政策，法规和规则

RUL 08.00.13 –网络打印机安全标准

授权： 由信息技术副校长颁发

历史： 首次发行：2015年8月24日。

相关政策：

POL 08.00.01 –计算机使用政策
REG 08.00.02 –计算机使用法规
REG 08.00.03 –数据管理程序

其他参考：

确定共享数据的敏感度级别

https://oit.ncsu.edu/my-it/wolfprint/ SSL证书

联系信息：信息技术办公室安全与合规总监，513-1194

1. 介绍

以下标准旨在帮助NC状态联网打印机的用户（有关此术语的定义，请参阅下面的第2节）在设备受到威胁，丢失或被盗时保护敏感的大学数据。供应商特定的安全措施可能适用于某些设备。本标准描述了连接到大学网络的网络打印机所需的基本技术安全标准。它还提供了建议的最佳实践准则，以实现其他安全控制。

NC州立大学REG 08.00.02-计算机使用条例要求授权用户采取适当的安全预防措施，以保护和保护分配的大学帐户或其他大学和非大学IT资源中或之上的数据。IT资源包括但不限于大学机器，系统或存储设备，或可能包含大学记录/数据的非大学机器，系统或存储设备。为了遵守REG 08.00.02-《计算机使用法规》并确保适当的安全保护，NC州立大学采用以下规则，即所有用户，系统管理员，数据受托人，数据管理员和/或数据托管人（包括第三方服务提供商）必须遵循。

2. **定义**

联网打印机–联网打印机包括但不限于：打印机，多功能设备（MFD），复印机，扫描仪或类似设备。

3. **范围**

本标准适用于连接到大学网络的所有联网打印机，无论它们是否在单位级别获得和管理。

4. **安全要求的例外**

要求将第6节中列举的任何要求的例外情况提交给help@ncsu.edu。请求中应明确记录例外情况的理由和补偿控制措施，以保护网络打印机存储，处理或传输的大学数据。例外请求必须得到相应的园区IT主管（CITD）或其代表的批准。CITD成员负责按照OIT安全与合规性的要求，每年审核和重新认证例外列表。

5. **数据敏感性**

网络打印机可以存储，处理或传输超高度敏感或高度敏感（“紫色”或“红色”）大学数据。存储，处理或传输超高度敏感数据或高度敏感数据的联网打印机可能会受到REG 08.00.03 –数据管理程序中所述的其他安全控制措

施的约束。如果您的网络打印机存储，处理或传输超高度敏感的数据或高度敏感的数据，则必须遵守第6节中的要求。强烈建议您还遵守第7节中建议的最佳实践准则7

6. **网络打印机安全要求（基准技术控制）**

以下要求代表了连接到大学网络的网络打印机的基本技术安全控制措施：

6.1在供应商发布之日起90天内使用相关的重要安全修复程序更新固件。

许多联网打印机都有嵌入式固件，可以直接使用。注意：某些型号（例如HP）具有单独的网络接口卡（NIC）固件和打印功能（例如PostScript）固件。在这些情况下，应同时更新两者的安全修复程序。

6.2在支持的情况下启用内部存储设备（硬盘驱动器）的加密。

许多具有硬盘驱动器的联网打印机都具有完整的磁盘加密功能。在这种情况下，应启用加密功能，以防止未经授权访问硬盘驱动器上的数据。如果网络打印机不支持加密，请禁用缓存，并避免使用该设备打印，扫描或通过电子邮件发送超高度敏感或高度敏感（“紫色”或“红

色”）数据。请参阅数据敏感度级别，网址为：http：//oit.ncsu.edu/security-standards-compliance/determine-sensitiveivity#sensitivity。

6.3设置密码。

通常，每个管理界面都有一个单独的密码。确保每个管理界面都设置了密码，即使是已禁用的密码也是如此，因为下次固件升级可能会重新启用它们。

6.4设置网络访问控制

为了保护网络打印机以及您对碳粉和纸张的投资，请限制对网络打印机的网络访问。访问控制列表不仅可以决定谁可以打印到谁，而且可以决定谁可以连接到网络打印机的管理界面。启用网络打印机的本地防火墙功能，或将其放置在防火墙网络中，例如“复制/打印/扫描VLAN”（请参阅https://oit.ncsu.edu/my-it/wolfprint/；该页面需要Unity身份验证。）设置访问控制列表（ACL），用于限制对校园内客户端的访问：

6.4.1如果要在设备本身上使用本地防火墙来控制访问，请限制在需要打印或管理设备的地方，例如打印服务器，给定的建筑物或子网，或者至少在校园内。这些是

校园网络：152.1.0.0/255.255.0.0、152.7.0.0/255.255.0.0、152.14.0.0/255.255.0.0、10.0.0.0/255.0.0.0。

6.5禁用未使用的管理界面。

联网打印机可以支持许多不同的配置选项，包括内置的Web服务器，文件传输协议（FTP），Telnet和简单网络管理协议（SNMP）。通常，内置的Web服务器用于管理。必须按照指示禁用和修改以下选项：

6.5.1不使用时必须禁用FTP。

6.5.2必须禁用Telnet。

6.5.3 SNMP在不使用时必须被禁用。注意：无论是启用还是禁用SNMP，公共和私有“社区字符串”都必须从供应商默认值中更改。

6.6使用安全协议管理联网打印机。

必须使用事务层安全性（TLS）或等效协议来通过网络安全地连接和管理网络打印机。

6.7如果适用，请禁用未使用的打印接口。

联网打印机可能支持许多不同的协议来向它们发送打印作业。必须使用客户端计算机支持的最安全的打印协议。校园使用的可接受协议是IPP，IPPS和LPR。必须如下配置以下协议：

6.7.1禁用IPX / SPX

6.7.2禁用Appletalk

6.7.3禁用DLC / LLC

6.7.4禁用网页打印，因为它可能允许上传固件

6.8如果不使用，请禁用网络发现协议。

联网打印机可能支持许多不同的发现协议。如果确实使用网络发现协议（例如，mDNS，Bonjour或WS发现），请使用客户端计算机支持的最安全的协议。

6.9在处置或传输之前，请擦除硬盘驱动器上的数据。

根据REG 07.40.01 –在盈余或转让给第三方之前（例如，在退还租用的设备或获得异地维修或保养的情况下），应清除对网络打印机中大学财产硬盘的处理。当传输存储，处理或传输超高度敏感或高度敏感（“紫色”或“红

色”）数据的设备时，在传输之前必须从硬盘驱动器中删除数据。有关硬盘擦除和验证步骤，请参阅制造商的说明。有关将包含硬盘驱动器的联网打印机发送到剩余财产服务的适当步骤，请参阅剩余财产处置准则（http://materialsmgmt.ofb.ncsu.edu/surplus/Surplus-Property-Disposal.php）。

6.10正确配置或禁用网络打印机的电子邮件服务。

如果设备能够发送或接收电子邮件，请正确配置电子邮件服务，以防止对邮件系统的拒绝服务（DOS）攻击和对网络打印机存储，处理或传输的数据的未授权访问。示例方案可能包括但不限于：

6.10.1通知技术人员供应水平

6.10.2打印和/或扫描的文档副本

6.10.3验证“发件人”是有效的NCSU电子邮件帐户和出站电子邮件协议

7. **推荐的最佳做法指南**

7.1练习配置管理。

为确保在大量联网打印机上应用一致的设置，并避免手动配置，建议您使用自动工具来应用设置。通过BOOTP / DHCP / TFTP与安全的网络设置一起加载基准配置文件，和/或使用自动配置管理工具（如HP Web JetAdmin）。

7.2请勿使用自签名证书。

使用InCommon证书。参见http://oit.ncsu.edu/unit-sc/ssl-certs

7.3使用打印服务器。

在配置了适当的访问控制和打印机接口后，打印服务器可让您锁定设备并运行与打印服务器的用户连接。集中的作业管理使对特定设备的访问控制更加容易，并允许人们在特定设备上配置访问控制。通过打印服务器管理设备可以进行集中配置管理，而不必确定如何手动配置每个设备。

7.4。转发日志。

启用打印服务器日志并转发到syslog服务器，然后转发到OIT Security＆Compliance管理的Splunk服务以进行报告和分析。

观众：教师和工作人员。

类别：信息技术。

政策，法规和规则

北卡罗来纳州立大学

北卡罗莱纳州立大学

罗利分校

27695 919.515.2011