Q/XTY

福建新坦洋集团股份有限公司企业标准

Q/XTY BZ 205.4—2020

网络管理规范

2020－02－10 发布　　2020－02－10 实施

福建新坦洋集团股份有限公司　　发 布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由福建新坦洋集团股份有限公司提出并归口。

本标准起草单位：福建新坦洋集团股份有限公司。

本标准主要起草人:林嘉青、缪瑶 。

网络管理规范

1 范围

本标准规定了网络日常管理与维护、安全与应急。

本标准适用于公司网络管理事宜。

2 日常管理与维护

2.1 检查与记录

2.1.1 网络管理员应及时查阅相关的系统记录，定期检查，保证重要网络系统的安全配置应达到中华人民共和国国家标准《计算机信息系统安全保护等级划分准则》（GB 17859-1999）中规定的第二级－系统审计保护级以上，保障网络的正常运行，发现问题，提出相应的解决方案，及时解决。

2.1.2 网络维护人员应对操作系统和数据库管理系统中进行系统运行记录（Log）和数据库运行记录（Data Base Log）的转储保存以备查。重要大型数据库应运行于专门的服务器或工作站上，并异地备份。

2.1.3 网络维护人员应注意在设备维护过程中的注意事项，注意人身安全，保证网络设备的物理安全并尽可能的保证网络设备正常工作。对在维护、巡查过程中发现的问题，应及时形成相应的网络维护记录并汇报。

2.2 安全设置

2.2.1 网络维护人员应尽可能地改善网络系统的安全策略设置，尽量减少安全漏洞。

2.2.2 关闭不使用的服务，对不同级别的网络用户设置相应的资源访问权限。

2.3 数据与更新

2.3.1 工作人员、电子证照等数据内容库应根据人员实际变动情况及时更新。

2.3.2 网络维护人员及时了解最新的安全资讯，针对具体情况采取预防病毒技术、检测病毒技术和杀毒技术。

2.4 评价与改进

2.4.1 网络维护人员应当用网络安全检测工具对网络系统进行安全性分析，及时发现并修正存在的安全漏洞，并应编写检测报告，需详细记叙检测的对象、手段、结果、已实施的补救措施与安全策略和进一步提升网络安全的建议。

2.4.2 网络管理员应及时阅读检测报告，掌握当前网络安全中存在的问题，对提出的建议做出响应，并将检测报告存入系统档案。

3 安全与应急

3.1 内网建设统一的身份认证系统，用户密钥由行政部网络管理人员统一管理。

3.2　内网用户的访问操作权限（如授权、读、写、删除、复制、打印等）应严格加以控制。公用平台不得设置超级系统管理员，用户管理与具体业务应用的访问权限分开设置。各业务应用的访问权限由各业务部门确定，在系统正式运行期间，系统管理员不得私设用户。

3.3　内网与因特网完全物理隔离，内网计算机不得采用电话拨号、交替插拨、双网卡等任何方式接入因特网；不得修改或删除计算机的网络配置；不得私自安装网络设备；严禁笔记本电脑接入内网。

3.4　内网服务器及核心网络设备设专用区域，未经批准，无关人员不得进入。

3.5　建立应急处理和灾难恢复机制。重要的数据建立应急支援中心和数据灾难备份中心，实行异地备份。

3.6　应定期进行安全检查，对检查中发现的问题进行通报，并责令改正。