涉密信息系统集成资质保密标准

1 适用范围

本保密标准适用于涉密信息系统集成资质申请、审查与资质单位日常保密管理。

2 定义

2.1 本标准所称涉密人员，是指由于工作需要，在涉密信息系统集成岗位合法接触、知悉和经管国家秘密事项的人员。

2.2 本标准所称涉密载体，主要指以文字、数据、符号、图形、图像、声音等方式记载国家秘密信息的纸介质、磁介质、光盘等各类物品。磁介质载体包括计算机硬盘、软盘和录音带、录像带等。

2.3 本标准所称信息系统是指由计算机及其相关和配套设备、设施构成的，按照一定的应用目标和规则存储、处理、传输信息的系统或者网络。

2.4 本标准所称信息设备是指计算机及存储介质、打印机、传真机、复印机、扫描仪、照相机、摄像机等具有信息存储和处理功能的设备。

3 保密标准

3.1 保密标准实施原则

3.1.1 积极防范，突出重点，严格标准，依法管理。

3.1.2 业务工作谁主管，保密工作谁负责，保密责任落实到人。

3.1.3 具备健全的管理体系，保密管理与生产经营管理相融合。

3.1.4 开展保密风险评估与管理。

3.1.5 建立保密管理的持续改进机制。

3.2 保密组织机构及职责

3.2.1 保密工作领导小组

3.2.1.1 资质单位应当成立保密工作领导小组，为本单位保密工作领导机构。

甲级资质单位应当设置专职保密总监，保密总监为单位领导班子成员。

3.2.1.2 甲级资质单位保密工作领导小组由单位法定代表人（或主要负责人）、保密总监和有关部门主要负责人组成。组长由法定代表人（或主要负责人）担任，副组长由保密总监担任，保密工作领导小组各成员应当有明确的职责分工。

乙级资质单位保密工作领导小组由单位法定代表人（或主要负责人）、分管保密工作负责人和有关部门主要负责人组成。组长由法定代表人（或主要负责人）担任，副组长由分管保密工作负责人担任，保密工作领导小组各成员应当有明确的职责分工。

3.2.1.3 保密工作领导小组实行例会制度。例会应当组织学习党和国家保密工作方针政策及相关保密法律法规；研究部署、总结本单位的保密工作；解决保密工作中的重要问题。例会每年不少于**2**次，会议应当作记录并形成会议纪要。

3.2.1.4 法定代表人（或主要负责人）为本单位保密工作第一责任人，对本单位保密工作负全面责任，履行下列职责：

（**1**）保证国家相关保密法律法规在本单位贯彻落实；

（**2**）监督检查保密工作责任制的落实情况，解决保密工作中的重要问题；

（**3**）审核、签发单位保密管理制度；

（**4**）为保密工作提供人力、财力、物力等条件保障。

3.2.1.5 保密总监或者分管保密工作负责人对本单位保密工作负具体领导和监督责任，履行下列职责：

（**1**）组织制定单位保密管理制度、保密工作计划，审定保密工作总结；

（**2**）监督保密工作计划落实情况，组织保密检查；

（3）为保密管理办公室和保密管理人员履行职责提供保障。

3.2.1.6 涉密信息系统集成业务部门负责人对本部门的保密管理负直接领导责任，履行下列职责：

（1）严格按照工作需要，控制业务人员在工作中知悉涉密信息的范围和程度；

（2）组织开展保密风险评估，修订生产管理制度，优化业务流程，制定保密工作方案，落实保密风险防控措施；

（3）监督检查涉密信息系统集成业务管理和保密制度执行情况，督促业务人员履行保密职责；

（4）及时发现、研究解决保密管理中存在的问题。

3.2.2 保密管理办公室

3.2.2.1 资质单位应当设立保密管理办公室，为本单位的职能部门，负责人由中层以上管理人员担任。

甲级资质单位保密管理办公室应当为专门机构并配备专门的保密管理人员，乙级资质单位可指定有关机构承担保密管理办公室职能。

3.2.2.2 保密管理办公室负责本单位保密工作的日常管理，履行下列职责：

（1）组织落实保密工作领导小组的工作部署，提出工作建议，拟定工作计划、总结；

（2）制定、修订保密制度；

（3）参与单位各项管理制度的制定、修订工作；

（4）审查、确定保密要害部门部位，指导、监督保密设施设备的建设、使用和维护管理；

（5）组织开展保密宣传教育和培训；

（6）对涉密人员履行保密职责情况进行指导监督；

（7）对本单位各部门保密管理有关情况进行指导监督；

（8）组织开展保密检查，针对存在的问题提出整改意见，并督促落实；

（9）报告、配合查处泄密事件；

（10）管理保密工作档案；

（11）承办保密资质申请、延续、年度审查、事项变更登记等工作；

（12）承办保密工作领导小组交办的其他任务。

3.2.2.3 保密管理人员应当具备下列条件：

（1）具备良好的政治素质；

（2）熟悉保密法律法规，掌握保密知识技能，具有一定的管理能力；

（3）熟悉本单位业务工作和保密工作情况；

（4）通过保密行政管理部门组织的培训和考核。

3.3 保密制度

3.3.1 资质单位应当建立规范、操作性强的保密制度，并根据实际情况及时修订完善。保密制度的具体要求应当体现在单位相关管理制度和业务工作流程中。

3.3.2 保密制度包括以下主要方面：

（1）保密工作机构设置与职责；

（2）保密教育培训；

（3）涉密人员管理；

（4）涉密载体管理；

（5）信息系统、信息设备和保密设施设备管理；

（6）涉密信息系统集成场所等保密要害部位管理；

（7）涉密项目实施现场管理；

（8）保密监督检查；

（9）保密工作考核与奖惩；

（10）泄密事件报告与查处；

（11）保密风险评估与管理；

（12）资质证书使用与管理。

3.4 保密风险评估与管理

3.4.1 资质单位应当定期对系统集成业务、人员、资产、场所等主要管理活动进行保密风险评估。各业务部门应当按照业务流程对保密风险进行识别、分析和评估，提出具体防控措施。

3.4.2 资质单位应当将国家保密法规和标准要求、保密风险防控措施融入到管理制度和业务工作流程中，并建立相应的监督检查机制。

3.5 涉密人员管理

3.5.1 资质单位应当对从事涉密业务的人员进行审查，符合条件的方可将其确定为涉密人员。涉密人员应当通过保密教育培训，并签订保密承诺书后方能上岗。

3.5.2 涉密人员应当保守国家秘密，严格遵守各项保密规章制度，并符合以下基本条件：

（1）遵纪守法，具有良好的品行，无犯罪记录；

（2）资质单位正式职工，并在其他单位无兼职；

（3）社会关系清楚，本人及其配偶为中国境内公民。

3.5.3 涉密人员根据所在岗位涉密情况分为核心、重要、一般三个等级，实行分类管理。涉密等级发生变化时，应当履行审批程序。

3.5.4 资质单位与涉密人员签订的劳动合同或补充协议，应当包括以下内容：

（1）涉密人员的权利与义务；

（2）涉密人员应当遵守的保密纪律和有关限制性规定；

（3）因履行保密职责导致涉密人员利益受到损害，资质单位给予补偿的规定；

（4）涉密人员因违反保密规定而被无条件调离涉密岗位或给予辞退等处罚的规定；

（5）因认真履行保密职责，资质单位给予涉密人员奖励的规定；

（6）涉密人员应当遵守的其他有关事项。

3.5.5 资质单位应当将涉密人员基本情况和调整变动情况向所在地省、自治区、直辖市保密行政管理部门备案。

3.5.6 在岗涉密人员每年参加保密教育与保密知识、技能培训的时间不少于**10**个学时。

3.5.7 资质单位应当对在岗涉密人员进行定期考核评价。

3.5.8 资质单位应当向涉密人员发放保密补贴。

3.5.9 涉密人员离岗离职须经资质单位保密审查，签订保密承诺书，并按相关保密规定实行脱密期管理。

3.5.10 涉密人员因私出国（境）的，应当经资质单位同意，出国（境）前应当经过保密教育。擅自出境或逾期不归的，资质单位应当及时报告保密行政管理部门。

3.5.11 涉密人员泄露国家秘密或严重违反保密规章制度的，应当调离涉密岗位，并追究其法律责任。

3.6 涉密载体管理

3.6.1 资质单位应当按照工作需要，严格控制涉密载体的接触范围和涉密信息的知悉程度。

3.6.2 资质单位应当建立涉密载体台帐，台帐应当包括载体名称、编号、密级、保密期限等信息。

3.6.3 接收、制作、交付、传递、保存、维修、销毁涉密载体，应当遵守国家相关保密规定，履行签收、登记、审批手续。

3.6.4 复制本单位产生的涉密载体，应当经单位相关部门审批；复制其他涉密载体，应当经涉密载体制发机关、单位或所在地省、自治区、直辖市保密行政管理部门批准。涉密载体复制场所应当符合保密要求，采取可靠的保密措施；不具备复制条件的，应当到保密行政管理部门审查批准的定点单位复制。

3.6.5 机密、秘密级涉密载体应当存放在密码文件柜中，绝密级涉密载体应当存放在密码保险柜中。存放场所应当符合保密要求。

3.6.6 未经批准，个人不得私自留存涉密载体和涉密信息资料。确因工作需要保存的，应当建立个人台帐，内容包括载体密级、留存原因、审批部门或人员、留存期限等内容。

3.6.7 携带涉密载体外出，应当履行审批手续，采取可靠的保密措施，并确保涉密载体始终处于携带人的有效控制下。

3.6.8 资质单位应当定期对涉密载体进行清查。需要销

毁的涉密载体应当履行清点、登记、审批手续，送交保密行政管理部门设立的销毁工作机构或者保密行政管理部门指定的单位销毁；确因工作需要，自行销毁少量秘密载体的，应当使用符合国家保密标准的销毁设备和方法。

3.7 信息系统与信息设备管理

3.7.1 涉密信息系统的规划、建设、使用等应当符合国家有关保密规定。涉密信息系统应当按照国家保密规定和标准，制定分级保护方案，采取身份鉴别、访问控制、安全审计、边界安全防护、信息流转控制等安全保密防护措施。

3.7.2 涉密信息设备应当符合国家保密标准，有密级、编号、责任人标识，并建立管理台帐。

3.7.3 涉密计算机、移动存储介质应当按照存储、处理信息的最高密级进行管理与防护。

3.7.4 涉密信息设备的使用应当符合相关保密规定。禁止涉密信息设备接入互联网及其他公共信息网络；禁止涉密信息设备接入内部非涉密信息系统；禁止使用非涉密信息设备和个人设备存储、处理涉密信息；禁止超越计算机、移动存储介质的涉密等级存储、处理涉密信息；禁止在涉密计算机和非涉密计算机之间交叉使用移动存储介质；禁止在涉密计算机与非涉密计算机之间共用打印机、扫描仪等信息设备。

3.7.5 涉密信息设备应当采取身份鉴别、访问控制、违

规外联监控、安全审计、移动存储介质管控等安全保密措施，并及时升级病毒和恶意代码样本库，定期进行病毒和恶意代码查杀。

3.7.6 采购安全保密产品应当选用经过国家保密行政管理部门授权机构检测、符合国家保密标准要求的产品，计算机病毒防护产品应当选用公安机关批准的国产产品，密码产品应当选用国家密码管理部门批准的产品。

3.7.7 涉密信息打印、刻录等输出应当相对集中、有效控制，并采取相应审计措施。

3.7.8 涉密计算机及办公自动化设备应当拆除具有无线联网功能的硬件模块，禁止使用具有无线互联功能或配备无线键盘、无线鼠标等无线外围装置的信息设备处理国家秘密。

3.7.9 涉密信息设备的维修，应当在本单位内部进行，并指定专人全程监督，严禁维修人员读取或复制涉密信息。确需送外维修的，须拆除涉密信息存储部件。涉密存储介质的数据恢复应当到国家保密行政管理部门批准的单位进行。

3.7.10 涉密信息设备改作非涉密信息设备使用或淘汰处理时，应当将涉密信息存储部件拆除。淘汰处理涉密存储介质和涉密信息存储部件，应当按照国家秘密载体销毁有关规定执行。

3.7.11 涉密计算机及移动存储介质携带外出应履行审

批手续，带出前和带回后，均应当进行保密检查。

3.8 涉密办公场所保密管理

3.8.1 资质单位的涉密办公场所应当固定在相对独立的楼层或区域。

3.8.2 涉密办公场所应当安装门禁、视频监控、防盗报警等安防系统，实行封闭式管理。监控机房应当安排人员值守。

3.8.3 建立视频监控的管理检查机制，资质单位安全保卫部门应当定期对视频监控信息进行回看检查，保密管理办公室应当对执行情况进行监督。视频监控信息保存时间不少于 **3** 个月。

3.8.4 门禁系统、视频监控系统和防盗报警系统等应当定期检查维护，确保系统处于有效工作状态。

3.8.5 涉密办公场所应当明确允许进入的人员范围，其他人员进入，应当履行审批、登记手续，并由接待人员全程陪同。

3.8.6 未经批准，不得将具有录音、录像、拍照、存储、通信功能的设备带入涉密办公场所。

3.9 涉密信息系统集成项目管理

3.9.1 资质单位应当按照资质等级、类别承接涉密信息系统集成业务。不得将资质证书出借或转让。不得将承接的

涉密信息系统集成业务分包或转包给不具备相应资质的单位。

3.9.2 资质单位与其他单位合作开展涉密信息系统集成业务的，合作单位应当具有相应涉密信息系统集成资质，且应当取得委托方书面同意。

3.9.3 资质单位承接涉密信息系统集成项目的，应当在签订合同后，向项目所在地省、自治区、直辖市保密行政管理部门备案，接受保密监督管理。

涉密信息系统集成项目完成后，资质单位应当向项目所在地省、自治区、直辖市保密行政管理部门书面报告项目建设情况。

3.9.4 资质单位应当对涉密信息系统集成项目实行全过程管理，明确岗位责任，落实各环节安全保密措施，确保管理全程可控可查。

3.9.5 资质单位应当按照涉密信息系统集成项目的密级，对用户需求文档、设计方案、图纸、程序编码等技术资料和项目合同书、保密协议、验收报告等业务资料是否属于国家秘密或者属于何种密级进行确定。属于国家秘密的，应当标明密级，登记编号，明确知悉范围。

3.9.6 涉密信息系统集成项目实施期间，项目负责人对项目的安全保密负总体责任，应当按照工作需要，严格控制

涉密载体的接触范围和涉密信息的知悉程度。

3.9.7 资质单位应当对参与涉密信息系统集成项目的管理人员、技术人员和工程施工人员进行登记备案，对其分工作出详细记录。

3.9.8 涉密信息系统集成项目实施验收后，资质单位应当将涉密技术资料全部移交委托方，不得私自留存或擅自处理。需要保留的业务资料，应当严格按照有关保密规定进行管理。

3.9.9 涉密信息系统集成项目的设计方案、研发成果及有关建设情况，资质单位及其工作人员不得擅自以任何形式公开发表、交流或转让。

3.9.10 资质单位在与境外人员或机构进行交流合作时，应当严格遵守有关保密规定，交流材料不得涉及涉密信息系统集成项目的相关情况。

3.9.11 资质单位利用涉密信息系统集成项目申请专利，应当严格遵守有关保密规定。

秘密级和机密级的项目，应当按照法定程序审批后申请保密专利，符合专利申请条件的，应当按照有关规定办理解密手续；绝密级的项目，在保密期限内不得申请专利或者保密专利。

3.10 涉密项目实施现场管理

3.10.1 资质单位进入委托方现场进行涉密信息系统集成项目开发、工程施工、运行维护等应当严格执行现场工作制度和流程。

3.10.2 从事现场项目开发、工程施工、运行维护的人员应当是资质单位确定的涉密人员。

3.10.3 现场项目开发、工程施工、运行维护应当在委托方的监督下进行。未经委托方检查和书面批准，不得将任何电子设备带入涉密项目现场。

3.10.4 资质单位应当对现场项目开发、工程施工、运行维护的工作情况进行详细记录并存档备查。

3.11 宣传报道管理

3.11.1 资质单位通过媒体、互联网等渠道对外发布信息，应当经资质单位相关部门审查批准。

3.11.2 资质单位涉及涉密信息系统集成项目的宣传报道、展览、公开发表著作和论文等，应当经委托方批准。

3.12 保密检查

3.12.1 资质单位应当定期对保密管理制度落实情况、技术防范措施落实情况等进行检查，及时发现和消除隐患。

3.12.2 保密检查应当进行书面记录，内容包括：检查时间、检查人、检查对象、检查事项、存在问题、整改措施及落实情况等。

3.13 泄密事件处理

3.13.1 资质单位发生泄密事件，应当立即采取补救措施，并在发现后**24**小时内书面向所在地保密行政管理部门报告。内容包括：

（**1**）所泄露信息的内容、密级、数量及其载体形式；

（**2**）泄密事件的发现经过；

（**3**）泄密事件发生的时间、地点和经过；

（**4**）泄密责任人的基本情况；

（**5**）泄密事件造成或可能造成的危害；

（**6**）已采取或拟采取的补救措施。

3.13.2 资质单位应当配合保密行政管理部门对泄密事件进行查处，不得隐瞒情况或包庇当事人。

3.14 保密工作考核与奖惩

3.14.1 资质单位应当将员工遵守保密制度、履行保密职责的情况纳入绩效考核内容，考核结果作为发放保密补贴和评选先进的依据。

3.14.2 资质单位应当对严格执行保密规章的集体和个人给予表彰奖励。

3.14.3 资质单位应当对违反保密法规制度的有关责任人给予相应处罚；泄露国家秘密的，应当按照有关规定作出处理。

3.15 保密工作经费

3.15.1 保密工作经费分为保密管理经费和保密专项经费。保密管理经费用于单位保密宣传教育培训、发放保密补贴、奖励保密先进、保密检查等日常保密管理工作；专项经费用于保密设施设备的建设、配备、维护等。

3.15.2 甲级资质单位保密管理经费，年度标准不少于 **5** 万元;乙级资质单位保密管理经费,年度标准不少于**3**万元。保密管理经费应当单独列入单位年度财务预算，专款专用，保证开支。

3.15.3 保密专项经费应当按实际需要予以保障。

3.16 保密工作档案

3.16.1 资质单位应当建立保密工作档案，记录日常保密工作情况。

3.16.2 保密工作档案的内容应当真实、完整，全面反映保密工作情况，并能够与相关工作档案相互印证。

本保密标准未明确涉密事项的保密管理，须严格执行国家有关保密规定。