2020年技术服务部信息安全学习材料

2020.06

导言

信息安全对公司与部门运作意义重大，对所有信息资产进行恰当地安全保护，是保障公司与部门的核心竞争力的重要环节。

近期TS发现多起信息安全违规案例，为部门业务信息安全带来较大风险。通过本次学习，希望TS每位员工了解信息安全对于整个公司及每个人的重要性，熟悉公司信息安全的规章制度，正确识别信息安全风险，提高信息安全意识，掌握基本的信息安全知识和技能。

信息安全原则

（1）信息安全工作由高层牵头，领导负责，全员参与，专人管理。

（2）对保密信息的访问应遵循**工作相关性原则、最小授权原则和审批、受控原则**。

（3）**公司IT资源要求用于工作目的**，公司有权利对IT资源的使用进行审计和监控。

信息安全管理制度——主机安全（1）

1、员工在使用自己所属的计算机时，应该设置开机、屏幕保护口令；
屏幕保护程序启动等待时间为10分钟，并且屏幕保护程序必须为操作系统自带的或经公司批准使用；
对于便携机，建议设置硬盘口令；
在设置目录共享时，设置共享口令。

信息安全管理制度——主机安全（2）

2、在办公区域无人的时候，便携机及其它移动计算设备、存储设备应该存放在保密柜等安全的地方。

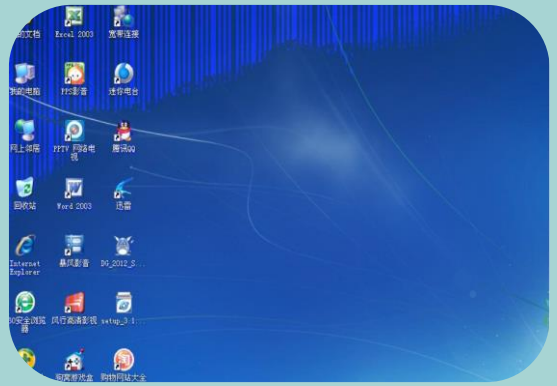
信息安全管理制度——主机安全（3）

3、未经许可不得使用USB盘等移动存储设备拷贝公司保密信息。

信息安全管理制度——主机安全（4）

4、严格禁止使用私人电脑接入公司网络进行办公。

信息安全管理制度——软件安全（1）



1、未经批准，员工机器上不得安装非标准软件。

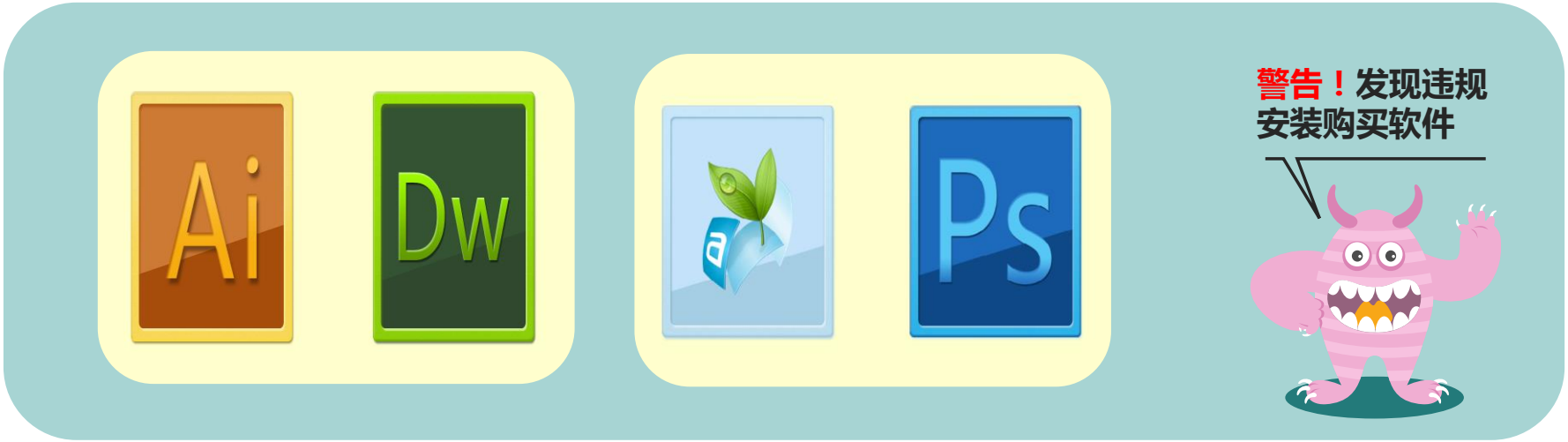
信息安全管理制度——软件安全（2）

2、员工必须安装、运行公司标准规定的防病毒软件并及时升级。

信息安全管理制度——软件安全（3）

3、严禁安装和运行黑客、系统破解或口令破解等软件。

信息安全管理制度——软件安全（4）



4、员工不得在公司配置的计算机上安装自己购买的软件。

信息安全管理制度——口令设置标准

1、如果技术上支持，口令至少要有6位长

2、口令必须是字母和非字母的组合

3、与前次口令比较，在任何位置不能有超过3个字符连续相同

4、口令中同一个符号出现不得大于2次

5、用户名不能作为口令一部分

6、与前4次相同的口令不能重复使用

7、重要系统的普通用户口令要求8位以上

8、帐号的使用人应当定期修改帐号口令，普通帐号应当小于6个月

9、员工之间不应私下互相转让、借用公司IT资源的帐号，如域账号、ERP帐户等

信息安全管理制度——邮箱使用管理规定

1、办公桌面客户端：使用Outlook邮件客户端，不支持其他第三方邮件客户端。

2、移动端设备：TS员工使用移动邮箱（Pushmail）服务。**若开通移动邮箱的移动设备遗失，需24小时内通过mail.h3c.com自助方式或联系IT热线协助进行内容擦除。**

3、业务或IT系统：使用邮件服务前必须通过身份验证环节，不支持匿名使用邮件服务。

4、未经批准，禁止自发自收邮件（主要指同一个人）。

5、开通移动邮箱的移动终端设备必须接受服务器端的安全策略，包括设置开机密码等。

6、不能以任何方式泄露通过邮件接收到的公司保密信息。

信息安全管理制度——网络使用安全

1、个人计算机的IP地址必须设置为自动获取方式，员工不应擅自配置固定IP地址。

2、如果员工工作需要使用固定IP地址，须向当地网络管理员或指定授权人申请，按照管理员指定的IP地址设置，以避免擅自设置的IP地址与其它员工计算机的IP地址或服务器的IP地址冲突。

3、员工的计算机网络设置必须符合公司制定的标准，严禁隐含和伪造上网终端基本信息；例如IP地址，MAC地址，用户名等信息。

4、严禁私自设立WWW、FTP、BBS、NEWS、DNS、DHCP等应用服务。

5、未经批准，严禁搭建网关型私有网络/虚机私有网络(私有网关自己分配IP地址，不受公司网络安全接入策略控制)，并将私有网络经NAT地址转换后接入公司办公网络。

6、未经批准，禁止将设备间私有网络直接接入公司内部网络。

7、需求人/责任人对申请的私有网络的安全防护负全部责任，包括不限于私有网络内部的防病毒软件安装、补丁安装/修复、数据保护等管理责任。

信息安全管理制度——保密信息管理要求

保密信息：保密信息是指对公司具有重要价值或敏感的信息，不能公开发布，需要进行恰当的保护，如果泄露，可能会给公司造成损失和不良影响。

保密信息包括但不限于:商业秘密包括技术秘密和经营秘密。

技术秘密包括但不限于工作进度、技术方案、工程设计、电路设计、制造方法、配方、工艺流程、技术指标、计算机软件、数据库、研究开发记录、技术报告、测试报告、检测报告、实验数据、试验结果、图纸、样品、样机、模型、模具、操作手册、技术文档、相关的函电等。

经营秘密包括但不限于客户名单、行销计划、采购资料、定价政策、财务资料、进货渠道、法律事务信息、人力资源信息等等。

信息安全管理制度——保密信息管理要求

保密信息根据其价值、内容的敏感程度、影响及发放范围不同，划分为绝密、机密、秘密、内参等四个级别。

信息的授权和使用必须经过信息所有人的批准，经过正常授权获得保密信息的人无权将所获得的保密信息再授权，也不得提供给第三人，禁止员工私下交流保密信息。

密级	内容	信息所有人
绝密	指包含公司最重要和最敏感的信息，关系公司未来发展的前途命运，对公司根本利益有着决定性影响的信息	信息所属部门一级及以上主管
机密	指包含公司的重要秘密，其泄露会使公司的安全和利益遭受严重损害的保密信息	信息所属部门二级及以上主管
秘密	指包含公司一般性信息，其泄露会使公司的安全和利益受到损害的保密信息	信息所属部门三级及以上主管
内参	指仅在公司内部或在公司某一部门内部公开，向外扩散有可能对公司的利益造成损害的保密信息信息所有人指对所管理业务领域内信息的创建、使用、维护和销毁等行使授权和管理职责的业务部门主管	信息所属部门三级及以上主管

信息安全管理制度——信息安全奖惩制度

级别	奖励
三级	重视信息安全工作，发现并举报安全管理或业务流程中存在的信息安全漏洞，并提供解决方案的人员给予现金奖励，并通报表扬。
二级	对于举报一般违规行为的人员，给予现金奖励并记入关键事件库 。
一级	对于举报泄密、窃密或其他严重损害公司利益事件的人员（恶劣违纪行为），根据具体情况给予现金奖励。并记入关键事件库。

信息安全管理制度——信息安全奖惩制度

H3C 数字化解决方案领导者

级别	违纪情节	处罚	考评
五级	违反信息安全制度，情节轻微，性质不严重的行为，没有造成公司经济损失，或尚未产生不良影响的违法违纪行为，但因故意或因工作严重疏忽造成公司较轻经济损失在壹(1)仟元或以下，或没有造成经济损失的行为	口头教育	当季考核不高于B
四级	违反信息安全制度，造成公司较轻经济损失在壹(1)仟元或以下，或产生较轻影响的违法违纪行为，或虽不直接违反信息安全制度但因故意或因工作严重疏忽造成公司一般经济损失在壹(1)仟元到伍(5)仟元（含伍仟元）人民币之间的行为	口头警告	当季考核C或D
三级	违反信息安全制度，情节、性质较为严重的行为，或造成公司一般经济损失，在壹(1)仟元到伍(5)仟元(含伍仟元)人民币之间，或造成较为严重影响的违法违纪行为，或虽不直接违反信息安全制度，但因故意或因工作严重疏忽造成公司较重经济损失在伍(5)仟元到壹（1）万元(不含壹万元)人民币之间的行为	书面警告	当季考评C或D，建议年度考评不高于B；至少6个月不得升职级，可视情况降职级；6个月之内不得任命，可视情况免职、降职
二级	违反信息安全制度，情节严重、性质较为恶劣的行为，造成或可能造成公司较重经济损失在伍(5)仟元到壹（1）万元(不含壹万元)人民币之间，或造成较为恶劣影响的违法违纪行为，或虽不直接违反信息安全制度，但因故意或因工作严重疏忽造成公司重大经济损失,在壹（1）万元人民币或以上的行为	最终书面警告	当季考评D，建议年度考评C或D；至少12个月不得升职级，可视情况降职级；12个月之内不得任命，可视情况免职、降职
一级	违反信息安全制度，情节非常严重、性质恶劣的行为，造成或可能造成公司重大经济损失在壹(1)万元人民币及以上，或造成恶劣影响的违法违纪行为	解除劳动合同或立即解除劳动合同	

信息安全管理制度——信息安全受理渠道

H3C
数字化解决方案领导者

IT热线

电话：400-818-2222
0571-86760818
Email: ithotline@h3c.com
IT 自助平台：ithelp.h3c.com

电子流

如您发现相关隐患或有相关建议意见，请提交电子流反馈：BPM——信息安全问题受理电子流

日常咨询

日常工作中遇到的信息安全问题可咨询部门信息安全员赵家煊16468

信息安全发文

公司信息安全发文归档查询路径：

（1）bpm平台--公司文件夹--信息技术部文件夹

（2）新华三信息门户--信息安全门户– 信息安全管理规定。

违规案例及处罚结果

违规案例一

➢ **案例一**

IT例行抽查中发现，员工刘某擅自使用USB端口拷贝了大量与工作有关的文档，涉嫌信息安全违规。经核实，员工刘某无正当工作需要擅自拷贝部分个人曾负责项目文档，内容属于保密信息的技术秘密，此行为构成信息安全违规。

➢ **处罚结果**

给予刘某四级违规 ，口头警告并部门内通报批评的处罚。

➢ **请思考：刘某的行为违反了哪些信息安全规定？**

违规案例二

➢ **案例二**

部分员工未经授权审批擅自下载并使用卓威公司Navicat 软件，导致我司法务部接到卓威公司法务来函，为我司带来侵权隐患。随后的 IT抽查中发现，部分员工多次被扫描到该软件使用记录。经核实，部分员工半年内多次在被明确要求卸载并用其他开源免费软件替代后重新安装该软件，此行为构成信息安全违规。

➢ **处罚结果**

给予相关员工五级违规，口头教育，部门内通报批评的处罚。

➢ **请思考：周某的行为违反了哪些信息安全规定？**

违规案例三

➢ **案例三**

信息安全部通过网络安全态势感知系统发现，技术服务部某公网实验室一台服务器遭到外部攻击、控制，同时被植入恶意程序，该恶意程序以服务器为跳板，攻击内网机器。经核实，该服务器使用人员违反网络安全管理规定，使用弱密码，导致被外部攻击、控制，同时私自将该外网服务器连接到公司内网，为威胁向内网扩散提供了通道。此行为构成信息安全违规。

➢ **处罚结果**

给予管理员云某四级违规，公司内通报批评的处罚。同时责令技术服务部公网实验室制定整改方案，消除安全隐患。

➢ **请思考：云某的行为违反了哪些信息安全规定？**

违规案例四

➢ **案例四**

IT例行抽查中发现，员工刘某擅自使用USB端口拷贝了大量与工作有关的文档，涉嫌信息安全违规。经核实，员工刘某因离职在即，拷贝曾负责的项目文档，此内容属于经营秘密，此行为构成信息安全违规。

➢ **处罚结果**

给予刘某三级违规，书面警告并部门内通报批评处罚。

➢ **请思考：刘某的行为违反了哪些信息安全规定？**

信息安全常见Q&A

常见Q&A

Q1、日常工作中，如果有不能通过邮件发送，必须使用U盘的情况，怎么办？

A：此类因工作需要必须使用U盘的情况需要提前报备，经部门主管审批并反馈信息安全员后，视为此类行为合规；同时使用者仍需保证在文档传输中不会发生泄漏及超范围传播的情况，如有内容泄漏仍视为违规，按照公司规定进行处罚。

Q2、第一种情况报备后，每次使用前还需要审批么？

A：不需要。只要此种业务场景已经过审批与记录，符合报备的条件，不需要员工每次使用前都审批，只要员工确保符合报备内容即可。

Q3、如果有的非标准软件是项目需要，不安装无法正常工作，怎么办？

A：此类因工作需要必须安装的非标准软件安装需要提前报备，经部门主管审批并反馈信息安全员后，视为此类行为合规。

Q4、如果想对电脑里的文档进行备份以防电脑故障导致数据丢失，怎么办？

A：各二级部门或三级部门可以根据部门需要申请服务器，用于员工数据备份。
服务器申请路径：BPM——IT需求电子流

Q5、公司标准软件清单是什么？

A：请见《新华三集团信字【2019】018号【内参】-办公桌面平台标准V7.0》
http://home03.h3c.com/dominobs/ITFile.nsf/docs/7A01DC0C00D31C48482583E0000A148A?OpenDocument。

Q6、公司标准软件安装包在哪里找到？

A：公司标准软件下载地址如下，
北京服务器地址：\\h3c-bjfs\Software\Application
杭州服务器地址：\\h3c-hzfs\Software\Application

Thanks！

新华三集团
www.h3c.com