ICS 03.100.01
CCS A 01

DB2101

沈　阳　市　地　方　标　准

DB2101/T0080—2023

企业商业秘密信息化安全防护规范

Specification for Information Security Protection of Enterprise Trade Secrets

2023-08-28 发布　　2023-09-28 实施

沈阳市市场监督管理局　发布

目　　次

前言.....II
1 范围.....1
2 规范性引用文件.....1
3 术语和定义.....1
4 机构与职责.....2
4.1 安全防护管理机构.....2
4.2 信息安全保密管理人员.....3
5 策略与制度.....4
6 技术要求.....4
6.1 物理环境安全.....4
6.2 网络及边界安全.....5
6.3 主机、应用、数据安全.....6
7 建设管理.....8
7.1 安全方案设计.....8
7.2 产品或服务的选择.....8
7.3 软件开发.....8
7.4 工程实施.....8
7.5 系统交付与验收.....8
8 运维管理.....9
8.1 环境管理.....9
8.2 资产管理.....9
8.3 存储载体管理.....9
8.4 维护管理.....9
8.5 漏洞与隐患管理.....9
8.6 升级管理.....10
8.7 配置管理.....10
8.8 变更管理.....10
8.9 备份与恢复管理.....10
8.10 外包运维管理.....10
9 风险监测与评估.....10
9.1 风险监测.....10
9.2 风险评估.....10
10 安全事件处置与应急管理.....10
10.1 安全事件处置.....10
10.2 应急预案管理.....11
参考文献.....12

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由沈阳市市场监督管理局（沈阳市知识产权局）提出并归口，同时负责标准的宣贯、监督实施等工作。

本文件起草单位：沈鼓集团股份有限公司、沈阳市市场监督管理局、沈阳市铁西区市场监督管理局、沈阳市市场监管事务服务中心。

本文件主要起草人：郝玉明、边作晰、于佳、田宁、赵永辉、张功、丁凯、靳川、刘爽、薛晓颖、勾颖、王磊、孙洁。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电、来函等方式进行反馈，我们将及时答复并认真处理，根据实施情况依法进行评估及复审。

本文件归口部门通讯地址：沈阳市市场监督管理局（沈阳市沈河区南关路 118 号）；联系电话：024-24011535。

本文件起草单位通讯地址：沈鼓集团股份有限公司(沈阳经济技术开发区开发大路 16 号甲)；联系电话：024-25801407。

企业商业秘密信息化安全防护规范

1 范围

本文件规定了企业商业秘密信息化安全防护体系的机构职责、策略与制度、技术要求、建设管理、运维管理、安全事件处置与应急管理。

本文件适用于企业商业秘密信息化安全防护体系的规划、建设、运维与改进管理，同时也可为机构、协会、科研院所等组织的商业秘密技术防护措施提供参考。主要用于有下列需求的企业：

a） 建立商业秘密信息化安全防护体系；

b） 运行并持续改进商业秘密信息化安全防护体系；

c） 寻求外部组织对其商业秘密技术防护体系进行评价。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2887-2011 计算机场地通用规范

GB/T 9361-2011 计算机场地安全要求

DB21/T 3659-2022 商业秘密保护管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

商业秘密 trade secret

不为公众所知悉，具有商业价值，并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

注：“不为公众所知悉”“具有商业价值”“相应保密措施”的具体内容详见《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》。

3.2

涉密设备 confidential device

采集、存储、处理、传输涉及企业商业秘密信息的各类设备。

3.3

涉密信息系统 confidential information system

由计算机及其相关和配套设施、设备构成的，按照一定应用目标和规则存储、处理、传输企业商业秘密信息的系统。

3.4

涉密载体 confidential carrier

以文字、数据、符号、图形、图像、视频和音频等方式记录或存储企业商业秘密信息的纸介质、磁介质、光介质以及半导体介质等各类物品。

3.5

安全域 security domain

由一组具有相同安全保护需求、并相互信任的信息系统、网络及设备组成的逻辑区域。

3.6

涉密区域 confidential area

企业内产生、存储、处理、传输涉及商业秘密信息的场所。

3.7

信息安全产品 information security products

专门用于保障信息安全的软件、硬件或其组合体。

4 机构与职责

4.1 安全防护管理机构

4.1.1 组织设置与职责

4.1.1.1 企业应成立商业秘密信息化安全防护委员会，负责本单位商业秘密信息化安全防护体系规划指导与总体管理，其最高领导由单位主管信息安全的领导担任或授权。

4.1.1.2 企业应设立商业秘密信息化安全防护管理工作的职能部门，负责本单位商业秘密信息化安全防护体系建设实施和日常管理。

4.1.2 岗位配置与职责

4.1.2.1 企业应设置专职或兼职信息安全与保密技术防护管理负责人岗位，并确定其职责。

4.1.2.2 企业应为各类涉密信息系统、信息安全产品设立信息安全保密管理岗位，包括：系统管理员、安全保密员和安全审计员等岗位，并确定各个工作岗位的职责。

4.1.2.3 对于涉及核心商业秘密（根据DB21/T 3659 商业秘密保护管理规范 5.1.2条款确定密级，以下相同）的涉密信息系统、信息安全产品，应配备专职安全管理员，不可兼任。

4.1.3 授权与审批

4.1.3.1 企业应对涉密信息系统和网络的规划、建设、变更等建立逐级审批程序，所有审批流程应经过所在部门、商业秘密保护职能部门、商业秘密信息化安全防护委员会审批，明确各审批节点的审批人员及审批权限，按照规定履行审批程序，并保存审批记录。

4.1.3.2 企业应根据各个部门业务内容和岗位职责确定具有的涉密信息系统、信息安全产品和网络权限，建立审批流程，所有审批流程应经过所在部门、商业秘密保护职能部门审批，明确各审批节点的审批人员及审批权限，所有权限的赋予应履行审批程序，并保存审批记录。

4.1.3.3 企业应定期审查审批人员审批事项及审批权限使用情况，并在人员及权限变更时及时更新授权，以确保审批过程的有效性和安全性。
4.1.3.4 企业应定期审查上述各类审批事项，保证各类审批程序按照要求执行，对不符合要求的情况予以整改。

4.1.4 内外部沟通和合作

4.1.4.1 企业应加强内部与外部的沟通合作，按照国家政策法规、标准规范、行业发展趋势和企业业务发展情况，及时调整、改进、完善商业秘密信息化安全防护体系，保障企业商业秘密安全。
4.1.4.2 企业应建立有效的内部沟通机制，定期通过现场调研、问卷调查、座谈、会议等方式，实现安全管理部门与业务部门间的有效沟通。
4.1.4.3 企业应建立有效的外部交流与沟通机制，与政府部门、机构、协会、科研院所、安全厂商等建立指导、合作、产学研等工作模式，有效提升企业安全防护能力。

4.1.5 检查、考核与整改

4.1.5.1 企业应定期组织各类涉密信息系统、信息安全产品及网络的安全保密检查，检查内容包括各类系统及网络运行情况、系统安全配置、系统及网络权限、数据备份与恢复、系统漏洞发现与修复等。
4.1.5.2 企业组织安全保密检查应制定并使用规范的检查表，对检查内容、检查时间、检查人等进行记录，汇总并形成检查报告。
4.1.5.3 企业应对安全保密检查中发现的问题和漏洞进行闭环管理和控制，并由组织责任单位进行问题与漏洞的整改，形成整改结论与报告。

4.2 信息安全保密管理人员

4.2.1 人员录用

4.2.1.1 企业应对信息安全保密管理人员（包括系统管理员、安全保密员、安全审计员及相关人员）的录用进行必要的背景调查与专业素质测评，包括对被录用人员的教育背景、专业资格或资质、从业经历、与原单位签订保密协议及竞业限制协议的情况、掌握原单位知识产权的情况等进行审查，对其所具有的专业技能进行测评。
4.2.1.2 企业应与信息安全保密管理人员签订保密协议，保密协议应明确保密内容、保密权利和义务、违约责任等。

4.2.2 人员岗位变更与离职

4.2.2.1企业应及时按照信息安全保密管理人员岗位职责权限的变更，及时调整信息安全保密管理人员系统、网络、硬件设备权限。
4.2.2.2 信息安全保密管理人员离职时，企业应与离职人员签署竞业限制协议后，及时收回离职信息安全保密管理人员的系统、网络权限，组织离职人员完成硬件设备与工作交接。

4.2.3 安全意识教育和培训

企业应定期制定信息安全保密管理人员的培训计划，内容包括安全保密技术知识、岗位技能、系统和设备操作规程等培训项目，根据培训计划定期对信息安全保密管理人员进行安全保密意识教育和培训，进行培训效果评价以及考核；企业应定期评估培训需求并更新培训计划，以确保培训内容与现行法律法规、当前安全技术和企业安全需求保持一致。

4.2.4 外部人员管理

4.2.4.1 企业应建立外部人员访问涉密区域、涉密信息系统、信息安全产品及网络的审批流程，所有外部人员访问应履行审批程序，对外部人员的物理访问或网络访问进行登记备案。
4.2.4.2 对于涉及访问涉密区域、涉密信息系统、信息安全产品及网络的外部来访人员，企业应明确告知其保密要求及义务。
4.2.4.3 外部人员访问涉密区域经审核批准后，应由接待部门安排专人全程陪同，并应对外部人员手机、照相机、摄像机等摄录像设备的使用进行管理，保证其访问行为的合规性。
4.2.4.4 外部人员访问涉密信息系统、信息安全产品或网络经审核批准后，应按照批复文件开通对应账户并设定权限，并通过技术手段记录和监督其访问行为，访问结束后应及时注销外部人员账户和权限。
4.2.4.5 对于涉及核心商业秘密的涉密信息系统、信息安全产品或网络，除国家政府部门监督检查、系统运维管理等情况外，应拒绝参观类访问行为。

5 策略与制度

5.1 安全策略

企业应根据商业秘密信息化安全防护体系建设需要，并充分考虑与企业战略目标的协同发展，制定总体安全规划及安全策略，确定商业秘密信息化安全防护体系建设的基本原则、管控范围与安全框架。

5.2 管理制度

5.2.1 企业应建立覆盖商业秘密信息化安全防护各方面的安全管理制度、操作规程，形成完备的管理制度体系。
5.2.2 安全管理制度应覆盖组织建设及职责分工、安全人员管理、物理环境安全管理、网络安全管理、主机安全管理、应用安全管理、数据安全管理、应急事件管理与处置等事项。
5.2.3 安全操作规程应覆盖涉密信息系统、信息安全产品、网络以及相关设备的操作规范、操作方法、操作说明等事项。

5.3 制定和发布

企业商业秘密信息化安全防护管理职能部门负责安全管理制度的制定，上报商业秘密信息化安全防护委员会审批后予以发布执行，并对安全管理制度的版本进行记录与控制。

5.4 评审和修订

企业商业秘密信息化安全防护管理职能部门应定期对安全管理制度的全面性、合理性、适用性进行评估，充分征求企业内部和外部利益相关方的意见和建议，组织进行安全管理制度的制定、完善与修订，以适应企业商业秘密信息化安全防护和业务实施的需要。

6 技术要求

6.1 物理环境安全

6.1.1 物理位置及防护

企业对数据中心或机房的物理位置选择和防震、防雷、防火、防水、防潮、防静电、温湿度控制、电力供应、电磁防护等技术防护措施应符合GB/T2887-2011 计算机场地通用规范、GB/T9361-2011 计算机场地安全要求标准中C级场地的要求，推荐企业按照该标准中B级场地要求执行。

6.1.2 物理空间访问控制

6.1.2.1 企业应对数据中心或机房的出入口应配置电子门禁系统或采用专人值守的方式，对出入数据中心或机房的企业内部授权人员进行验证、登记，并对人员出入记录进行存档备查。

6.1.2.2 企业应建立数据中心或机房设备进出审批程序，所有设备的进出应严格履行审批流程，应对设备的进出情况进行登记，并应将设备出入记录进行存档备查。

6.1.2.3 企业应在数据中心或机房的出入口及内部安装视频监控系统，对所有出入和内部活动进行不间断地视频录制，历史视频保存期限应不少于3个月。

6.1.2.4 企业内部临时授权人员、外来人员进入数据中心或机房，应安排值守人员进行全程陪同。

6.2 网络及边界安全

6.2.1 网络架构

6.2.1.1 企业应按照业务系统及技术防护软硬件系统需要建设内部网络，并设置有合理的设备冗余，保证网络及网络设备处理及吞吐能力可满足业务和安全需要。

6.2.1.2 企业应按照业务、安全等方面划分不同的网络区域，可将企业内部网络划分为业务系统区、安全管理区、工控区、办公区、外联区、无线网络区、其他区域等不同的安全域，并按照便于管理和控制的原则为各网络区域分配地址。

6.2.1.3 企业应重点保障网络区域的安全，不应将网络区域部署在网络边界处，企业内网与外部网络、网络区域与其他网络区域之间应采取可靠的技术隔离和防护手段。

6.2.1.4 企业应对涉及核心商业秘密的区域设置单独的网络区域，并采取可靠的技术隔离和防护手段。

6.2.2 通信传输

企业应采用符合国家标准要求的密码技术，保证网络通信过程中数据的完整性和保密性。

6.2.3 边界防护与访问控制

6.2.3.1 企业应根据安全域划分情况，明确各网络区域边界和访问控制策略，采用技术手段进行防护，根据访问控制策略设置访问控制规则，对跨网络边界的访问和数据流进行控制和验证。

6.2.3.2 企业应采用必要的技术手段对接入内网的设备进行可信验证，可采用Internet Protocol（简称“IP”）和Media Access Control Address（简称“MAC地址”）绑定、用户账号密码认证等方式进行验证。

6.2.3.3 企业应采用必要的技术手段对内部网络访问外部网络的行为进行可信验证，可采用IP认证、用户账号密码认证等方式进行验证。

6.2.3.4 企业应限制无线网络的使用，无线网络应通过受控的边界设备且经过可信验证后接入内部网络。

6.2.3.5 企业应采用必要的技术手段对外网访问内部网络的行为进行可信验证，通过Virtual Private Network（简称“VPN”）、零信任等远程访问系统对该类行为进行管理和控制。

6.2.3.6 企业应采用必要的技术手段对非授权设备私自接入内部网络或内部非授权用户联到外部网络的行为进行检测与监控，可以定位出具体位置，并对该类行为进行有效阻断。

6.2.3.7 对于涉及核心商业秘密的网络区域，企业应采用物理或逻辑隔离的方式实现网络区域与其它区域之间的网络隔离，对于网络边界和网络区域间访问采取加强型技术防护措施。

6.2.4 入侵和恶意代码防范

6.2.4.1 企业应采用必要的技术手段对内网与外网相邻边界网络节点进行检测与监控，防止或限制从外部发起的网络攻击、恶意代码注入、垃圾邮件等行为。

6.2.4.2 企业应采用必要的技术手段对内网各安全域边界网络节点进行检测与监控，防止或限制从内部发起的网络攻击行为网络攻击、恶意代码注入、垃圾邮件等行为。

6.2.4.3 企业应采取技术措施对入侵、恶意代码、垃圾邮件等网络行为进行记录与分析，对网络攻击行为进行报警与处置。

6.2.5 安全审计

6.2.5.1 企业应对各类网络访问和网络设备日志进行存档，保存时限不低于6个月。

6.2.5.2 企业应制定对网络的安全审计规则，定期对各类网络进行安全审计，包括内网访问行为、外网远程访问内网行为、内网访问互联网行为等，并形成审计记录，审计记录应进行存档备查。

6.3 主机、应用、数据安全

6.3.1 身份鉴别

6.3.1.1 企业应建立身份鉴别机制，包括身份鉴别信息、复杂度要求、定期更换要求等，对登录涉密主机、涉密信息系统及数据库的用户进行身份鉴别，至少采用口令方式进行身份鉴别。

6.3.1.2 企业应设置涉密信息系统及安全防护软硬件系统口令规则，口令长度应至少8位以上，采用数字、大小写英文字母、特殊字符中两种或两种以上组合方式设置口令，口令中不得包含账号、生日等特殊信息。用户应对默认口令进行及时变更，口令应定期进行更换，普通用户口令更换时限不得长于6个月，管理用户口令更换时限不得长于3个月，对于未更换的用户应采用技术手段强制更换口令。

6.3.1.3 涉密信息系统及安全防护类软硬件系统应开启登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出、锁定账户等相关措施。

6.3.1.4 对于涉及核心商业秘密的主机、涉密信息系统应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

6.3.2 访问控制

6.3.2.1 企业应根据部门业务范围及员工岗位职责，对员工分配账户和权限，账户应保证唯一性，避免共享账户的存在。

6.3.2.2 涉密信息系统用户账号和权限的申请应建立审批程序，经批准后赋予用户对应的权限，权限应满足最小化原则。

6.3.2.3 企业应定期对账户信息进行清查，及时禁用、注销或删除离职人员账户、测试账户、临时账户等无用账户。

6.3.2.4 企业应根据服务器、涉密信息系统、安全防护软硬件系统的管理用户按照角色分配权限，管理用户授权应经过商业秘密信息化安全防护管理工作的职能部门批准，应授予管理用户所需的最小权限，实现管理用户的权限分离。

6.3.2.5 企业应建立主机端软件白名单或黑名单，采取必要的技术手段对主机的软件安装和使用进行控制。

6.3.2.6 企业应采用必要技术手段对主机端用户行为进行监控，对用户操作行为进行监控，对违规行为进行阻断。

6.3.2.7 对于涉及核心商业秘密的主机、涉密信息系统应采用加强访问控制，不可直接接入外部网络或由外部网络远程进行访问。

6.3.3 安全审计

6.3.3.1 企业应对各类涉密信息系统、安全防护软硬件系统日志和用户操作日志进行存档，保存时限不低于6个月。

6.3.3.2 企业应建立对于主机、应用、数据的安全审计规则，由审计管理员根据系统日志、用户操作日志对系统管理员、安全管理员及用户的操作行为等进行全面的审计，并形成审计记录，审计记录应进行存档备查。

6.3.4 入侵和恶意代码防范

6.3.4.1 企业应加强主机的管理，遵循最小安装的原则，仅安装需要的组件和应用程序，关闭不需要的系统服务、默认共享和高危端口。

6.3.4.2 企业应加强涉密信息系统、安全防护软硬件系统的管理，按照应用需要设置系统参数和策略，关闭不需要的功能组件、高危端口。

6.3.4.3 企业应在主机上安装必要的防病毒及防入侵软件，识别、记录、告警并处置各类入侵和病毒行为，有效的阻断病毒或恶意代码入侵。

6.3.4.4 企业应采用必要的技术防护手段定期对主机、各类涉密信息系统、安全防护软硬件系统进行漏洞扫描，对发现的漏洞进行评估后，采用合理的方式修复或防护漏洞。

6.3.5 数据完整性与保密性

6.3.5.1 企业应按照国家数据安全法律法规及标准规范要求，对各类数据进行分类分级，明确涉及商业秘密的数据的管控规则，对不同数据设定不同的授权访问机制，对于涉密数据的知悉范围和访问权限应满足最小化原则。

6.3.5.2 企业应采用符合国家标准要求的密码技术进行加密，保证涉及商业秘密的数据在产生、传输、存储等全生命周期的完整性与保密性，包括但不限于鉴别数据、业务数据、审计数据、配置数据、视频数据和个人信息等。

6.3.5.3 企业应采用必要的防泄漏技术手段进行管控，并应用数据脱敏技术将对外传递数据进行脱密处理。

6.3.6 数据备份恢复

6.3.6.1 企业应建立数据备份与恢复机制，包括备份方式、备份周期、存储介质、保存期限等。

6.3.6.2 企业应对所有商业秘密数据进行定期本地备份，并定期进行备份恢复测试，保证备份数据的及时性、可靠性、可用性，在异常情况下可有效恢复数据。

6.3.6.3 企业应根据数据的重要性和敏感性进行分类备份，并对备份数据进行分类管理。

6.3.6.4 对于涉及核心商业秘密的数据，企业应实行异地实时备份机制，利用网络将重要数据实时备份至备份场地。

6.3.7 剩余信息保护

企业应采用必要的技术手段或策略对鉴别信息及商业秘密数据所在的临时缓冲存储空间进行完全清除。

6.3.8 个人信息保护

企业对个人信息的收集、存储、使用、加工、传输、提供、公开、删除等活动，应按照《中华人民共和国个人信息保护法》等国家法律法规要求执行。

7 建设管理

7.1 安全方案设计

企业应制定商业秘密信息化安全防护体系规划和方案，组织内部或外部安全专家对规划和方案的合理性、适用性、合规性、经济型等进行论证和评审，最后经企业商业秘密信息化安全防护委员会批准后正式实施。

7.2 产品或服务的选择

7.2.1 企业应选择具备资质及技术能力的软硬件产品或服务供应商。

7.2.2 企业应按照国家法律法规、标准规范要求和行业发展趋势，结合企业实际业务需求，制定安全产品及服务供应商评价标准，建立软硬件产品或服务供应商目录，并定期对供应商进行评价。

7.2.3 企业所选择的软硬件产品或服务应获得国家许可或认证，且满足企业业务及安全基本要求。

7.2.4 企业采购软硬件产品或服务应进行必要的测试，可自行测试或委托集成单位进行专项测试，确定其符合企业业务及安全实际需求。

7.2.5 企业应与软硬件产品或服务供应商签订保密协议，明确双方的保密权利及义务。

7.3 软件开发

7.3.1 企业应建立软件开发管理制度，明确软件开发的立项、开发过程、测试、验收、上线等各环节的管理。

7.3.2企业应采用安全开发生命周期等方法，对软件开发全过程实施安全管理。

7.3.3 企业应在软件上线前，对软件进行功能和安全性测试，功能应满足业务需求，并对可能存在的恶意代码进行必要的检测。

7.3.4 企业应对软件程序的修改、更新、发布进行审批，并对软件版本进行控制。

7.3.5 对于外包软件开发，应由开发单位提供软件源代码，企业应从安全保密角度对软件中可能存在的后门和隐蔽信道等方面进行审查，识别可能存在的问题或潜在风险。

7.3.6 企业应对已完成开发的软件的业务符合性和安全性进行测试和验收，并形成测试和验收报告。

7.4 工程实施

企业应由专门的部门或人员负责工程实施过程的管理，也可委托第三方工程监理对项目的实施过程进行管理。

7.5 系统交付与验收

7.5.1 企业应按合同及技术协议对系统进行验收，包括对合同及技术协议内约定的设备、软件、文档、服务等进行清点，并对软件功能及安全性进行测试，软件验收应形成验收报告。

7.5.2　企业应组织供应商对负责运行维护的技术人员进行相应的技能培训。
7.5.3　企业在系统交付和验收完成后，应组织对技术防护体系进行重新评估。

8　运维管理

8.1　环境管理

企业应指定专门的部门或人员定期对数据中心或机房的供配电、空调、温湿度控制、消防等设施进行运行与维护管理。

8.2　资产管理

8.2.1企业应建立资产清单，包括资产基本信息、责任部门、责任人、重要程度、涉密等级和所处位置等内容，并及时进行更新。
8.2.2企业应根据资产的重要程度对资产进行标识管理，并采取合理的管理措施，对于涉密设备及涉密载体应加强管理。
8.2.3 涉密设备的销毁应履行审批程序，销毁应采用合理的技术手段清除涉及商业秘密的数据。

8.3　存储载体管理

8.3.1 企业应建立存储载体清单，包括载体基本信息、责任部门、责任人、重要程度、涉密等级和所处位置、保存期限等内容，并进行定期盘点与更新。
8.3.2 企业应将涉密载体存放在安全的环境中，采用合理技术或物理加密方式对涉密载体进行加密，由专人进行管理，对各类涉密载体使用、传递应进行登记记录。
8.3.3 涉密载体的销毁应履行审批程序，销毁应采用合理的技术手段清除涉及商业秘密的数据。

8.4　维护管理

8.4.1企业应建立系统、设备、网络维护的管理制度和操作规程，明确维护管理部门、人员、职责权限、维护流程、操作方法等。
8.4.2 企业维护管理部门应指定专门人员按照管理制度和操作规程要求对各种设备、线路等进行检查与维护管理，并对维护过程和结果进行监督。
8.4.3 企业应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
8.4.4 企业应规范运维工具的使用，指定运维工具的具体类别，远程运维应经过审批并使用指定远程工具软件进行运维。
8.4.5 企业如需将设备外送维修，应履行审批程序，并由专人送至具备相关安全资质的维修厂商或机构进行修复。
8.4.6 企业对于带有存储介质的设备，在该设备报废或重用前，应采用合理的技术手段清除涉及商业秘密的数据。

8.5　漏洞与隐患管理

8.5.1 企业应建立漏洞与隐患管理机制，对漏洞与隐患的发现、评估、处置、记录和跟踪等进行全过程进行规范、有效的管理。
8.5.2 企业应采取必要的技术措施识别各类安全漏洞和隐患，定期进行安全漏洞扫描，对发现的安全漏洞和隐患经评估后，进行合理的修补或处置。

8.6 升级管理

企业应定期或不定期对入侵、恶意代码、垃圾邮件、防病毒等技术防护软硬件系统进行升级，保证病毒、木马、恶意代码及垃圾邮件特征库的实时更新，以及对漏洞进行及时进行补丁升级。

8.7 配置管理

8.7.1 企业应建立网络及系统配置信息档案，记录和保存基本配置信息，包括网络拓扑结构、系统版本及补丁信息、系统参数配置信息、设备配置信息、系统安全策略等。
8.7.2 网络及系统配置信息变更应按照变更管理要求，履行相关程序后进行变更，并及时更新网络及系统配置信息档案。

8.8 变更管理

企业应建立系统或网络变更审批程序，所有系统或网络变更应制定变更方案，方案应进行可行性论证，并经过评审、审批后方可实施。

8.9 备份与恢复管理

8.9.1 企业应按照制定的备份与恢复机制，定期进行各类本地备份或异地备份，并按照需要进行恢复工作。
8.9.2 在备份和恢复过程中，从备份数据的安全性和完整性角度处罚，对备份数据进行加密、压缩和验证等处理。

8.10 外包运维管理

8.10.1 企业应选择具备资质和技术能力的外包运维服务商。
8.10.2企业应建立外包服务商评价机制，定期对外包服务商的技术能力、资质等进行评价。
8.10.3 企业应与外包运维服务商签订保密协议，明确双方的保密权利及义务。
8.10.4 企业应对外包运维服务商进行严格的权限管控，并做好外包运维人员行为审计和记录。

9 风险监测与评估

9.1 风险监测

企业应建立风险监测机制，采用必要的技术手段对商业秘密数据的全生命周期进行风险监测，及时处置存在的问题和潜在的风险。

9.2 风险评估

企业应采用自主或委托外部专业机构开展风险评估，采用技术手段对物理环境、网络、主机、应用、数据技术防护措施的有效性、可靠性进行检测，形成风险评估报告，并及时对存在的问题和潜在的风险进行整改。

10 安全事件处置与应急管理

10.1 安全事件处置

10.1.1 企业应制定安全事件处置管理制度，明确安全事件的管理职责，规范各类安全事件的报告、处置和响应流程。

10.1.2 企业应对安全事件进行调查，分析安全事件产生的原因，收集证据，记录处理过程，调查处置后应形成记录并进行存档。

10.1.3 企业应根据安全事件调查分析情况，制定改进措施，防止安全事件的再发。

10.2 应急预案管理

10.2.1 企业应建立应急预案，包括应急组织机构及人员分工、启动预案的条件、应急处置程序、应急资源保障、事后教育和培训等内容。

10.2.2 应急预案应经商业秘密信息化安全防护委员会审批后予以发布执行，并对应急预案的版本进行记录与控制。

10.2.3 企业应定期组织相关人员进行应急预案培训，并定期组织应急演练，并对演练过程和结果进行评价。

10.2.4 企业应定期对原有的应急预案进行评估，并根据需要对应急预案进行修订完善，修订后应进行审批与发布。

参 考 文 献

[1] 《中华人民共和国反不正当竞争法》
[2] 《中华人民共和国个人信息保护法》
[3] GB/T 22080 信息技术 安全技术 信息安全管理体系要求
[4] GB/T 22239 信息安全技术 网络安全等级保护基本要求
[5] GB/T 25058 信息安全技术 网络安全等级保护实施指南
[6] GB/T 29490 企业知识产权管理规范
[7] 《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》
[8]《中央企业商业秘密安全保护技术指引》