哈尔滨工程大学信息化处文件

信息化处发〔2022〕 18 号

关于印发《IDC 运行支撑软硬件巡检规范汇编》的通知

各办公室：

《IDC 运行支撑软硬件巡检规范汇编》经 2022 年第 14 次处长办公会讨论通过，现印发给你们，请认真贯彻执行。

哈尔滨工程大学信息化处

2022 年 6 月 8 日

IDC 运行支撑软硬件巡检规范汇编

为保障 IDC 运行支撑软硬件安全和稳定的运行，提高巡检工作的规范化管理，特制定相应规范。本规范汇编适用于支撑学校信息系统、网站运行的 IDC 服务器、存储、网络等各类软硬件的日常巡检工作，具体如下：

1.《IDC 机房岛内巡检规范》；

2.《服务器设备巡检规范》；

3.《存储设备巡检规范》；

4.《IDC 网络巡检规范》；

5.《虚拟化平台巡检规范》；

6.《数据备份设备巡检规范》；

7.《DNS 系统巡检规范》；

8.《负载均衡设备巡检规范》；

9.《反向代理系统巡检规范》；

10.《VPN 系统巡检规范》；

11.《网闸设备巡检规范》。

以上规范由信息化处信息系统管理办公室负责解释，自发布之日起施行，原有相关规范自行废止。规范内容根据软硬件建设部署情况，实施动态调整更新。

IDC 机房岛内巡检规范

为了加强 IDC 机房岛内设备管理，保障各项设备运行的安全和稳定，特制定本规定，本规定适用于 IDC 机房岛内巡检管理。

对 IDC 机房岛内实行巡检制度，每天对机房岛内设备进行三次常规巡检，检查服务器、存储及网络等设备运行状态和机房岛内环境状况。岛内设备巡检负责人:A 角-王建、B 角-刘金路。

第一条 巡检时间: IDC 机房岛内巡检具体时间是在每天上午 8:30、中午 11:00、下午 17:00 进行。

第二条 巡检内容: 机房岛内服务器、存储、网络等设备工作状态。

第三条 巡检流程:

1.检查岛内服务器、存储、网络等设备的通电状态，电源指示灯、运行状态指示灯是否正常，有无异常警告;

2.检查机房岛内温度是否过高，湿度是否正常;

3.检查机房岛内是否堆放其它无关物品;

4.下班前还应检查机房岛内机柜等是否锁好;

5.填写放置在 IDC 机房的《IDC 机房巡检记录表》。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度，不得擅自泄露机房岛内设备相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.机房岛内设备由专人负责统一管理和日常维护，其他人员未经允许，不得擅自动更改任何机房岛内设备配置信息。

4.原则上不得在巡检设备上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理，初步

判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

服务器设备巡检规范

为了加强 IDC 服务器管理，保障服务器设备运行的安全和稳定，特制定本规定，本规定适用于 IDC 服务器巡检管理。

对 IDC 服务器实行巡检制度，每天对服务器设备进行常规巡检，检查服务器运行状态和运行环境状况。巡检负责人:A 角-王建、B 角-刘金路。

第一条 巡检时间：IDC 服务器设备巡检具体时间是在每天上午 8:00-9:30 进行。

第二条 巡检内容：服务器设备运行环境，服务器设备工作状态等。

第三条 巡检流程:

1.检查服务器设备表面温度是否过高、设备运转声音是否正常、网线和电源线是否松动等;

2.检查服务器设备的通电状态，电源指示灯、运行状态指示灯是否正常;

3.检查服务器前面板有无故障灯闪烁，或者面板有无提示报警信息;

4.检查服务器硬盘每个硬盘指示灯是否有报警灯闪烁;

第四条 巡检人员职责:

1.巡检人员应恪守保密制度，不得擅自泄露服务器设备相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严

禁进行越权操作。

3.服务器设备由专人负责统一管理和日常维护，其他人员未经允许，不得擅自动更改任何服务器设备配置信息。

4.原则上不得在巡检设备上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理，初步判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

存储设备巡检规范

为了加强存储设备管理，保障存储设备运行的安全和稳定，特制定本规范，本规范适用于存储设备巡检管理。

对 IDC 存储设备实行巡检制度，每天对存储设备进行巡检，巡检对象为:

序号	名称	数量
1	光纤交换机	6 台
2	双活存储	1 套
3	Unity 存储	3 套
4	Vnx 存储	1 套
5	Nas 存储	1 套
6	全闪存储	1 套
7	分布式存储	1 套

巡检存储设备硬件状态信息、设备功能等。

存储设备巡检负责人:A 角-刘金路、B 角-王建。

第一条 巡检时间: IDC 存储设备巡检具体时间为每天上午 8:00-9:30。

第二条 巡检内容: 存储设备硬件信息、链路状态、容量使用和服务健康状况检查等。

第三条 巡检流程:

1.设备巡检:

通过统一存储管理平台的设备管理、网络管理、容量管理功能，进行链路和服务健康状况检查，主要检查容量使用情况、链路健康状况、系统健康状况以及存储健康情况。

2.告警处理:

（1）通过统一存储管理平台的告警管理功能检查光纤交换机以及各类存储设备系统告警状态，当出现告警信息时，根据告警类型、告警位置以及告警描述分析系统状况并及时处置。

（2）当“告警管理”中出现严重告警时，需登录光纤交换机以及各类存储设备自身管理平台，通过系统告警日志、事件详细内容，具体分析告警信息，联系厂家处理。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度,不得擅自泄露存储设备相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.存储设备由专人负责统一管理和日常维护,其他人员未经允许，不得擅自动更改任何存储设备配置信息。

4.原则上不得在巡检设备上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理,初步判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

IDC 网络巡检规范

为了加强 IDC 网络可靠性管理,保障网络设备运行的安全和稳定，特制定本规范，本规范适用于 IDC 网络巡检管理。

对 IDC 网络实行巡检制度，每天对网络进行巡检，巡检对象为 IDC 网络对外提供服务、网络流量、交换机及防火墙。巡检网络设备硬件状态信息、设备功能等。网络巡检负责人:A 角-徐千、B 角-孙彦飞。

第一条 巡检时间:IDC 网络巡检具体时间为每天上午 8:00-9:30。

第二条 巡检内容: IDC 网络对外提供服务、网络流量、网络设备硬件信息检查等。

第三条 巡检流程:

1.网络 IDC 网络对外提供服务，通过互联网、校园网检查 IDC 服务网络联通性。

2.网络流量，通过 MRTG、CACTI 平台检查 IDC 网络流量信息。

3.交换机与防火墙，登录各核心交换机、接入交换机、IDC 防火墙及专网防火墙终端，输入相应命令，分别检查以下项目:

（1）接口状态检查: 要求检查日志中端口连接、断开事件情况。

（2）光模块功率检查: 要求设备可插拔模块的输入输出光功率在标准区间范围内。

（3）设备温度检查：要求设备单板运行温度小于告警温度数值。

（4）电源运行状态检查：要求设备所有在位电源模块运行在正常状态。

（5）集群运行状态检查：要求集群内设备在线且为双活状态。

（6）设备 CPU 利用率检查：要求设备的 CPU 利用率在合理的阈值设定范围之内。

（7）风扇运行状态检查：要求设备所有风扇模块运行在正常状态。

（8）设备运行时间检查：要求设备时间准确，设备运行时间符合维护计划，与上次有计划重启时间相符。

第四条 巡检人员职责：

1.巡检人员应恪守保密制度，不得擅自泄露网络设备相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.网络设备由专人负责统一管理和日常维护，其他人员未经允许，不得擅自动更改任何网络设备配置信息。

4.原则上不得在巡检设备上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理，初步判断问

题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

虚拟化平台巡检规范

为了加强虚拟化平台管理,保障虚拟化平台运行的安全和稳定，特制定本规定，本规定适用于 IDC 虚拟化平台巡检管理。

对虚拟化平台实行巡检制度,每天对虚拟化平台进行常规巡检，巡检对象三套虚拟化平台，版本均为 VMware Vcenter6.7。巡检虚拟化平台服务状态、系统功能等。虚拟化平台巡检负责人:A 角-王建、B 角-徐千。

第一条 巡检时间: IDC 虚拟化平台巡检具体时间是在每天上午 8:00-9:30 进行。

第二条 巡检内容:巡检虚拟化平台的计算资源、网络资源、存储资源、系统日志等是否异常。

第三条 巡检流程:

1.登录虚拟化管理平台界面,在虚拟化平台顶端,选中“监控”，查看最近虚拟化平台所有问题和已触发的警报。

2.巡检虚拟化平台宿主机硬件是否正常，在 WEB 管理界面里,点击主页上的“主机和集群”图标，然后点击物理机，选中“监控”，查看主机硬件所有问题和已触发的警报。

3.巡检虚拟化平台宿主机时间配置是否正常， 检查 NTP 客户端， NTP 服务状态和 NTP 服务器是否正常。

4.巡检虚拟化平台宿主机网卡速率和全双工状态,确保每块网卡都是全速,全双工。宿主机应用和管理的网络流量分离到不同的物理网卡。

5.巡检虚拟化平台宿主机的存储设备是否正常，在 WEB 管理界面里,点击宿主机的“数据存储”图标，查看存储状态是否正常。

6.巡检虚拟化平台宿主机是否可以远程登录,默认使用时,为安全考虑,宿主机默认禁止 ssh 远程登录。

7.巡检虚拟化平台虚拟机服务器 VMware Tools 是否安装了正确的版本。

8.巡检虚拟化平台高可用集群无警告标识,高可用集群需能提供足够冗余资源容量,确保虚拟机高可用切换正常。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度,不得擅自泄露虚拟化平台相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.虚拟化平台由专人负责统一管理和日常维护,其他人员未经允许，不得擅自动更改任何虚拟化平台配置信息。

4.原则上不得在虚拟化平台上安装软件和插件,若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理,初步判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和

可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

数据备份设备巡检规范

为了加强备份设备管理，保障备份设备运行的安全和稳定，特制定本规范，本规范适用于备份设备巡检管理。

对 IDC 备份设备实行巡检制度，每天对备份设备进行巡检，巡检对象为:

序号	名称	数量
1	Avamar	4 台
2	备份一体机	1 台

巡检备份设备硬件状态信息、设备功能等。

备份设备巡检负责人:A 角-刘金路、B 角-王建。

第一条 巡检时间: IDC 备份设备巡检具体时间为每天上午 8:00-9:30。

第二条 巡检内容: 备份设备硬件信息、链路状态、容量使用和服务健康状况检查等。

第三条 巡检流程:

1.设备巡检

通过备份设备 Console 管理界面，检查系统信息、任务活动和存储空间的状态:

（1）系统信息没有告警，即为正常状态。

（2）存储空间使用率<90%，则空间为正常。

（3）任务活动中 All Failures 数量为 0 为正常。

2.告警处理:

（1）单一设备 Capacity 使用率>=90%时，迁移部分备份虚拟机至其他 Capacity 使用率正常的备份设备。

（2）任务活动中 All Failures 数量>0 时，找到具体失败的备份虚拟机，重新备份至成功。

（3）系统信息中出现告警信息，需登录备份设备自身管理平台，通过系统告警日志、事件详细内容，具体分析告警信息，联系厂家处理。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度,不得擅自泄露备份设备相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.备份设备由专人负责统一管理和日常维护,其他人员未经允许，不得擅自动更改任何备份设备配置信息。

4.原则上不得在巡检设备上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理,初步判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

DNS 系统巡检规范

为保障 DNS 系统平稳运行、加强 DNS 系统管理，更好地提供 DNS 权威发布、递归解析服务，特制定本巡检规范，本规范适用于 DNS 系统巡检管理。

对 DNS 系统实行巡检制度，每天对 DNS 系统进行巡检，巡检对象 DNS 系统的一个管理节点和两个工作节点。巡检内容为各服务器的运行状态、配置文件备份情况等。DNS 系统巡检负责人:A 角-孙彦飞、B 角-王建。

第一条 巡检时间:DNS 系统巡检具体时间为每天上午 8:00-9:30。

第二条 巡检内容: DNS 系统的一个管理节点和两个工作节点的性能、网络以及重要进程和服务的运行状态，各工作节点的运行情况，权威、递归解析状态以及网络中 DNS 终端的异常行为等。

第三条 巡检流程:

1.通过 DNS 系统管理界面检查 DNS 系统运行状态,包括磁盘监控、进程监控、网络监控、DNS 节点监控、DNS 权威域监控、DNS 策略监控。特别注意巡检: CPU 使用率（建议 CPU 使用率在 70%以下）、负载情况(各节点负载不超过 8)、磁盘使用情况(建议磁盘使用率在 70%以下）。

2.通过 DNS 系统管理界面,重点查看“全网请求响应速率”，查看请求速率和响应速率，我校平均请求速率为 1.8KQPS，如果

出现大幅度的增加，需排查是否有DNS请求攻击问题。

3.通过DNS系统管理界面，查看系统本身配置文件是否每日进行定期备份。查看近一个月内保存日志访问记录，每月月初确认日志服务器是否保存180天内DNS系统日志记录。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度，不得擅自泄露DNS系统相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.DNS系统由专人负责统一管理和日常维护，其他人员未经允许，不得擅自动更改任何DNS系统配置信息。

4.原则上不得在巡检系统上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理，初步判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

负载均衡设备巡检规范

为了加强负载均衡设备管理,保障负载均衡设备运行的安全和稳定,特制定本规范,本规范适用于IDC负载均衡设备巡检管理。

对IDC负载均衡设备实行巡检制度,每天对负载均衡设备进行巡检,巡检对象为一台A10 TH3030S,两台A10 TH 1040。巡检负载均衡设备硬件状态信息、设备功能等。负载均衡设备巡检负责人:A角-王建、B角-徐千。

第一条 巡检时间: IDC 负载均衡设备巡检具体时间为每天上午8:00-9:30。

第二条 巡检内容: 负载均衡设备硬件信息、链路状态、流量和服务健康状况检查等。

第三条 巡检流程:

1.通过负载均衡设备管理界面检查负载均衡硬件系统状态,检查CPU信息、CPU温度、系统温度、磁盘使用情况、风扇运转情况、电源情况。特别注意巡检: CPU使用情况(建议CPU占用率在70%以下)、内存使用情况(建议内存使用率在80%以下)、系统日志、设备接口状态。

2.通过负载均衡设备管理界面,进行链路、服务器流量和服务健康状况检查,主要分析服务器流量分配使用情况、链路健康状况、Real server健康状况、Service Group健康状况、VIRTUAL SERVER健康状况。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度,不得擅自泄露负载均衡设备相关密码和配置信息。

2.巡检人员应明确操作权限,严格按照本人的权限操作,严禁进行越权操作。

3.负载均衡设备由专人负责统一管理和日常维护,其他人员未经允许,不得擅自动更改任何负载均衡设备配置信息。

4.原则上不得在巡检设备上安装软件,若确需要安装,应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理,初步判断问题类型,对权限许可处理的问题及时研究并提出补救措施,处理时要汇报负责处领导。

6.对无权处理或不能处理的问题,将异常现象、发生时间和可能的原因做详细记录,并立即通知厂家,对异常情况进行分析和处理。

反向代理系统巡检规范

为保障反向代理系统的平稳运行，加强网站与信息系统安全、稳定运行，特制定本规范，本规范适用于反向代理系统巡检管理。

对反向代理系统实行巡检制度，每天对反向代理系统进行巡检，巡检对象为反向代理系统的一个管理节点和六个工作节点。巡检内容为各服务器的运行状态、资源访问情况等。反向代理系统巡检负责人：A 角-孙彦飞、B 角-王建。

第一条 巡检时间：反向代理系统巡检具体时间为每天上午 8:00-9:30。

第二条 巡检内容：反向代理系统的一个管理节点和六个工作节点运行状态的各项指标信息、系统备份、资源访问和日志存储等情况。

第三条 巡检流程：

1.通过反向代理系统管理界面检查反向代理系统运行状态，检查 CPU 使用率、内存使用情况、磁盘使用情况、负载情况及流量情况。特别注意巡检：CPU 使用率（建议 CPU 使用率在 70%以下）、负载情况（管理节点负载不超过 16、各工作节点负载不超过 8）、磁盘使用情况（建议磁盘使用率在 85%以下）。

2.通过反向代理系统管理界面，查看系统本身配置文件是否每日进行定期备份。查看当前系统告警是否新增域名告警情况。查看是否存在 IP 地址恶意大量访问网站情况。查看近一个月内保存日志访问记录，每月月初定期确认日志服务器是否保存 180

天内反向代理系统日志记录。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度,不得擅自泄露反向代理系统相关密码和配置信息。

2.巡检人员应明确操作权限,严格按照本人的权限操作,严禁进行越权操作。

3.反向代理系统由专人负责统一管理和日常维护,其他人员未经允许,不得擅自动更改任何反向代理系统配置信息。

4.原则上不得在巡检系统上安装软件,若确需要安装,应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理,初步判断问题类型,对权限许可处理的问题及时研究并提出补救措施,处理时要汇报负责处领导。

6.对无权处理或不能处理的问题,将异常现象、发生时间和可能的原因做详细记录,并立即通知厂家,对异常情况进行分析和处理。

VPN 系统巡检规范

为加强 WEBVPN 系统和 SSLVPN 系统管理,保障广大师生访问校内网络资源的需求,满足技术人员在校外访问和管理 IDC 内网服务器的需求，特制定本规范。本规范适用于 WEBVPN 系统和 SSLVPN 系统（以下统称 VPN 系统）巡检管理。

对VPN系统实行巡检制度,每天对VPN系统进行巡检,WEBVPN系统巡检对象为一台主控设备,一台隧道设备;SSLVPN 系统巡检对象为一台 SSLVPN 设备。巡检 VPN 系统的运行、网络状态等信息。VPN 系统巡检负责人:A 角-孙彦飞、B 角-王建。

第一条 巡检时间:VPN 系统巡检具体时间为每天上午 8:00-9:30。

第二条 巡检内容: VPN 系统的运行状态、用户访问情况、网络通断情况。

第三条 巡检流程:

1.WEBVPN 系统巡检流程:

（1）检查系统运行状态: 包括系统负载、磁盘使用、内存用量。

（2）检查用户访问情况: 包括访问次数、访问流量、用户数，是否存在异常增大情况。

（3）检查网络状态: 包括主控与隧道连接、页面访问、流量情况。

2.SSLVPN 系统巡检流程:

（1）检查系统运行状态：包括内存用量、CPU 使用率、磁盘使用、设备温度、风扇状态。

（2）用户访问情况：包括 24h 内登录用户总数、实时登录用户数。

（3）检查网络状态：内部端口链接状态、页面访问、流量情况。

（4）日志监控：查看关键事件是否新增告警。

第四条 巡检人员职责：

1.巡检人员应恪守保密制度，不得擅自泄露 VPN 系统相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.VPN 系统由专人负责统一管理和日常维护，其他人员未经允许，不得擅自动更改任何 VPN 系统设备配置信息。

4.原则上不得在巡检设备上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理，初步判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

网闸设备巡检规范

为了加强网闸设备管理，保障网闸设备运行的安全和稳定，特制定本规定，本规定适用于 IDC 网闸巡检管理。

对 IDC 网闸实行巡检制度，每天对网闸设备进行常规巡检，巡检网闸设备硬件状态、设备功能等。设备巡检负责人:A 角-王建、B 角-孙彦飞。

第一条 巡检时间：网闸设备巡检具体时间是在每天上午 8:00-9:30 进行。

第二条 巡检内容：网闸设备硬件情况、功能情况、流量和系统运行状况等。

第三条 巡检流程:

网闸设备分为内网区域和外网区域两部分,均需要进行检查,检查方法相同。

1.使用管理员帐号登录网闸设备,在系统管理-系统概览中,确定系统运行时间，隔离卡状态是否开启,检查 CPU 利用率（建议 CPU 占用率在 20%以下）,内存利用率（建议内存占用率在 30%以下）,磁盘利用率（建议内存占用率在 80%以下）是否正常。

2.检查网闸设备网络链路接口是否正常,同时查看网络流量状态监控图和流量统计图是否正常。查看服务状态情况（包括安全传输和 HA 模块）是否正常，检查 license 是否正常，检查业务日志和管理日志，确定没有异常报错信息。

第四条 巡检人员职责:

1.巡检人员应恪守保密制度，不得擅自泄露网闸设备相关密码和配置信息。

2.巡检人员应明确操作权限，严格按照本人的权限操作，严禁进行越权操作。

3.网闸设备由专人负责统一管理和日常维护，其他人员未经允许，不得擅自动更改任何网闸设备配置信息。

4.原则上不得在巡检设备上安装软件，若确需要安装，应由厂家人员实施。

5.巡检人员发现故障和问题要及时汇报和处理，初步判断问题类型，对权限许可处理的问题及时研究并提出补救措施，处理时要汇报负责处领导。

6.对无权处理或不能处理的问题，将异常现象、发生时间和可能的原因做详细记录，并立即通知厂家，对异常情况进行分析和处理。

哈尔滨工程大学信息化处综合办公室　　2022年6月8日印发