



国家电网公司
STATE GRID
CORPORATION OF CHINA

信息安全 反违章工作手册

(专业版)



国家电网公司 编



中国电力出版社
CHINA ELECTRIC POWER PRESS



国家电网公司
STATE GRID
CORPORATION OF CHINA

信息安全 反违章工作手册

(专业版)

国家电网公司 编



中国电力出版社
CHINA ELECTRIC POWER PRESS

图书在版编目 (CIP) 数据

信息安全反违章工作手册：专业版 / 国家电网公司编.
—北京：中国电力出版社，2015.1
ISBN 978-7-5123-4460-0

I. ①信… II. ①国… III. ①信息安全—手册 IV. ①TP309-62

中国版本图书馆CIP数据核字 (2013) 第101448号



中国电力出版社出版、发行
(北京市东城区北京站西街19号 100005 <http://www.cepp.sgcc.com.cn>)
北京瑞禾彩色印刷有限公司印刷

2015年1月第一版 2015年1月北京第一次印刷
889毫米×1194毫米 32开本 8.625印张 172千字

定价 45.00 元

敬告读者

本书封底贴有防伪标签，刮开涂层可查询真伪
本书如有印装质量问题，我社发行部负责退换

版权专有 翻印必究

信息安全基本方针	安全第一、预防为主、综合治理
信息安全责任	谁主管谁负责、谁运行谁负责、谁使用谁负责
信息安全保密纪律	涉密不上网、上网不涉密
“三同步”原则	坚持信息安全与信息化工作同步规划、同步建设、同步投入运行
“三纳入”原则	将等级保护纳入信息安全工作中，将信息安全纳入信息化中，将信息安全纳入公司安全生产管理体系中
信息安全防护策略	管理信息系统安全防护策略：分区分域、安全接入、动态感知、全面防护 电力二次系统安全防护策略：安全分区、网络专用、横向隔离、纵向认证

前言



Preface

信息安全作为生产自动化和管理信息化深入推进的重要保障，其基础性、全局性、全员性作用日益增强，对电网安全有着重大影响。

信息安全习惯性违章是指相关人员由于安全意识不足，以及对安全事件的危害认识不够，在日积月累中渐渐养成的一种不良习惯。为帮助国家电网公司广大员工提高信息安全意识，认识和克服日常工作中的信息安全习惯性违章行为，公司组织编写了《信息安全反违章工作手册》，旨在为广大员工对照检查和克服信息安全习惯性违章行为提供帮助。

针对普通信息系统用户和信息化工作人员等不同读者对象，《手册》分成了普及和专业两个版本。本书是专业版，整理出了安全管理制度、人员安全管理、系统建设管理、系统运行管理、物理安全、网络及边界安全、主机安全、应用安全、数据安全及备份恢复九类，共234种信息安全习惯性违章行为，并对每种行为提出了防范措施与建议。对广大信息技术与管理人员提高信息安全意识、更好地辨识和克服信息安全违章行为，起到很好的参考作用。

全书由国家电网公司办公厅、信息通信部负责拟定内容大纲并审核校正，国网河南省电力公司、南瑞集团公司、中国电力科学研究院、国网智能电网研究院承担了大量的编写工作。在《信息安全反违章工作手册》的编写过程中得到了国家级专家、公司专家、各单位领导及相关信息安全管理与技术人员的大力支持，他们提出了许多的宝贵意见和建议，在此一并表示衷心感谢。

国家电网公司办公厅

国家电网公司信息通信部

2015年1月

目录



Contents

前言



A 安全管理制度

- A-1 未明确信息安全总体方针和策略.....2
- A-2 信息安全制度未说明安全工作的总体目标、范围、原则和安全框架.....3
- A-3 未制定信息系统运维人员和督查人员的日常操作规程.....4
- A-4 未定期对安全管理制度进行修编或评审.....5
- A-5 未针对系统变更、重要操作、物理访问和系统接入等重要事项建立审批程序.....6
- A-6 安全管理员兼任网络管理员、系统管理员、数据库管理员等.....7
- A-7 安全运维员职责未包括定期对系统日常运行、系统漏洞和数据备份等情况进行检查.....8
- A-8 未在制度中明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等.....9
- A-9 未制定制度对网络安全配置、日志保存时间、安全策略、补丁升级与漏洞修补、口令更新等内容作出规定.....10



B 人员安全管理

- B-1 未签署保密协议，重要安全岗位人员离职时未签署保密协议.....12

- B-2 未制订安全培训计划.....**13**
- B-3 未开展覆盖全员的安全意识教育和培训.....**14**
- B-4 未对关键岗位人员进行全面、严格的安全审查和技能考核.....**15**
- B-5 员工离职、调动后未注销其在信息系统中所有的账号和访问权限.....**16**
- B-6 未对外部人员允许访问的区域、系统、设备、信息等内容进行书面规定，并未按照规定执行.....**17**
- B-7 未明确安全岗位录用要求.....**18**
- B-8 安全管理制度中无第三方人员管理内容.....**19**
- B-9 操作时未严格执行“两票制度”**20**
- B-10 值班人员在工作时间擅自离岗.....**21**
- B-11 员工岗位变动造成人员信息变更时未及时通知信息系统运维人员.....**22**



C 系统建设管理

- C-1 无系统定级报告，未确定安全保护等级，导致不能按照相应等级要求进行安全防护.....**24**
- C-2 未向行业监管部门和公安部门申请进行信息系统等级定级审批，无系统备案报告和公安部门备案记录.....**25**
- C-3 未评审业务系统的信息安全等级保护定级情况.....**26**
- C-4 未与信息系统外部合作单位签订保密协议及承诺书.....**27**

- C-5 外部合作单位在非公司网络中存储、运行公司信息.....28
- C-6 已上线试运行系统未制定系统安全防护方案.....29
- C-7 在系统规划阶段未组织制定业务系统信息安全防护方案
.....30
- C-8 安全防护方案未包括风险分析、防护目标、边界、网络、
主机、应用、数据等防护措施及内容.....31
- C-9 安全防护方案未经专家委评审32
- C-10 信息化建设和推广项目开发环境与工作环境未纳入信息
内网统一管理，未在信息内网划分独立的安全域.....33
- C-11 开发环境与实际运行环境未分离.....34
- C-12 未对项目开发人员进行信息安全及保密培训.....35
- C-13 应用系统未通过公司代码安全检测.....36
- C-14 未成立研发安全组织机构，未能统一组织开展研发安全
工作.....37
- C-15 系统运维部门（单位）未在系统建设阶段前介入，未对
信息安全防护措施及运行维护中的信息安全风险提出意
见和建议.....38
- C-16 安装软件之前未检测软件中可能存在的恶意代码.....39
- C-17 信息系统安全建设过程中涉及的信息安全软硬件产品和
密码产品未全部采用国产产品.....40
- C-18 未开展产品预先选型和安全测试.....41
- C-19 系统无上线、安全性测评报告.....42

C-20 合作单位标注“国家电网”标识时未履行相应手续.....43

C-21 对非公司认可的信息化成果标注公司标识.....44

C-22 信息安全测评工作由无资质测评机构完成.....45

C-23 信息系统上线和版本升级前未开展软件著作权备案工作.....46

C-24 未建设漏洞库，无法发布漏洞预警；安全补丁未开展统一测试，测试后未录入统一补丁库.....47



D 系统运行管理

D-1 未及时更新资产清单，设备清单无固定、规范的格式.....49

D-2 机房内的服务器、机柜、网络设备等设施无标识.....50

D-3 信息处理设备未经过审批就被带离机房或办公地点.....51

D-4 无应急物资（设备）清单或台账.....52

D-5 应急物资无可靠性或可用性验证记录.....53

D-6 应急预案未经专家评审.....54

D-7 未定期组织开展应急培训和应急演练.....55

D-8 监测日志和审计记录被违规篡改.....56

D-9 未保存运行日志和审核记录，不能为安全事件及系统故障后的处理工作提供有力的证据信息.....57

D-10 无分析运行日志和审计日志.....58

- D-11 无日常监测和值班记录.....**59**
- D-12 日常监测工作未覆盖通信线路、主机、网络设备和应用系统的运行状态、网络流量、用户行为、安全告警等内容.....**60**
- D-13 未指定专人负责运行日志、网络监控记录的日常维护、报警信息分析和处理.....**61**
- D-14 未定期对网络信息系统进行漏洞扫描，未对发现的漏洞进行修补.....**62**
- D-15 未对设备状态、恶意代码、补丁升级、安全审计等内容进行集中分析.....**63**
- D-16 内网办公计算机通过3G上网卡等方式连接互联网.....**64**
- D-17 未定期开展网络与系统漏洞扫描，未及时修补漏洞.....**65**
- D-18 在安装系统补丁前，未在测试环境中进行测试及系统备份.....**66**
- D-19 外来计算机在接入公司网络前未进行计算机安全检查.....**67**
- D-20 未针对系统变更制定应急预案及恢复流程.....**68**
- D-21 在信息系统运行维护、数据交互和调试期间，未执行“两票制度”，擅自进行在线调试和修改.....**69**
- D-22 变更、检修等文档和记录未保存（包括系统中未保存）.....**70**
- D-23 通过互联网或信息外网远程运维方式进行设备和系统的

维护和技术支持工作.....71

D-24 未对在机房内开展的线路、设备的检修、施工等工作进行全程监督.....72

D-25 随意开展检修操作，检修工作无计划.....73

D-26 核心信息系统未实现主业化运维.....74

D-27 内网远程运维未履行审批程序.....75

D-28 未制定信息系统安全事件处理预案和事件处置流程.....76

D-29 未按规定备份的周期、存储介质方式及恢复演练的周期.....77

D-30 未按照管理要求，确定需要定期备份的重要业务数据及软件.....78

D-31 备份操作中无详细的操作记录.....79

D-32 移动存储介质未更改初始口令、内部人员口令通用导致信息泄露.....80

D-33 业务系统存在公共账户及口令.....81

D-34 未对安全事件分类，且安全事件分类与国家、公司分类标准不符.....82

D-35 无安全事件处置记录或安全事件处置记录不完整、不详细、未分析安全事件产生的原因.....83

D-36 通过互联网接入信息内网进行远程维护.....84

D-37 未开启网络运行监控，不能对网络设备性能、流量进行实时监测.....85

- D-38 未对下属单位互联网出口进行严格管控、合并、统一设置和集中监控.....**86**
- D-39 未开展互联网出口攻击、病毒木马敏感信息的安全监测与内容审计.....**87**
- D-40 未全面监测主机，不了解其性能和运行状态，导致主机故障后无法查询原因和恢复.....**88**
- D-41 权限调整、链路变更、DNS调整、策略调整、系统升级等影响级联贯通访问的变更操作未报公司审批.....**89**
- D-42 未将业务系统及安全与运维级联贯通情况纳入日常监控.....**90**
- D-43 未开启数据库运行监控及审计功能，不能及时了解数据库的运行状况和性能.....**91**
- D-44 未定期对监测和报警记录进行分析、评审，未形成分析报告.....**92**
- D-45 重要信息系统未部署应用服务器和数据库集群.....**93**
- D-46 重要信息系统未采取措施验证集群切换有效性.....**94**
- D-47 重要信息系统负载均衡设备参数配置不当，致使承载压力不均，业务接管无效.....**95**
- D-48 重要信息系统数据库集群参数配置不当致使压力不均，切换无效.....**96**
- D-49 重要信息系统集群配置不当，致使无法自动隔离故障节点.....**97**
- D-50 集群部署重要信息系统未按要求健全系统运行应急预案

和现场处置方案.....98

D-51 集群部署重要信息系统未按要求定期开展应急演练.....

99

D-52 集群部署重要信息系统所用操作系统存在补丁更新未测试、不及时现象，或存在已知但未解决的重要bug.....100

D-53 集群部署重要信息系统共享存储设备或共享文件系统运行不稳定.....101

D-54 集群部署系统参数配置不当致使无法完整收集系统运行异常时的状态信息等资料.....102

D-55 未开启桌面终端监控，桌面终端注册率、防病毒软件安装率、保密检测系统安装率未达到100%.....103

D-56 与银行等外部单位的互联专线未部署安全防护措施.....
104

D-57 网站未使用公司统一域名.....105

D-58 对外发布的网站未采取网页防篡改措施.....106

D-59 在运信息系统未向总部备案.....107

D-60 信息外网无线网络未启用网络接入控制和身份认证措施.....108

D-61 网络核心交换机、路由器等网络设备配置未定期离线备份.....109

D-62 将承担安全责任的对外网站托管于外部单位.....110

D-63 在信息内网设立与工作无关的娱乐、论坛、视频等网站.....111

- D-64 家属区网络违规接入信息内、外网.....**112**
- D-65 邮箱开启自动转发功能.....**113**
- D-66 私设外网邮件系统，未使用公司统一外网邮件系统.....
114
- D-67 邮件系统未开启收发日志审计和敏感内容拦截策略等功能.....**115**
- D-68 防火墙策略变更、审批记录不完备.....**116**
- D-69 对临时开通的防火墙访问控制策略与端口，在操作结束后未及时履行注销手续.....**117**
- D-70 对设备进行重启时未经过核对程序，无人监督.....**118**
- D-71 未指定专人负责对网络和主机进行恶意代码检测并保存检测记录.....**119**
- D-72 未对防恶意代码软件的授权使用、恶意代码库升级、定级汇报等作出明确规定.....**120**
- D-73 未定期检查及记录信息系统内各种产品恶意代码库的升级情况，未对主机防病毒产品、防病毒网关和邮件防病毒网关拦截的恶意代码进行及时分析处理，未形成书面总结汇报.....**121**
- D-74 发生信息安全事件时，未及时上报上级有关部门.....
122
- D-75 备案设备未粘贴信息安全备案标签.....**123**
- D-76 系统及设备备案信息不完整，不准确，信息更新不及时.....**124**

- D-77 已下线设备及系统在IMS中显示为在运.....**125**
- D-78 在运设备未纳入IMS资产管理.....**126**
- D-79 防火墙未按照公司防火墙基线标准进行防火墙账号、服务等安全配置及防火墙策略规范性、有效性和冗余性等策略配置.....**127**
- D-80 未对在公司信息外网出口使用社会邮箱发送邮件行为进行审计及阻断.....**128**
- D-81 未对用户URL访问行为进行记录，无法按照国家及公司要求进行行为溯源.....**129**
- D-82 内网办公计算机中的商秘文件无保护措施.....**130**
- D-83 对外发送敏感内容文件未采取保护措施.....**131**
- D-84 未对下线或变更用途的电子存储介质中存储的电子数据进行擦除或销毁.....**132**
- D-85 通过未获得国家相关权威机构授权的外部单位或机构进行数据擦除、销毁和恢复.....**133**
- D-86 采用未通过国家相关权威机构安全性测试的设备进行数据擦除、销毁.....**134**
- D-87 通过光驱刻录、安全移动存储介质拷贝办公计算机数据的行为未进行审计.....**135**
- D-88 系统接入开通时，防火墙等重要设备策略由厂家配置，造成安全策略泄露.....**136**
- D-89 个人手机或智能可穿戴设备连接办公计算机.....**137**

- D-90 对采用APN等内网第三方专线接入的终端，未严格遵循“五限制”策略（“内网安全终端、无线加密专网、终端入网绑定、交互操作固定、数据传输加密”）.....**138**
- D-91 新增的公司公共微博、微信账号未备案.....**139**
- D-92 在公司公共微博、微信上发布未经审核的内容.....**140**
- D-93 在公司外网随意用wi-fi组网.....**141**
- D-94 红、蓝队未建立队伍联合处置机制，未进行对抗演练.....**142**
- D-95 蓝队未按要求开展信息安全综合审计工作.....**143**
- D-96 对国内外的信息安全形势和公司信息安全态势未定期形成分析材料.....**144**
- D-97 为便于调试与运维，设备、系统、应用等采用默认配置.....**145**
- D-98 由于业务需求紧迫，未对上线系统进行安全性测评.....**146**
- D-99 应用系统代码编写规范要求不严，源代码安全考虑欠缺.....**147**



E 物理安全

- E-1 服务器或重要网络设备未部署在机房内.....**149**
- E-2 机房未安装24小时实时视频监控系统，无法对机房内环境情况进行实时观测.....**150**

- E-3 机房内未设置防雷保安器，在雷雨天气容易受到感应雷，导致计算机设备故障.....**151**
- E-4 机房未安装火情检测报警系统及气体消防系统.....**152**
- E-5 机房消防设备未进行定期检查、维护、更新.....**153**
- E-6 机房未采用防静电地板.....**154**
- E-7 机房未设置温、湿度自动调节措施.....**155**
- E-8 机房UPS设备供电时间不足.....**156**
- E-9 机房未配备冗余或并行的电力电缆线路为机房供电.....**157**
- E-10 重要设备未配置双电源.....**158**
- E-11 机房电源线缆和通信线缆未进行隔离铺设，可能互相干扰.....**159**
- E-12 机房位置处于建筑物地下、一层或者顶层.....**160**
- E-13 机房未配备电子门禁系统.....**161**
- E-14 机房未划分区域管理，未设置过渡区域.....**162**
- E-15 出入机房无记录.....**163**
- E-16 机房设备未上架或机柜未上锁.....**164**
- E-17 UPS电源未按要求定期进行充放电试验.....**165**
- E-18 机房无除尘装置，或除尘装置损坏.....**166**
- E-19 将机房门禁卡随意借给他人.....**167**
- E-20 门禁密码设置过于简单，更换周期长.....**168**