与相关业务角色的准确对应，并且在职位变动后不会继续拥有访问权限。此过程经过审核并记录在 SOC1 [1] type II 报告中。在身份管理系统内，一支专门的 ADP 团队负责授予、拒绝、取消、终止以及停运/停用对 ADP 设施和信息系统的访问权限。ADP 使用集中式身份和访问管理 (IAM) 工具，由专门的 GETS 团队集中管理。根据通过集中式 IAM 工具请求的访问权限，将触发可能涉及用户主管的验证工作流程。访问权限是临时提供的，并且存在工作流程以防止此类访问保持永久。员工在最后一个工作日之后，立即通过停用其门禁卡（员工工牌）来取消对设施的访问权限。该员工的用户 ID 将被立即停用。所有员工的资产均由主管直线经理归还和检查，并与配置管理数据库中的资产清单进行比较。在职位变动或组织变更后，相关业务单位管理层和 IAM 团队需要对用户个人资料或用户访问权限进行修改。此外，每年会进行一次正式的访问权限审查，以验证个人用户的权限是否与其相关的业务角色相符，并确保在职位转移后没有剩余的不相关访问权限。

密码政策

ADP 关联的密码政策在服务器、数据库、网络设备和应用程序中强制执行，具体取决于设备/应用程序的允许程度。密码复杂性源自对受保护数据和内容的风险分析。这些政策符合现行的行业强度和复杂性标准，包括但不限于在适当情况下使用分级、双因素或生物特征身份验证。

客户端应用程序的身份验证要求因产品而异，并且联合服务 (SAML 2.0) 可在使用由 GETS 管理的统一网络和安全层的特定 ADP 应用程序上使用。

会话超时

ADP 根据符合行业标准的基于风险的方法对所有服务器、工作站、应用程序和 VPN 连接实施自动超时。仅在用户提供了有效密码后才可以重新建立会话。

[1] 对于 ADP 提供的某些美国服务，将在 SOC 2 Type 2 报告中进行审计。

第 6 部分——密码学

加密控制

ADP 要求，ADP 与 ADP 第三方之间交换的敏感信息必须使用行业认可的加密技术和强度进行加密（或传输通道必须加密）。或者，也可以使用专用租用线路。

密钥管理

ADP 拥有内部加密安全标准，其中包括明确的密钥管理和密钥托管程序，包括对对称密钥和非对称密钥的管理。

用于 ADP 信息的加密密钥始终被归类为机密信息。对这些密钥的访问严格限制在有必要知道的人士，并且需要提供例外批准。加密密钥和密钥生命周期管理遵循行业标准惯例。

第 7 部分——物理和环境安全

ADP 在物理安全方面的做法有两个目标——为 ADP 员工打造安全的工作环境，并保护存放在 ADP 数据中心和其他战略性 ADP 地点的个人信息。

ADP 安全政策要求 ADP 管理层识别需要特定级别物理安全的领域。只有获得授权的同事方可出于授权目的进入这些区域。ADP 安全区域采用各种物理安全措施，包括视频监控系统、安全徽章（身份控制访问）以及驻守在出入口的安保人员。访客仅可在获得授权的情况下进入，且须始终受到监督。

第 8 部分——运营安全

IT 运营流程规范化

GETS 是负责 IT 基础设施运营和维护的 ADP 部门。GETS 正式维护并记录 IT 运营政策和程序。这些程序包括但不限于以下内容：

- 变更管理
- 备份管理
- 系统错误处理
- 系统重启与恢复
- 系统监控
- 作业调度和监控

基础设施变更管理

GETS 定期召开变更咨询委员会 (CAB)，其成员包括来自各个 ADP 团队的代表。CAB 会议讨论影响部署窗口和生产推广，以及协调生产基础设施中的其他任何变更。

系统容量规划与验收

容量需求受到持续监控和定期审查。根据这些审查，系统和网络会相应地进行扩展或缩减。当由于容量变化或技术发展而必须做出重大更改时，GETS 基准测试团队可能会对相关应用程序和/或系统进行压力测试。在压力测试结束时，团队通过评估以下方面的变化来进行分析：(i) 组件，(ii) 系统配置或版本，或 (iii) 中间件配置或版本，来提供一份详细的性能演变报告。

防范恶意代码

利用行业标准端点保护技术，按照行业标准最佳实践保护 ADP 资产。

备份管理政策

ADP 有政策要求所有生产托管操作必须备份生产信息。备份的范围和频率根据相关 ADP 服务的业务需求、所涉及信息的安全要求以及信息在灾难恢复中的重要性进行执行。定期备份的监控由 GETS 执行，以识别备份问题或异常情况。

安全日志记录和监控

ADP 已实施了中央只读日志基础设施 (SIEM) 以及日志关联和警报系统 (TPSI)。日志警报由 CIRC 及时监控和处理。

所有这些系统都使用独特的网络时间协议 (NTP) 时钟参考进行同步。

每个单独的日志至少包含：

- 时间戳
- 人物（操作员或管理员的身份）
- 内容（有关事件的信息）

ADP 应用程序的审计跟踪和系统日志记录旨在跟踪以下信息：

- 授权访问
- 特权操作
- 未经授权的访问尝试
- 系统警报或故障
- 系统安全设置的更改（当系统允许此类日志记录时）

这些日志仅对 ADP 授权人员可用，并以实时模式发送，以防止数据在存储到安全日志设备之前被篡改。

基础设施系统和监控

ADP 采用适当措施，每周 7 天、每天 24 小时提供基础设施监控。干扰警报由不同的团队根据其严重性等级和解决所需的技能进行管理。

ADP 托管中心设施采用在所有相关处理系统和网络组件上持续运行的监控应用程序，以便向 ADP 员工主动通知问题和警告，以预防可能出现的问题。

技术漏洞管理

所有安装在托管基础设施中的计算机必须遵循安装专门的安全加固操作系统（或安全构建过程）。托管操作为我们基础设施中使用的每种类型的服务器采用了经过强化、批准和标准化的构建。禁止使用开箱即用的操作系统安装，因为这些安装可能会产生漏洞（例如通用系统账户密码），从而引入基础设施风险。这些配置减少了托管计算机运行不必要服务的风险，这些服务可能导致漏洞。

ADP 拥有一套文档化的方法，用于对面向互联网的基于网络的应用程序及其相应的基础设施组件进行发布和定期漏洞评估及合规性审查，其中包括至少 15 个主要类别的测试。评估方法基于内部和行业最佳实践，包括但不限于开放式 Web 应用程序安全项目 (OWASP)、SANS 研究所和 Web 应用程序安全联盟 (WASC)。

第 9 部分——通讯安全

网络安全管理

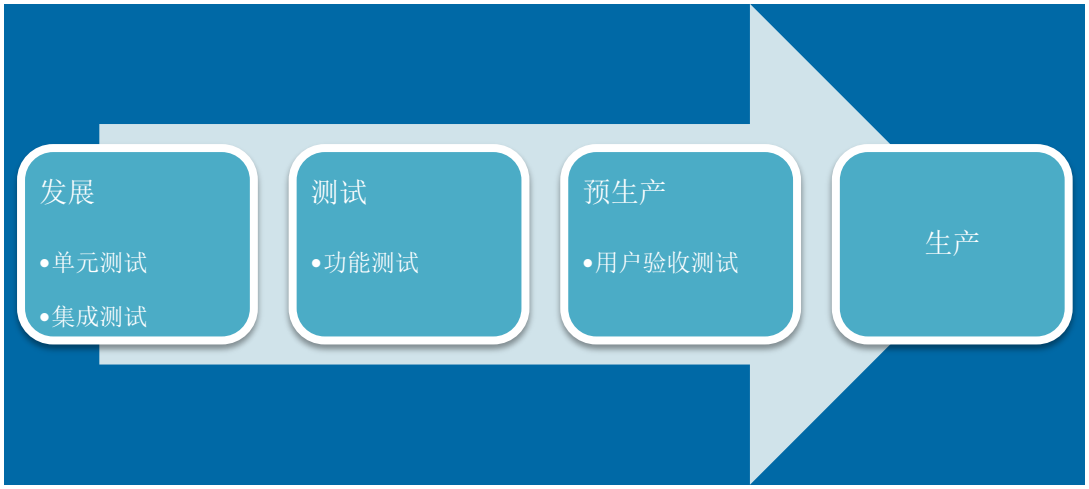
ADP 采用基于网络的入侵检测系统，全天候（每周 7天、每天 24 小时）监控网络基础设施层的流量，并识别可疑活动或潜在攻击。

信息交换

ADP 实施适当的控制措施，以确保 ADP 客户的信息仅在授权的信息系统和资源之间传输，且仅通过 ADP 的安全和授权传输机制进行交换。

开发和支持流程中的安全性

在开发周期中，会生成适用的文档，并为测试阶段制定测试计划。每种环境都定义了不同的阶段，并在每个阶段获得相关批准：



- 要从测试环境转移到预生产环境，需要获得 ADP 质量团队的批准。
- 要从预生产转向生产，需要获得 IT 运营部门的批准。

开发团队必须使用安全编码方法。应用程序变更在进入生产系统之前会在开发和回归环境中进行测试。已进行测试并记录。经批准后，变更将被部署到生产中。在发生重大变化后进行渗透测试。

GETS 定期召开 CAB，参与者包括来自各个 ADP 团队的代表。CAB 会议定期举行，旨在讨论影响、达成部署窗口的共识、批准软件包的生产推广，以及通报生产基础设施的其他变更。

ADP 的 IT 运营团队在软件包推广到生产环境之前提供最终批准。

开发环境的安全性

生产环境和开发环境彼此分开，各自独立。采用适当的访问控制来强制执行适当的职责分离。软件包在开发过程的每个阶段都可以访问，仅限于参与该阶段的团队。

测试数据

根据 ADP 的应用程序管理政策，除非客户明确要求和授权，否则不允许在开发和测试中使用真实或未经净化的数据。

第 11 部分——供应商关系

识别与外部方相关的风险

对需要访问 ADP 和/或客户信息的第三方进行定期的风险评估，以确定其是否符合针对第三方的 ADP 安全要求，并识别所应用控制措施中的任何差距。如果发现安全漏洞，则将与外部方商定新的控制措施。

与外部方的信息安全协议

ADP 与所有第三方签订协议，其中包括适当的安全承诺，以满足 ADP 的安全要求。

第 12 部分——信息安全事件管理

信息安全事故管理及改善

ADP 拥有及时、一致且有效地应对安全事件的记录方法。

一旦发生事故，预先定义的 ADP 员工团队将启动正式的事故响应计划，该计划将解决以下问题：

- 根据事件分类或事件严重程度进行升级
- 事件报告/升级联系人列表
- 初步回应和跟进相关客户的指南
- 遵守适用的安全漏洞通知法律
- 调查日志
- 系统恢复
- 问题解决、报告和审查
- 根本原因和补救措施
- 经验教训

ADP 政策定义了安全事件、事件管理以及所有员工在报告安全事件方面的责任。ADP 还定期对 ADP 员工和承包商进行培训，以帮助确保他们了解报告要求。对培训进行跟踪以确保完成。

第 13 部分——业务弹性管理的信息安全方面

ADP 业务弹性项目

ADP致力于保持我们的服务和运营顺畅，以便为客户提供最佳服务。我们的首要任务是识别并减轻可能妨碍我们提供业务服务的技术、环境、流程和健康风险。ADP 打造出综合框架，其中列出了我们的缓解、准备、响应和恢复流程，并包括：

- 风险评估
- 风险威胁分析
- 业务影响分析
- 计划制定
- 业务连续性计划
- 灾难恢复规划
- 健康与安全规划
- 现实世界响应
- 危机管理
- 紧急响应
- 测试和验证
- 审查
- 修订
- 练习

第 14 部分——合规性

遵守安全政策和标准

ADP 采用一套流程定期在内部进行合规性审查。此外，ADP 还执行 SOC1[2]定期进行第二类审计。这些审计由一家知名的第三方审计公司进行，审计报告在适用时可根据客户的请求每年提供。

技术合规性

为了强制技术符合最佳实践，ADP 会定期执行网络漏洞扫描。然后对扫描结果进行优先排序，并与主办团队及其管理层一起制定纠正行动计划。

定期对内部和外部环境进行漏洞扫描。此外，还会根据每个产品进行源代码扫描和渗透测试。利用专门的应用扫描工具，识别应用层漏洞（如有），并与产品开发管理团队共享，将其纳入质量保证流程以采取纠正措施。对结果进行分析，制定纠正行动计划并确定其优先顺序。

数据保留

ADP 有关客户信息的数据保留政策旨在遵守适用法律。在客户合同结束时，ADP 遵守与客户信息相关的合同义务。ADP 将返回或允许客户检索（通过数据下载）所有客户信息，以确保客户业务活动的连续性（如之前未提供）。然后，ADP 将安全销毁剩余的客户信息，但法律要求、客户授权或争议解决所需的信息除外。

[2] 对于 ADP 在美国提供的某些服务，还会有 SOC 2 Type II 高管报告