如何保护个人身份信息

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Learn How to Secure Personally Identifiable Information, Now		
原文作者	米歇尔·格林利（Michelle Greenlee）	**原文发布日期**	2020 年 8 月 31 日
作者简介	米歇尔·格林利是一位自由技术作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/personally-identifiable-information-security/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

如何保护个人身份信息

米歇尔·格林利

2020 年 8 月 31 日

随着越来越多的员工开始远程工作，企业也面临着更多的安全挑战。员工从各种设备连接到企业的内部网络资源，很多员工甚至使用个人设备进行连接。异地工作给企业带来更大的意外/恶意数据泄露风险。在这种威胁形势下，保护个人身份信息（PII）就更加重要了。

PII 颇受攻击者青睐。IBM 发布的《2020 年数据泄露成本报告》指出，80%的泄露数据包含 PII 数据，这远高于其他类型的数据。在遭泄露的数据中，PII 和身份鉴别凭证高居榜首。

与各端点访问的系统一样，这些端点的安全也非常重要。设备丢失或被盗仍然是企业关心的问题。《2020 年数据泄露成本报告》指出，设备丢失或被盗是数据泄露成本增加的 Top 7 关键因素之一。

保护 PII

保护个人信息是一个持续的过程。企业应遵守网络安全最佳实践，以达到或超过要求的监管标准，这样能够在保护个人隐私的同时将风险降至最低。企业可以采取以下措施，尽全力保护 PII。

1. 将处理、收集和保留的数据最小化

企业可以将数据收集和存储限制在开展业务所需的范围，从而将风险降至最低。在收集个人数据之前，需先征得当事人的许可，且仅在指定的时间内收集信息。此外，还要通过系统控制和使用策略限制对数据的访问。

2. 在传输和存储期间加密数据

企业应加密所有状态的数据——在 PII 传输过程中以及到达目的地时都要对其进行加密。加密标准应满足影响本行业的隐私法规和法律的要求。

3. 限制数据访问和移动

鉴于员工和第三方导致的数据泄露持续增长，企业应限制他们对数据的访问。这包括限

制企业系统内的数据移动，限制、监控并定期评估第三方合作伙伴的访问等。

4. 遵守数据收集和保存规定

隐私法和行业法规会影响企业的数据处理、存储方式和保存时间。企业应遵守行业法规要求，以最好地实现合规性。企业应确保其实践、策略和程序符合监管标准，以及相关的隐私和安全框架。《通用数据保护条例》（GDPR）和《加利福尼亚消费者隐私法案》（CCPA）是新推出的两个法案，对特定地区居民数据的使用和存储做出了规定。

5. 制定数据监管策略

企业应制定一套策略来管理内部的数据访问和使用。这些策略应确保企业的行为符合法规要求。外部法规会影响企业披露数据泄露的方式。企业应通过内部策略提出适当的响应和修复方法。

6. 部署数据丢失防护（DLP）策略

企业应考虑部署下一代 DLP 策略，以减少由于员工离职或潜在内部人员威胁而造成的数据丢失。通过全面的 DLP 策略，企业可以在数据丢失的情况下获得情境信息，以深入了解先前的活动。在应对当前事件时，企业可以分析前几个月的活动。这样能够清晰地了解潜在问题，搞清楚哪里出现了数据泄露；或者明白事件并没有造成严重的后果。

7. 定义数据销毁时间表

随着时间的流逝，某些形式的 PII 会过时。企业应确保数据的准确性，例如定期消除不必要的数据，定期更新数据销毁策略以提高效率，及时调整策略以最好地满足企业的隐私目标等。

8. 维护访问控制策略

企业应跟踪设备签入/签出以及设备上的实际数据，部署设备加密策略并限制设备使用（旅行、个人使用等）。此外，企业应及时更新数据窃取的响应策略以满足其需求，并将这些设备纳入端点管理。

9. 就 PII 访问和处理开展员工培训

企业应将正确的 PII 培训作为整体安全策略的一部分，以防止意外的数据泄漏，阻止恶意的数据泄露。

定期进行安全培训（包括如何识别个人信息）可以防止大量的意外数据泄漏事件。企业应明确规定哪些数据属于 PII，并就这些对员工开展培训。不要想当然地认为所有层级的员工都知道自己在数据保护中所扮演的角色——员工对数据保护的了解可能会有很大差异。

创建安全意识文化

如果未对员工进行恰当的培训，告知他们什么是 PII 以及如何处理 PII，员工就很难确定 PII。安全意识文化可以帮助员工更好地了解数据和信息系统的角色和职责。具有风险意识的员工可以更好地评估潜在的风险情况，尽力规避风险。

员工应了解，在哪些情况下他们会被限制访问某些系统。如果员工不了解这些信息，就会认为限制其访问是不公平或过度控制的，某些员工可能无法接受。

企业可以考虑启动内部人员威胁计划。内部人员威胁仍是企业最主要的安全风险之一。通过这样一个计划，员工可以匿名报告恶意行为，监控系统中的非法活动，帮助防止数据丢失。

关于保护 PII 的最终思考

对攻击者来说，PII 仍然是很有吸引力的高价值攻击目标。要想保护这些宝贵的数据，企业需要持续监控，深入了解数据如何流动以及谁可以访问这些数据。企业应对员工和第三方供应商开展培训，帮助他们正确处理 PII 数据；仅允许经过培训的员工出于必要的业务用途访问 PII 数据；制定适当的措施来管理数据收集；进行适当的数据销毁和存储操作，以符合相关的隐私法规标准。此外，企业应定期检查所有数据操作，以确保数据受到适当的保护。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com