天津市红桥区信用信息共享平台
安全建设管理制度
（试行）

第一章　安全建设管理要求

第一条 定级和备案要求

一、应以书面的形式说明保护对象的边界、安全保护等级及确定等级的方法和理由。

二、应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定。

三、应确保定级结果经过相关部门的批准。

四、应将材料报主管部门和相应公安机关。

第二条 安全方案设计要求

一、应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

二、应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，并形成配套文件。

三、应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后

才能正式实施。

第三条 产品采购和使用要求

一、应确保信息安全产品采购和使用符合国家的有关规定。

二、应确保产品采购和使用符合国家主管部门的要求。

三、应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

第四条 自行软件开发要求

一、应确保开发环境与实际运行环境物理分开，测试数据和测试结果受到控制。

二、应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。

三、应制定编写安全规范，要求开发人员参照规范编写。

四、应确保具备软件设计的相关文档和使用指南，并对文档使用进行控制。

五、应确保在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测。

六、应确保对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制。

七、应确保开发人员为专职人员，开发人员的开发活动

受到控制、监视和审查。

第五条 外包软件开发要求

一、应在软件交付前检测软件质量和其中可能存在的恶意代码。

二、应要求开发单位提供软件设计文档和使用指南。

三、应要求开发单位提供软件源，并审查软件中可能存在的和隐蔽信道。

第六条 工程实施要求

一、应指定或授权专门的部门或人员负责工程实施过程的管理。

二、应制订工程实施方案控制安全工程实施过程。

三、应通过第三方工程监理控制项目的实施过程。

第七条 测试验收要求

一、制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告。

二、应进行上线前的安全性测试，并出具安全测试报告。

第八条 系统交付要求

一、应制定交付清单，并根据交付清单对所交接的设备、

软件和文档等进行清点。

二、应对负责运行维护的技术人员进行相应的技能培训。

三、应确保提供建设过程中的文档和指导用户进行运行维护的文档。

第九条 等级测评要求

一、应定期进行，发现不符合相应标准要求的及时整改。

二、应在发生重大变更或级别发生变化时进行等级测评。

三、应选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

第十条 服务供应商选择要求

一、应确保服务供应商的选择符合国家的有关规定。

二、应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的信息安全相关义务。

三、应定期监视、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

第二章　安全建设管理措施

第十一条　定级和备案

制度是我国保证信息系统安全的重要手段，是在合规性管理的重要工作内容。信息系统定级和备案是开展等级保护

工作的重要内容，也是最先开展的环节，定级的准确性决定了信息系统在后续规划、设计和项目建设阶段是否全面、准确。因此，必须建立与等级保护相关的管理制度，要求信息系统的规划和建设者必须参照国家相关标准，以书面的形式准确地描述保护对象，包括其安全边界、信息资产、业务功能、安全保护等级，以及等级确定的方法和依据，并填写公安机关要求的其他备案材料。在完成材料准备后，应组织相关业务部门和外部安全技术专家对定级结果的合理性和准确性进行审定，如果有上级主管部门，还应当通过上级主管部门的审核，在按照专家和主管部门的审定意见完成备案材料的修订后，应将修改后的材料报主管部门和公安机关审查，完成备案。

第十二条　安全方案设计

确定信息系统的安全等级保护级别后，就唯一确定了一组针对该等级的控制措施，应该根据信息系统面临的风险和相应的安全措施，进行安全整体规划和安全方案的设计，并组织业务部门、上级部门和外部安全专家对设计方案进行评价审定。

第十三条　产品采购和使用

产品是落实控制措施的重要手段之一，如何采购到符合

组织需要的、符合国家相关部门标准的产品是非常重要的，一旦购买的产品不能满足信息安全保护的要求，可能会给相关业务系统带来严重损失。因此，必须按照项目管理的采购知识领域的要求，建立产品采购相关的制度，控制产品采购的过程。建议制定不同类型产品必须满足的资质级别要求，特别是商用密码产品必须满足国家密码主管部门的相关要求。在开始采购产品之前预先对产品的性能和功能进行测试，确保产品不存在性能虚标，可以满足项目建设的功能要求，产品本身的安全防护能力可以达到信息系统相同等级保护级别的要求；而产品的测试结果形成组织候选产品清单，并根据国家相关部门要求的变化及组织业务的需要定期审定和更新该产品清单。产品采购阶段应考虑:

（一）为了满足用户身份鉴别要求，需要确认厂商所宣称身份的信任级别。

（二）无论是业务用户、特权用户，他们的访问资源调配与授权过程应该是相同的。

（三）用户和操作员的权限及职责。

（四）资产需要达到的保护要求，包括但不限于可用性、保密性和完整性等。

（五）源自业务过程的要求，例如交易记录、监视和抗抵赖等。

（六）其他安全控制强制的要求，例如日志记录和监视

或数据泄露检测系统之间的接口。

如果购买产品，则需要遵循一个正式的测试和获取过程。与供应商签订的合同需要给出已确定的安全要求，如果推荐的产品的安全功能不能满足要求，在购买产品之前需要重新考虑引入的风险和相关控制措施。

第十四条　自行软件开发管理措施

软件源、测试数据和测试结果作为组织的重要资产，一旦泄露会导致非常严重的后果，因此必须建立软件开发相关的管理制度，明确开发环境的安全性要求，例如开发和测试环境要和生产环境物理隔离，从生产环境抽取的测试数据必须进行必要的脱敏工作；明确开发过程安全，例如开发过程中由谁负责的审核、由谁负责的安全性测试，并注意权限职责的分离；应明确编码安全规范，至少包含变量的命名、连接等临界资源的获取和释放、输入数据的过滤和数据流的控制、程序异常的处理等内容，必要时，对开发人员进行安全开发方面的培训；明确文档管理和版本控制，对开发过程中产生的设计文档、测试文档、使用文档等进行合理的分类分级，确定不同类型和级别的文档的阅读人员和访问权限，并注意这些文档和的更新等；明确开发人员的行为准则，包括职业道德、保密要求、BYOD 工作中个人设备的保护要求等。

安全开发是建立安全服务、安全架构、安全软件和系统

的必然要求。基于一个安全开发策略，以下方面需要充分考虑：

（一）开发环境安全。

（二）软件开发方法的安全。

（三）所使用编程语言的安全编码指南。

（四）设计阶段的安全要求。

（五）项目里程碑中的安全核查点。

（六）安全知识库。

（七）安全版本控制。

（八）所要求的应用安全知识。

（九）开发人员避免、发现和修复软件脆弱性的能力。

考虑制定安全编码标准并且强制使用，对开发人员进行代码开发、测试或评审标准的培训，并对标准落实情况进行控制和验证。

第十五条　外包软件开发管理措施

外包软件的开发过程不在组织的掌控之下，因此必须对软件质量和文档提出相关要求。例如要求开发商提供软件的源，进行，发现存在的方法误用、授权验证、数据验证、异常处理、加密等方面的问题，以及可能存在的软件。

外包软件开发时，在组织的整个外部供应链中，需要考虑下列要点：

（一）有关外包内容的许可证安排、代码所有权和知识产权。

（二）安全设计、编码和测试实践的合同要求。

（三）为外部开发者提供被认可的威胁模型。

（四）交付物质量和准确性的验收测试。

（五）用于建立安全和隐私质量最小化可接受级别（阈值）的证据的条款。

（六）已应用足够的测试来防止交付过程中有意或无意的恶意内容的证据的条款。

（七）已应用足够的测试来防止存在已知脆弱性的证据的条款。

（八）当开发出现重大问题时的处理措施，例如，如果源代码不可用时。

（九）审核开发过程和控制措施的合同权利。

（十）创建可交付使用的有效文档。

（十一）组织应确保自身可以实现验证控制措施有效的职责。

第十六条　工程实施管理措施

组织应建立工程实施相关的管理制度，明确工程实施管理的目的、要点和责任部门，包括安全建设工程实施的组织管理工作以及落实安全建设的责任部门和人员，保证建设资

金足额到位，选择符合要求的安全建设整改服务商，采购符合要求的信息安全产品，管理和控制安全功能开发、集成过程的质量等方面。并且为保证建设工程的安全和质量，信息系统安全建设工程可以实施监理。监理内容包括对工程实施前期安全性、采购外包安全性、工程实施过程安全性、系统环境安全性等方面的核查。

工程实施阶段的主要目的是将所有的模块（软硬件）集成为完整的系统，并且检查确认集成以后的系统符合要求。

本阶段应完成以下具体信息安全工作:

由授权或指定专职人员代表组织负责工程实施过程的管理；由工程实施单位根据具体项目情况制定详细的工程实施方案来控制实施过程，并监督工程实施单位认真执行安全工程过程；找出并描述实现安全方案后系统和模块的安全要求和限制，以及相关的系统验证机制及检查方法；完善系统的运行程序和全生命周期的安全计划，如密钥的分发等；对项目参与人员进行信息安全意识培训；对参加项目建设的安全管理和技术人员的安全职责落实情况进行检查。

安全建设整改工程实施的组织管理工作包括保证落实安全建设整改的责任部门和人员，保证建设资金足额到位，选择符合要求的安全建设整改服务商，采购符合要求的信息安全产品，管理和控制安全功能开发、集成过程的质量等方面。

第十七条 测试验收管理措施

组织应建立工程测试验收相关的管理制度，明确要求在测试验收前制定针对本次工程的测试验收方案，工程验收的内容包括全面检验工程项目所实现的安全功能，设备部署、安全配置等是否满足设计要求和安全规范，工程施工质量是否达到预期指标，工程档案资料是否齐全等方面，并形成测试验收报告和安全测试报告。在通过安全测评和试运行的基础上，组织业务、技术人员以及安全专家进行工程验收。

一般项目可按照以下三步骤进行项目测试验收工作。

（一）安全测试

安全测试阶段应制定测试大纲，在项目实施完成后，由组织和项目承接单位共同组织测试。对于第三级以上的应用系统整改建设，由组织委托第三方测试单位对系统进行安全性测试，并独立不受干扰地出具安全性测试报告。在测试大纲中应至少包括以下安全性测试和评估内容:

配置管理：系统开发单位应使用配置管理系统，并提供配置管理文档。

安装、生成和启动程序: 应制定安装、生成和启动程序，并保证最终产生了安全的配置。

安全功能测试：对系统的安全功能进行测试，以保证其符合详细设计并对详细设计进行检查，保证其符合概要设计以及总体安全方案。

系统管理员指南：应提供如何安全地管理系统和如何高效地利用系统安全功能和保护功能等详细准确的信息。

系统用户指南：必须包含两方面的内容：首先，它必须解释那些用户可见的安全功能的用途以及如何使用它们，这样用户可以持续有效地保护他们的信息；其次，它必须解释在维护系统安全时用户所能起的作用。

安全功能强度评估：功能强度分析应说明以概率或排列机制（如，口令字或哈希函数）实现的系统安全功能。例如，对口令机制的功能强度分析可以通过说明口令空间是否足够大来判断口令字功能是否满足强度要求。

脆弱性分析：应分析所采取的安全对策的完备性（安全对策是否可以满足所有的安全需求）以及安全对策之间的依赖关系。通常可以使用穿透性测试来评估上述内容，以判断它们在实际应用中是否会被利用来削弱系统的安全。

测试完成后，项目测试小组应提交安全测试报告，其中应包括安全性测试和评估的结果。不能通过安全性测试评估的，由测试小组提出修改意见，项目开发承担单位应做进一步修改。

（二）安全试运行

测试通过后，由项目应用单位组织进入试运行阶段，应有一系列的安全措施来维护系统安全，它包括处理系统在现场运行时的安全问题和采取措施保证系统的安全水平在系

统运行期间不会下降。具体工作如下:

监测系统的安全性能，包括事故报告；进行用户安全培训，并对培训进行总结；监视与安全有关的部件的变更或移除；监测新发现的对系统安全的攻击、系统所受威胁的变化以及其他与安全风险有关的因素；监测安全部件的备份支持，开展与系统安全有关的维护培训；评估系统改动对安全造成的影响；监测系统物理和功能配置，包括运行过程。在试运行情况报告中应对上述工作做总结性描述。

（三）测试验收

系统安全试运行过后，可以组织由项目开发承担单位和相关部门人员参加的项目验收组对项目进行验收。验收应增加以下安全内容:

项目是否已达到项目任务书中制定的总体安全目标和安全指标，实现全部安全功能；采用技术是否符合国家、行业有关安全技术标准及规范；是否实现验收测评的安全技术指标；项目建设过程中的各种文档资料是否规范、齐全。

在测试验收报告中也应在以下条目中反映对系统安全性验收的情况：项目设计总体安全目标及主要内容；项目采用的关键安全技术；验收专家组中的安全专家出具安全验收评价意见。

第十八条　系统交付管理措施

组织应建立系统交付相关的管理制度，明确系统建设完成后，项目承建方要向组织交付的内容，建议至少包括详细的系统交付清单、制定项目培训计划、系统建设的各类过程文档、系统运行维护的操作手册和帮助，并且系统交付过程文档必须有项目承建和组织双方项目负责人进行签字确认。

系统建设完成后，项目承建方要依据项目合同的交付部分向组织进行项目交付，交付的内容至少包括：制定详细的系统交付清单，对照系统交付清单，对交付的设备、软件和文档进行清点；制定项目培训计划，对系统人员进行技能培训，目标是经过培训的系统人员能胜任日常的工作；提供系统建设的各类过程文档，包括但不限于：实施方案、实施记录等；提供系统运行维护的帮助和操作手册；系统交付工作由组织、项目承建方共同参与，双方签字确认后，交付物交由组织方管理。

第十九条　等级测评

应结合等保的定级部分的要求建立相关等级保护测评的管理制度，明确信息系统按照国家相关部门的要求进行等级保护测评工作，一旦系统发生重大变更或保护级别变化时要重新进行测评工作。此外，还应当对备选的测评机构进行资质审查，形成候选测评机构清单，并根据国家相关部门要

求的变化及组织业务的需要定期审定和更新该清单。

第二十条 服务供应商选择管理措施

组织应建立服务供应商选择和管理相关的管理制度，明确系统集成商的资质要求，产品、系统或服务提供单位的工商管理要求，安全服务商的资质要求，人员的资质要求，与这些供应商需要签订安全责任合同书或保密协议等文档的内容。

为降低供应商访问组织资产带来的风险，需要与供应商协商并记录相关信息安全要求。

组织需要确定和授权特定说明的供应商，允许其访问组织策略中的信息安全控制措施信息。这些控制措施需要说明组织已实施的过程和规程，以及组织需要供应商实施的过程和规程，包括:

1）确定和记录允许访问组织信息的供应商类型，例如IT 服务、物流服务、金融服务、IT 基础组件服务等。

2）管理供应商关系的标准化过程和生命周期。

3)定义允许不同类型供应商访问信息的类型，监视和控制访问。

4）每种类型信息和访问的最小化安全要求作为单个供应商协议的基础，最小化信息安全要求基于组织的业务需求及其风险轮廓确定。

5）监视的过程和规程遵从为每种类型供应商及访问建立的信息安全要求，包括第三方评审和产品验证。

6）准确性和完整性控制以确保信息或由任何一方所提供信息处理的完整性。

7）为了保护组织信息，适用于供应商的业务类型。

8）处理供应商访问相关的事件或突发事件，涉及组织和供应商的职责。

9）如果必要，实施复原、恢复和应急计划确保任何一方所提供信息处理的可用性。

10）针对与供应商人员交互的组织人员开展意识培训，培训内容涉及基于供应商类型和供应商访问组织系统及信息级别的规则和行为。

11）在一定条件下，将信息安全要求和控制措施记录在双方签订的协议中。

12）为管理信息、信息处理设施及其他还需删除的信息设立必要过渡期，确保整个过渡期的信息安全。

需要建立供应商协议并文件化，以确保在组织和供应商之间关于双方要履行的信息安全相关义务不存在误解。

为满足识别的信息安全要求，需要考虑将下列条款包含在协议中：

1）被提供和访问信息的描述以及提供和访问信息的方法。

2）根据组织的分类方案进行信息分类，如果需要，则要将组织自身的分类方案和供应商的分类方案进行映射。

3）包括数据保护、知识产权和版权的法律、法规要求，并描述如何确保这些要求得到满足。

4）每个合同的合约方有义务执行一套已商定的控制措施，包括访问控制、性能评审、监视、报告和审核。

5）信息可接受的使用规则，如果需要也包括不可接受的使用规则。

6）授权访问或接收组织信息和规程的供应商人员列表及授权和撤销供应商人员访问或接收组织信息的条件。

7）合同具体约定的相关信息安全策略。

8）事件管理要求和规程（特别是故障修复期间的通告和合作）。

9）具体规程和信息安全要求的培训和意识要求，例如事件响应、授权规程等。

10）分包的相关规则，包括需要实施的控制措施。

11）相关协议方，包括处理信息安全问题的联系人。

12）如有对供应商人员的审查要求，包括实施审查的职责、审查未完成或审查结果引起疑问或关注的通知规程。

13）审核供应商协议相关过程和控制措施的权力。

14）缺陷和冲突的解决过程。

15）供应商有义务定期递交一份关于控制措施有效性的

独立报告，并且同意及时纠正报告中提及的问题。

16）供应商有义务遵从组织安全要求。