科道芯国 KEYDOM 四川科道芯国智能技术股份有限公司

逻辑安全检查记录单
Logic Security Check List

检查人： Checker:		陪同人： Escorted by:		检查完成日期： Date of end of the Audit:	
评审人： Reviewer:				审核类型： Audit Type:	周检查 Weekly inspection

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
IT系统/终端 IT System/ Terminal				
服务器、终端是否锁定或注销 Servers and terminals logging out.	终端的屏幕保护策略应设置为3分钟；同时确保人员离开时要进行手动锁屏。抽样数：8 Choose terminals to check if the screen saver policy is set as 3 minute, at the same time to check if employee logged out manually when they were leaving. Sample number: 8			
病毒防护功能和病毒库版本 Anti-virus and virus base version	终端上的病毒防护功能是正确开启，病毒库文件版本更新至一周以内。抽样数：8 Choose terminals to check if the anti-virus function is enabled appropriately and if the virus base is updated to the latest version within 1 week. Sample number: 8			
定期全盘扫描 Regularly running full system scan	确保病毒防护软件扫描策略包含“升级后全盘扫描”，通过检查终端日志，确认策略得到执行 抽样数：8 Check that if the scanning policy of the antivirus software includes “Full scan after update”. Check terminal logs to confirm that the policy has been enforced. Sampling number：8			
IT系统/存储 IT System/Storage				
可移动存储接口功能禁用 Removable storage port disabling	检查USB接口，确保可移动存储设备不被识别； 采取物理方式禁用的，应确保物理禁用措施是完整的，没有破损 抽样数：8 Check the USB ports to ensure the removable storage equipment couldn’t be identified. Physical protection actions are integrate. Sampling number:8			
IT系统/系统账户控制与审计 IT System/System Account Control and Audit				

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)

账户创建、删除与变更
Account creation, deletion and change
	1、确保账户的创建、删除与变更拥有正确的流程;
	2、操作是由授权的系统管理员执行的;
	1. Check that if all the account creation, deletion and change are with required documentation.
	2. Check that if the account creation, deletion and change are conducted by authorized system administrator.			

检查账户登录失败 Failed log-in event	确认因登录失败被锁定的账户是账户持有人操作的，并对频度较高的员工组织培训计划 抽样数：8 Investigate the failed log-in event to confirm if the locked account is logged by the account holder. Sampling number:8			
审计策略的配置 Audit policy configuration	确保审核策略的配置与要求的一致，包括域控GPO及本地: 审核帐户登录事件 (成功,失败) 审核帐户管理 (成功,失败) 审核目录服务访问 (无审核) 审核登录事件 (成功,失败) 审核对象访问 (失败) 审核策略更改 (失败) 审核特权使用 (失败) 审核过程追踪 (无审核) 审核系统事件 (成功,失败) Check that if the audit policy configuration is compliance with requirement, including domain control GPO and local: Account log-in event, account mgt., directory service access, log-in event, policy change, privilege using, process tracking and system event.			
账户锁定策略配置 Account lockout policy configuration	确保账户锁定策略与要求一致，包括域控GPO及本地: 账户锁定时间　　0分钟 账户锁定阀值　　6次 重置账户锁定计数器 99999分钟 Check that if the account lockout policy is compliance with requirement, including the domain GPO and local. Account lockout duration:0 minutes Account lockout threshold: after 6 invalid logon attempts			

控制要求 Control	方法和要求 How and References	日期和时间 Date and Time	结果 Result	备注（抽样样品ID） Comments (IDs of Samples being Checked)
IT系统/监控 IT System/Monitor				
IDS/IPS设备的日志 IDS/IPS logs	1、IDS/IPS设备的日志应被审计, 2、IDS/IPS设备配置应有备份 3、检查系统日志是否有被篡改 1. Check that if the IDS could generate 2. IDS/IPS device configuration should be backed up 3. Check that if the system log has been tempered.			
IT系统/防火墙 IT System/Firewall				
防火墙的物理控制 Physical Control of firewall	现场检查防火墙的物理环境: 1、全部的防火墙都应被锁在机柜中 2、机柜、防火墙没有明显的破坏痕迹 3、防火墙接口上没有可疑的连接 Check the physical environment of the firewall: 1 If all the firewalls are locked in the cabinet 2 If there is any oblivious sign of destroy 3 If there is any suspicious contact to firewall port			
IT系统/日志审计 IT System/Log Audit				
使用日志软件系统进行日志分析，包括防火墙日志、数据处理日志、操作系统日志 Logs analysis according to log software system, including firewall logs, data processing logs, and operation system logs.	定期登录日志系统，对系统收集的日志进行分析, Check the log system regularly, record referring to Production Log Checklist.			