上海 XXXXX 印刷厂审核案例

案例类型：信息安全管理体系认证

推荐人员：葛嘉炜

推荐机构：北京新世纪检验认证有限公司

一、 案例背景

审核类型：初审

审核时间：2014-5-20~~5-23AM

审核依据：GB/T22080-2008/ISO/IEC27001:2005

审核组成员：组长：葛嘉炜，组员：戎林、沈向阳

上海 XXXXX 印刷厂是专业从事票据印刷的企业之一，本公司是上海市税务局、市财政局、广电局、邮电局定点印刷发票，财政收据、电影票、信封的定点厂之一,主营业务是商业表格印刷，特种防伪数码印刷。主要产品是发票、收据、无碳复印印刷品、电脑连续纸商业表格印刷品、供激光打印的各种热敏纸影戏舞票，各种压敏、热敏、电脑保密信封及纸质移动通信充值卡，复卷式电脑发票，具有多种防伪印刷功能的各种有价票证等等。

此次审核目的是评价信息安全体系的建立和运行的符合性和有效性，特别是信息安全控制措施的落实情况。

二、 主要审核发现、沟通过程

1） 在综合管理部查对离职人员门禁权限的管理，门禁系统显示聂XX（门禁卡号：3640030）对1楼废品库和晒版车间有权限，实际聂XX已离职，另外系统显示刘XX（门禁卡号：10030090）有对胶印车间的权限，但刘XX也已离职；

现场与负责人沟通：对门禁权限的管理由综合管理部负责，并制定了《门禁系统管理制度》，但是门禁系统管理员本身信息安全意识不强且对管理制度理解不充分，对确认离职人员的权限未能及时撤销，导致系统中仍保留原有权限；经指出，受审核人员意识到自身工作的疏忽，表示会加强对信息安全标准和管理制度的学习。

2） 查见位于一楼的独立小机房，用于放置电话交换机以及支持办公网络的设备，机房由网管负责,现场查见该机房内堆放了部分杂物，配备了空调但未开启，现场也未配备灭火器等消防设施；

公司网管称由于物理场地的限制，目前没有配备专用机房来存放支持日常办公的网络设备，暂时放置在小机房内；经沟通，指出应对存放网络设备的场所的物理环境进行管控，配备必要的支持性设施，确保设备的稳定运行以保证不影响正常办公，受审核人员表示接受。

3） 在办公现场查见资产编号“HAD-01”工作电脑，设置了3位连续数字开机口令，口令强度不符合要求 ；该电脑未进行清屏操作，电脑桌面上存放各类工作文件，包括有《月平均工资、公积金》、《秘密载体基本情况》等敏感的工作文件；

经查，公司制定《内部非涉密计算机管理办法》规定了开机口令和屏保要求，该员工对信息安全意识不足，对该电脑口令设置过于简单，不符合规定要求，且未按照信息安全管理体系要求对使用后电脑桌面上的敏感文件进行清屏。

三、 标准解读及问题分析

1） GB-T22080-2008 A.8.3.3 条款要求“所有雇员、承包方人员和第三方人员对信息和信息处理设施的访问权应在任用、合同或协议终止时删除，或在变化时调整”；

对信息资产和信息处理设施的访问权限在任用终止或变更前是否减少或删除，依赖于对风险因素的评价；

该公司涉及各类发票、收据产品的印刷，对印刷车间和仓库等区域均为重要安全区域，未经授权人员不得进入，因此对门禁权限的管理尤为关键，公司针对门禁制定了《门禁系统管理制度》，所有门禁权限的开通均需经总经理批准后由综合管理部进行分配；但是

在实际工作中系统管理员只关注了对新入职员工和调岗员工的门禁权限管理，忽略了对离职人员权限的删除，也未能定期对门禁系统中的权限分配情况进行复查；另外该员工的信息安全意识较为薄弱，对标准条款中要求理解不充分，未能按照 A.8.3.3 条款的要求在员工任用终止时撤销访问权限。

2）GB-T22080-2008 A.9.2 条款要求“应安置和保护设备，以减少由环境威胁和危险所造成的各种风险”，“应保护设备使其免于由支持性设施失效而引起的电源故障和其他中断”；

根据标准要求要采取控制措施以最小化潜在物理威胁的风险如：火灾、尘埃、电源干扰等；并对可能对信息处理设施运行状态产生负面影响的环境条件予以监视；另需要有足够的支持性设施来支持系统，保持连续性；

公司由于主要从事票据印刷，日常工作中对网络信息化要求相对较低，因此网管对存放电话交换机和网络设备的小机房的管理不够重视，且网管对标准 A.9.2 条款中的相关要求认识不足，对机房缺少规划和管理，导致机房环境杂乱，配备的空调未使用，且缺少温湿度监控、灭火器等支持性设施，无法对机房内的物理环境和设备安全进行有效的管控。

3）GB-T22080-2008 A.11.3 条款要求“应要求用户在选择及使用口令时，遵循良好的安全习惯”，“应采取清空桌面上文件和清空信

息处理设施屏幕的策略”；根据标准要求应避免连续相同的、全数字的或全字母的字符，并定期变更口令；同时对于敏感或涉密的文件在使用后应立即从电脑桌面或打印机中清除，以降低正常工作时间之中和之外对信息的未授权访问；

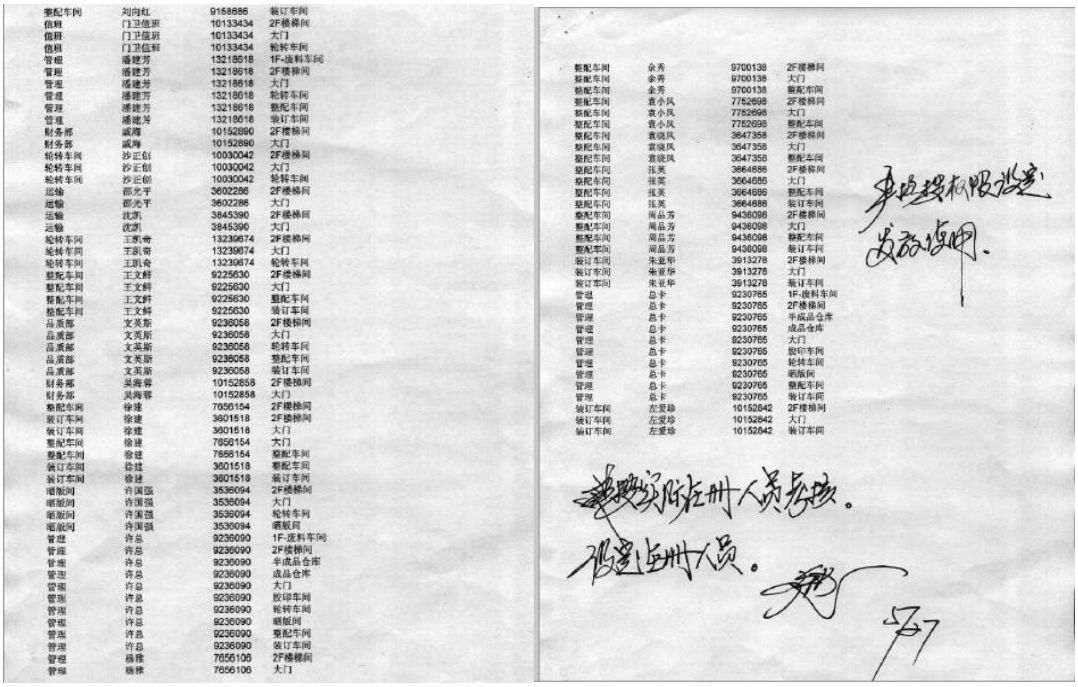
公司制定了《内部非涉密计算机管理办法》，对开机口令强度和屏保要求进行了明确，但受审核人员信息安全意识不强，为了使用方便，开机口令设置过于简单，且在电脑桌面上放置有非公开的敏感工作文件，未能对所管理的信息资产进行有效的管理和防护，也不符合标准条款和公司管理规定的要求。

四、 改进过程及取得的成效

基于以上事实和沟通，受审核组织领导对我们发现的问题欣然接受，并表示此次审核人员指出的问题工作中没有关注到，但却存在很大的安全隐患和风险,一定认真整改。现场审核后，受审核组织对提出的不符合项均进行原因分析并制定了纠正措施，并举一反三，排查所有信息处理设施，取得了良好的管理成效。

1）对于 A.8.3.3 条款提出的不符合采取的纠正措施包括：立即门禁系统中离职人员的权限进行撤销，并对全体员工的门禁权限进行复查，将现有人员的门禁权限上报总经理审批后，编制《门禁权限一栏表》，明确各道门禁授权的人员；后续要求系统管理员建立管理日志，定期对门禁系统及人员信息进行检查，确保全公司各道门禁监控的正常运行；组织员工学习公司《门禁系统管理制度》和 GB-T22080-2008

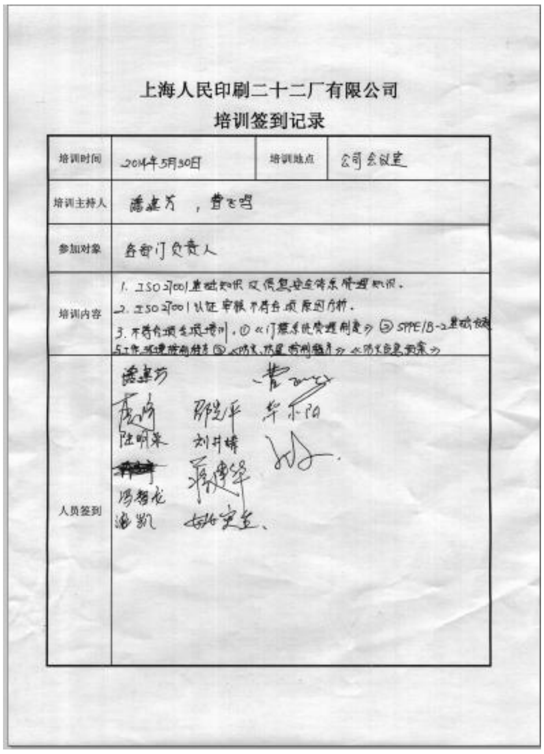
A.8.3.3 条款要求件，增强员工的信息安全意识。



整配车间	刘向红	9158686	装订车间
值班	门卫值班	10133434	2F楼梯间
值班	门卫值班	10133434	大门
值班	门卫值班	10133434	轮转车间
管理	潘建芳	13218618	1F-废料车间
管理	潘建芳	13218618	2F楼梯间
管理	潘建芳	13218618	大门
管理	潘建芳	13218618	轮转车间
管理	潘建芳	13218618	整配车间
管理	潘建芳	13218618	装订车间
财务部	臧海	10152890	2F楼梯间
财务部	臧海	10152890	大门
轮转车间	沙正创	10030042	2F楼梯间
轮转车间	沙正创	10030042	大门
轮转车间	沙正创	10030042	轮转车间
运输	邵光平	3602286	2F楼梯间
运输	邵光平	3602286	大门
运输	沈凯	3845390	2F楼梯间
运输	沈凯	3845390	大门
轮转车间	王凯奇	13239674	2F楼梯间
轮转车间	王凯奇	13239674	大门
轮转车间	王凯奇	13239674	轮转车间
整配车间	王文鲜	9225630	2F楼梯间
整配车间	王文鲜	9225630	大门
整配车间	王文鲜	9225630	整配车间
整配车间	王文鲜	9225630	装订车间
品质部	文英斯	9236058	2F楼梯间
品质部	文英斯	9236058	大门
品质部	文英斯	9236058	轮转车间
品质部	文英斯	9236058	整配车间
品质部	文英斯	9236058	装订车间
财务部	吴海蓉	10152858	2F楼梯间
财务部	吴海蓉	10152858	大门
整配车间	徐建	7656154	2F楼梯间
装订车间	徐建	3601518	2F楼梯间
装订车间	徐建	3601518	大门
整配车间	徐建	7656154	大门
整配车间	徐建	7656154	整配车间
装订车间	徐建	3601518	整配车间
装订车间	徐建	3601518	装订车间
晒版间	许国强	3536094	2F楼梯间
晒版间	许国强	3536094	大门
晒版间	许国强	3536094	轮转车间
晒版间	许国强	3536094	晒版间
管理	许总	9236090	1F-废料车间
管理	许总	9236090	2F楼梯间
管理	许总	9236090	半成品仓库
管理	许总	9236090	成品仓库
管理	许总	9236090	大门
管理	许总	9236090	胶印车间
管理	许总	9236090	轮转车间
管理	许总	9236090	晒版间
管理	许总	9236090	整配车间
管理	许总	9236090	装订车间
管理	杨雅	7656106	2F楼梯间
管理	杨雅	7656106	大门

整配车间	余秀	9700138	2F楼梯间
整配车间	余秀	9700138	大门
整配车间	余秀	9700138	整配车间
整配车间	袁小凤	7752698	2F楼梯间
整配车间	袁小凤	7752698	大门
整配车间	袁小凤	7752698	整配车间
整配车间	袁晓凤	3647358	2F楼梯间
整配车间	袁晓凤	3647358	大门
整配车间	袁晓凤	3647358	整配车间
整配车间	张英	3664686	2F楼梯间
整配车间	张英	3664686	大门
整配车间	张英	3664686	整配车间
整配车间	张英	3664686	装订车间
整配车间	周品芳	9436098	2F楼梯间
整配车间	周品芳	9436098	大门
整配车间	周品芳	9436098	整配车间
整配车间	周品芳	9436098	装订车间
装订车间	朱亚华	3913278	2F楼梯间
装订车间	朱亚华	3913278	大门
装订车间	朱亚华	3913278	装订车间
管理	总卡	9230765	1F-废料车间
管理	总卡	9230765	2F楼梯间
管理	总卡	9230765	半成品仓库
管理	总卡	9230765	成品仓库
管理	总卡	9230765	大门
管理	总卡	9230765	胶印车间
管理	总卡	9230765	轮转车间
管理	总卡	9230765	晒版间
管理	总卡	9230765	整配车间
管理	总卡	9230765	装订车间
装订车间	左爱珍	10152842	2F楼梯间
装订车间	左爱珍	10152842	大门
装订车间	左爱珍	10152842	装订车间

2） 对于 A.9.2 条款提出的不符合采取的纠正措施包括：立即对机房进行打扫整理，检查网络设备的布线，开启空调使机房内温度处于恒温状态，并购置灭火器，后续要求网管定期对机房进行巡检，保留记录，确保机房物理环境适宜，设备运行处于正常状态；并对员工进行标准和体系文件的培训，增强其信息安全意识；



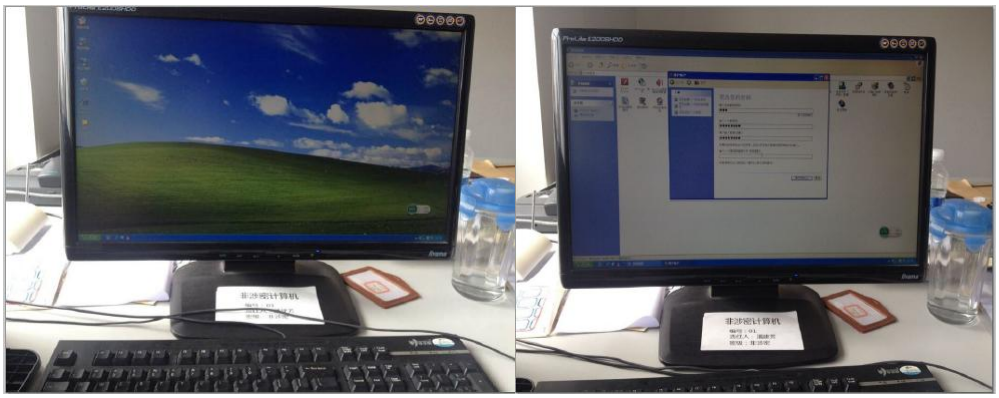
上海人民印刷二十二厂有限公司

培训签到记录

培训时间	2014年5月30日	培训地点	公司会议室
培训主持人	潘建芳，曹飞鸣		
参加对象	各部门负责人		
培训内容	1. ISO27001基础知识及信息安全体系管理知识。 2. ISO27001认证审核不符合项原因分析。 3. 不符合项专项培训。①《门禁系统管理制度》②SPPE/B-2基础设施与工作环境控制程序 ③《防火、防盗控制程序》《防火应急预案》		
人员签到	潘建芳 [illegible] [illegible] 邵晓平 华东阳 陆明荣 刘丹婧 [illegible] [illegible] 冯智龙 潘凯 [illegible]		

3）对于 A.11.3 条款提出的不符合采取的纠正措施包括：立即对办公电脑桌面进行清屏，不存放敏感文件；按照《内部非涉密计算机管理办法》，要求重新设置开机口令，长度至少 6 位，且有数字、字母相结合，并规定每半年对口令进行变更；举一反三，检查公司内其他工作电脑的口令设置情况和清屏策略执行情况，严格按照标准和管理制度的要求执行；

组织员工学习公司《内部非涉密计算机管理办法》和 GB-T22080-2008 A.11.3 条款要求件，增强员工的信息安全意识



取得成效：

通过此次审核，受审核方领导和员工充分意识之前虽然已进行了信息安全管理体系的贯标，但是在日常工作中对标准要求的理解实施还有所欠缺，员工更多的关心本职工作及业务上的事，忽略了信息安全的要求，员工总体信息安全意识较为薄弱，利用对审核中提出不符合整改的机会重新对公司的体系文件进行了培训学习，加强全员的信息安全意识；

同时**通过审核，受审核方对信息安全标准中的要求有了更深入的认识，也发现了在日常工作过程中实际存在的信息安全隐患和信息安全管理漏洞，经过与企业领导层以及各部门人员沟通交流后，企业认可了认真执行标准中规定的控制措施对公司的信息安全管理带来帮助，并表示今后会对信息安全更加重视，结合实际工作加强培训教育，做到持续改进，不断提升信息安全体系的实施效果和公司信息安全的管理水平。**