

 IMB standardization office【IMB 5AB- IMBK 08- IMB 2C】

网络数据和信息安全管理规范

**XXXX有限公司**

**WHB-08**

**网络数据和信息安全管理规范**

 **版本号: A/0**

**编制人： XXX**

**审核人： XXX**

**批准人： XXX**

**20XX年X月X日发布 20XX年X月X日实施**

**目的**

计算机网络为公司局域网提供网络基础平台服务和互联网接入服务。为保证公司计算机信息及网络能够安全可靠的运行，充分发挥信息服务方面的重要作用，更好的为公司运营提供服务，依据国家有关法律、法规的规定，结合公司实际情况制定本规定。

**术语**

本规范中的名词术语（比如“计算机信息安全”等）符合国家以及行业的相关规定。

计算机信息安全是指防止信息财产被故意的或偶然的非授权泄露、更改、破坏或使信息被非法系统辨识，控制。即确保信息的完整性、保密性、可用性和可控性。包括操作系统安全、数据库安全、病毒防护、访问权限控制、加密与鉴别等七个方面。

狭义上的计算机信息安全，是指防止有害信息在计算机网络上的传播和扩散，防止计算机网络上处理、传输、存储的数据资料的失窃和毁坏，防止内部人员利用计算机网络制作、传播有害信息和进行其他违法犯罪活动。

网络安全，是指保护计算机网络的正常运行，防止网络被入侵、攻击等，保证合法用户对网络资源的正常访问和对网络服务的正常使用。

计算机及网络安全员，是指从事的保障计算机信息及网络安全工作的人员。

普通用户，是指除了计算机及网络安全员之外的所有在物理或者逻辑上能够访问到互联网、企业计算机网及各应用系统的公司内部员工。

主机系统，指包含服务器、工作站、个人计算机在内的所有计算机系统。本规定所称的重要主机系统指生产、办公用的Web服务器、Email服务器、DNS服务器、OA服务器、企业运营管理支撑系统服务器、文件服务器、各主机系统等。

网络服务，包含通过开放端口提供的网络服务，如WWW、Email、FTP、Telnet、DNS等。

有害信息，参见国家现在法律法规的定义。

重大计算机信息安全事件，是指公司对外网站（电子公告板等）上出现有害信息；有害信息通过Email及其他途径大面积传播或已造成较大社会影响；计算机病毒的蔓延；重要文件、数据、资料被删除、篡改、窃取；由安全问题引起的系统崩溃、网络部分或全部瘫痪、网络服务部分或全部中断；系统被入侵；页面被非法替换或者修改；主机房及设备被人为破坏；重要计算机设备被盗窃等事件。

**组织架构及职责分工**

公司设立计算机信息及网络安全领导小组，作为公司计算机信息安全工作的领导机构，统一归口负责外部部门（政府和其他部门）有关计算机信息安全工作和特定事件的处理。

计算机信息及网络安全领导小组负责领导、检查、督促、制定信息安全策略、规章制度和措施，加强计算机信息安全工作的管理和指导，落实国家有关计算机信息安全的法律、法规和上级有关规定，保障公司的计算机信息的安全。

计算机信息及网络安全工作实行“谁主管，谁负责”的原则，各部门负责人对本部门计算机信息及网络安全负直接责任。

各部门必须配备由计算机技术人员担任本部门的计算机及网络安全员，并报公司计算机信息及网络安全领导小组备案。各部门计算机及网络安全员负责本部门计算机信息及网络安全的技术规划和安全措施的具体实施和落实。

相关岗位信息安全职责：

1）负责本部门计算机信息及网络安全工作的具体实施，及时掌握和处理有关信息安全问题。

2）定期或不定期检测本部门计算机信息及网络安全情况，发现安全漏洞和隐患及时报告，并提出整改意见、建议和技术措施。

3）指导和监督、检查本部门员工在计算机信息安全防护、数据保护及账号、口令设置使用的情况。

4）发现计算机信息安全问题，及时处理，保护现场，追查原因，并报部门计算机信息安全领导小组。

5）定期分析计算机安全系统日志，并作相应处理。

6）验证本部门重要数据保护对象的安全控制方法和措施的有效性，对于不符合安全控制要求的提出技术整改措施，对本部门的数据备份策略进行验证并实施。

7）负责所管理的计算机主机系统及网络设备的安全管理和安全设置工作。

8）负责所管理计算机主机系统和网络设备的用户账号及授权管理。

9）定期分析操作系统日志,定期或不定期检查系统进程，在发现异常的系统进程或者系统进程数量的异常变化要及时进行处理。

10）负责指导并督促用户设置高安全性的账号口令和安全日志。

11）进行计算机信息安全事件的排除和修复，包括操作系统、应用系统、文件的恢复以及安全漏洞的修补。

12）在正常的系统升级后，对系统重新进行安全设置，并对系统进行技术安全检查。

13）根据上级和本级计算机信息安全领导的要求，按照规定的流程进行系统升级或安全补丁程序的安装。

14）管理本部门的计算机网络服务和相应端口，并进行登记备案和实施技术安全管理。

15）根据数据备份策略，完成所管理系统数据的备份、备份介质保管、数据恢复工作。

1）自觉遵守计算机信息及网络安全的法律、法规和规定。

2）负责所使用个人计算机设备及数据和业务系统账号的安全。

3）发现本部门计算机网存在的安全隐患及安全事件，及时报告部门计算机管理部门。

4）不得擅自安装、维护公司所有网络设备（包括路由器、交换机、集线器、光纤、网线），不得私自接入网络。

各部门应保持计算机及网络安全员的相对稳定，并加强对计算机及网络安全员的教育和技术培训。在计算机及网络安全员调动、离职或者其他原因离开原岗位时，应将其涉及的用户账号和权限及时进行变更或注销。

 **系统安全规定**

公司计算机机房由计算机管理部门负责管理，并建立出入登记和审批制度。携带计算机设备及磁盘等存储介质进、出主机房，应经主管部门同意，并由机房管理人员进行核查登记。

各部门计算机管理部门应指定专人负责本部门计算机设备的管理，做好计算机设备的增添、维修、调拨等的审核与管理。计算机设备维修特别是需离场维修或承包给企业外部人员维护、维修时，应核实该设备中是否存储有涉及企业秘密、不宜公开的内部资料和账号、密码等，如有应采取拆卸硬盘、有效删除有关资料等有效措施，防止泄密。

使用、操作计算机设备时，应遵循以下安全要求：

1）保管好自己使用或所负责保管计算机设备的账号、口令，并不定期更换口令，不得转借、转让账号。

2）不安装和使用来历不明、没有版权的软件，对于外来的软件、数据文件等，必须先经病毒检测，确认无感染、携带病毒后方可使用。

3）不在个人使用的计算机上安装与工作无关的软件。

4）不擅自更改设备的IP地址及网络拓扑结构及软、硬件配置。

5）在存储有重要数据的计算机上，应设置开机密码、屏幕保护密码。

6）在个人计算机上安装防病毒软件，并开启实时病毒监测功能，及时升级病毒库和软件。

7）非经计算机管理部门的有效许可，不得对网络进行安全（漏洞）扫描和对账号、口令及数据包进行侦听；不得利用网络服务实施网络攻击、散布病毒和发布有害信息。在网络设备及主机系统进行操作还应该遵循有关网络安全规定。

 **账号管理安全**

账号的设置必须遵循“唯一性、必要性、最小授权”的原则。

唯一性原则是指每个账号对应一个用户，不允许多人共同拥有同一账号。

必要性原则是指账号的建立和分配应根据工作的必要性进行分配，不能根据个人需要、职位进行分配，禁止与所管理主机系统无关的人员在系统上拥有用户账号，要根据工作变动及时关闭不需要的系统账号。

最小授权原则是指对账号的权限应进行严格限制，其权限不能大于其工作、业务需要。超出正常权限范围的，要经主管领导审批。

系统中所有的用户（包括超级权限用户和普通用户）必须登记备案，并定期审阅。

严禁用户将自己所拥有的用户账号转借他人使用。

员工发生工作变动，必须重新审核其账号的必要性和权限，及时取消非必要的账号和调整账号权限；如员工离开本部门，须立即取消其账号。

在本部门每个应用系统、网络工程验收后，应立即删除系统中所有的测试账号和临时账号，对需要保留的账号口令重新进行设置。

系统管理员必须定期对系统上的账号及使用情况进行审核，发现可疑用户账号时及时核实并作相应的处理，对长期不用的用户账号进行锁定。

 一般情况下不允许外部人员直接进入主机系统进行操作。在特殊情况下（如系统维修、升级等）外部人员需要进入系统操作，必须由系统管理员进行登录，并对操作过程进行记录备案。禁止将系统用户及口令直接交给外部人员。

 **口令安全管理**

口令的选取、组成、长度、修改周期应符合安全规定。禁止使用名字、姓氏、电话号码、生日等容易猜测的字符串作为口令，也不要使用单个单词作为口令，在口令组成上必须包含大小写字母、数字、标点等不同的字符组合，口令长度要求在8位以上。

重要的主机系统，要求至少每个月修改口令，对于管理用的工作站和个人计算机，要求至少每两个月修改口令。

重要的主机系统应逐步采用一次性口令及其它可靠的身份认证技术。

本地保存的用户口令应加密存放，防止用户口令泄密。

**软件安全管理：**

不安装和使用来历不明、没有版权的软件。

不得在重要的主机系统上安装测试版的软件。

开发、修改应用系统时，要充分考虑系统安全和数据安全，从数据的采集、传输、处理、存贮，访问控制等方面进行论证，测试、验收时也必须进行相应的安全性能测试、验收。

操作系统和应用软件应根据其本身存在的安全漏洞及时进行必须的安全设置、升级和打安全补丁。

个人计算机上不得安装与工作无关的软件。在服务器系统上禁止安装与服务器所提供服务和应用无关的其它软件。

系统设备和应用软件的登录提示应对可能的攻击尝试、非授权访问提出警告。

主机系统的服务器、工作站所使用的操作系统必须进行登记。登记记录上应该标明厂家、操作系统版本、已安装的补丁程序号、安装和升级的时间等内容，并进行存档保存。

重要的主机系统在系统启用、重新安装或者升级时应建立系统镜像，在发生网络安全问题时利用系统镜像对系统进行完整性检查。

服务器、网络设备、计算机安全系统（如防火墙、入侵检测系统等）等应具备日志功能并必须启用。网络信息安全管理员要定期分析网络安全系统和操作系统日志，在发现系统遭受攻击或者攻击尝试时采取安全措施进行保护，对网络攻击或者攻击尝试进行定位、跟踪并发出警告，并向网络信息安全领导小组报告。系统日志必须保存三个月以上。

新建计算机网络、应用系统必须同时进行网络信息安全的设计。

 **互联网信息安全**

公司对外网站、需定期做安全检查，并设置好相关的信息发布、管理权限，防止有害信息传播。

各部门搭建的电子邮件系统，禁止开启匿名转发功能，并应按有关规定从技术、管理上采取有效措施过滤垃圾电子邮件及有害信息。

**数据安全**

需要保护的重要数据至少包括：

1）重要文件、资料、图纸（电子版）。

2）财会系统数据库。

3）重要主机系统的系统数据。

4）其他重要数据。

各部门计算机管理部门应制定数据备份策略及重要数据灾难恢复计划，及时做好数据备份及恢复。

对数据备份必须有明确的记录，在记录中标明备份内容、备份时间，备份操作人员等信息。对于重要数据的备份必须异地存放，并做好相关的异地备份记录。

各部门必须每年至少进行一次数据备份策略的有效性的验证，对数据恢复过程进行试验，确保在发生安全问题时能够从数据备份中进行恢复。

各部门计算机管理部门应对所管理系统上存储的数据进行登记备案，登记的内容主要包括：需要保护的数据、存储的位置、存储的形式、安全控制的方法和措施、负责安全管理和日常备份的人员、可以访问数据的用户、访问的方式以及权限。

涉及企业秘密及具有高保密性要求（如口令文件）的数据在传输、存贮时应加密。

禁止在没有采用安全保护机制的计算机上存储重要数据，在存储重要数据的计算机至少应该有开机口令、登录口令、数据库口令、屏幕保护等防护措施。禁止在个人计算机上存放重要数据。

不得以软盘或者笔记本电脑等形式将重要数据带出系统。如确实必需，须将数据用安全可靠的加密手段加密存储，并将存储的软盘或笔记本电脑比照密级文件管理。

**安全管理**

各部门必须对本部门的计算机信息及网络安全进行经常性的检查、检测：

1）系统安全检查应每月检查、检测一次；

2）计算机病毒防治应每月至少全面检查一次；

3）数据备份应每月检查一次。

检查发现计算机信息及网络安全隐患，应组织安全隐患整治，不能马上整治的，应采取有效措施预防网络信息安全事件和案件的发生。

发生计算机信息及网络安全事件，应马上组织人员妥善处理，防止扩散影响。触犯刑律的，应保存证据，报告公安机关，并配合查处。

发生重大计算机信息及网络安全事件须在24小时内上报。

各部门应对用户及本部门员工进行网络信息安全宣传，宣传有关国家法律、法规和网络信息安全知识，加强用户的法律意识和安全意识，不得从事任何危害网络信息安全的行为。

 **顾客网络信息安全**

 维护人员不得将顾客系统的密码泄露给他人。

 维护人员因工作原因进入顾客系统是，不得复制、删除、修改顾客信息。

 进入顾客系统应使用专用计算机，该计算机应每周进行杀毒，以防将病毒传入顾客系统。

 维护人员的客户端应及时升级或更新，确保其与顾客系统的版本保持一致。