ZWLINK 展旺				文件编号：ZW-RBA-OP-075	
				制定日期：2025-03-05	
文件类型	程 序 文 件	制定部门	品质部	版　　次：　　A0	
文件名称	网络信息安全管理程序			页　　次：　第 1 页/共 3 页	

文件履历表

版本	修订内容描述	修订日期	制定人	审核人	批准人
A0	首次发行	2025-03-05	李勤	张楠	刘仁

制定人/日期	审　核/日期	批　准/日期
李勤/2025-03-05		刘仁

文件发行章
展旺公司 2025.03.05 文件受控

1 目的

为确保网络安全，依据安全策略，加强与信息相关网络设备的配置管理和网络服务的安全管理，特制定本程序。

2 范围

本程序适用于在组织内使用的所有主要网络设备的安全参数设置管理和网络服务管理，包括：

1) 防火墙设备及软硬件；
2) 网关设备及软硬件；
3) 网络交换机及 HUB 等。
4) 网络服务的安全

3 职责

3.1 技术中心

负责对组织内所有主要网络设备的配置参数设定和网络服务安全控制。

4 相关文件

《信息安全和信息技术服务管理手册》
《信息系统访问与使用监控控制程序》

5 程序

5.1 网络设备安全配置策略

5.1.1 通用策略

网络设备的配置必须由技术中心 IT 专职人员实施。
设备系统日志的记录内容和保存期限应该符合《信息系统访问与使用监控控制程序》。

5.1.2 防火墙安全配置策略

对外连接防火墙配置要求：

1) 除内部向外部提供的服务外，其他任何从外部向内部发起的连接请求被禁止；
2) 除内部向外部提供的服务相关部分外，内部向外部的访问需经技术中心经理批准。

内部防火墙配置要求：

1) 内部防火墙的内外部分分为不同的安全等级，外部为等级低的部分，内部为等级高的部分；
2) 除内部向外部提供的服务外，其他任何从外部向内部发起的连接请求被禁止；
3) 除内部向外部提供的服务相关部分外，内部向外部的访问需经技术中心经理批准。

5.1.3 网关设备安全配置策略

VPN 网关设备安全配置策略：

1) 访问许可列表应根据申请并经过审批获得；
2) 对许可的访问发起者的身份认证应至少在两项或以上；
3) 非许可访问的部分应禁止；
4) 许可的访问发起者应体现相对静态的信息记录，如有明确意义的用户名、静态访问 IP 地址等；
5) 许可的访问发起者的访问权利应不被滥用。

5.1.4 网络交换机设备安全配置策略

关键路径网络交换机安全配置策略

1） 关键路径网络交换机是指位于公司网络中间节点或信息交换中心位置的网络交换机；
2） 关键路径网络交换机安全配置策略应考虑和周边网络设备的连接的兼容性、安全性、可靠性和可变性；
3） 关键路径网络交换机安全配置策略应尽量减少不必要的限定以保证合理的通信能力。

周边网络交换机安全配置策略

1） 周边网络交换机是指位于公司网络非中间节点或信息交换相对不重要的位置的网络交换机；
2） 周边网络交换机安全配置策略应考虑和关键路径网络设备的连接的兼容性、安全性、可靠性和可变性；
3） 关键路径网络交换机安全配置策略应根据需要减少不必要信息向更高级的网络层的传输。

5.2 网络中间设备配置过程

技术中心 IT 专职人员根据安全配置策略和特定安全要求填写《网络设备安全配置表》，经信息安全管理小组组长审核批准后，由技术中心 IT 专职人员对网络设备参数进行配置。配置实施后必须进行检查，测试，填写《验收报告》，并在《网络设备安全配置表》签署姓名和日期。

5.3 网络服务的安全控制

1）网络中的隔离

在网络中隔离信息服务、用户和信息系统，由技术中心负责。域之间的隔离可以使用不同的物理网络或逻辑网络。域的选择可以基于信任级别、所属的组织单元或某些组合。明确界定每个域的边界，边界处使用网关进行控制。无线网络边界难以界定，把无线访问是为外部链接，从内部网络隔离。

2）网络服务的安全

网络服务，包括接入服务、私有网络服务、电子商城等，必须确认安全机制、服务级别和管理要求，包括在网络服务协议中。定期监视网络服务提供商的服务水平，安全特征和控制措施。安全特征可以是：鉴别、加密、网络连接控制等。技术中心负责网络服务的安全。

6 记录

《网络设备安全配置表》
《验收报告》