中国地质大学（北京）

信息网络中心文件

信息网络中心　　2020.9.21

中国地质大学（北京）系统建设管理规定

第一章　总则

第一条 为全面提升中国地质大学（北京）信息系统的安全性、可靠性和可用性，加强信息系统生产环境和测试环境的管理，加强业务系统的管理和维护，降低信息系统变更风险，特制定本制度。

第二条 本规定适用于中国地质大学（北京）所管署信息系统的定级备案、安全服务商选择、安全方案设计、产品采购和使用、开发管理、工程实施管理、测试管理和发布管理，系统交付管理以及业务系统的运行管理和维护；本制度规定了发生生产系统变更时，进行测试和发布的管理要求、职责与分工和操作步骤，以及业务系统上线后的管理和维护。

第二章　系统定级及备案

第三条 信息网络中心负责组织对中国地质大学（北京）所管署信息系统的定级备案工作。

第四条 信息网络中心与系统使用部门共同负责对信息系统进行等级保护定级工作，确定信息系统的边界，并编写相应的定级报告，组织相关业

务使用部门和安全技术专家对定级结果进行审定，经网络安全和信息化领导工作小组批准，将定级结果上报公安机关和主管部门备案。

第五条 新建信息系统，应在开发前对其进行定级备案工作，信息系统的立项申报处室负责所申报信息系统的业务实现和系统功能，应配合信息网络中心对申报信息系统的技术路线和安全体系架构确认，并编写网络安全等级保护定级报告；对于已经投入运行的信息系统，需要根据对业务系统的定级分析，编写网络安全等级保护定级报告，确定其安全需求，进行安全性建设。

第六条 系统备案管理应履行的职责

1. 系统定级、系统属性等材料由信息网络中心负责管理，并控制这些材料的使用；

2. 按相关要求将系统等级和系统属性等资料报系统主管部门备案；

3. 按相关要求将系统等级、系统属性、等级划分理由及其他要求的备案材料报相应公安机关备案。

第三章　安全服务商的选择

第七条 中国地质大学（北京）对信息系统进行安全建设时，对安全服务商的选择需遵循以下原则：

1. 确保安全服务商的选择符合国家的有关规定；

2. 与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

3. 确保选定的安全服务商提供技术培训和服务承诺，必要的应与其签订服务合同。

第四章　安全方案设计

第八条 信息网络中心定期组织开展对信息系统的风险评估工作，并根据风险评估的结果对安全策略和安全措施进行调整。

第九条 新建系统应由信息网络中心与系统使用部门共同组织完成其近期和远期的安全规划工作计划；根据等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件，并定期组织相关系统使用部门和安全技术专家对安全方案的合理性和正确性进行论证和审定，且需经过批准后的安全方案才能正式实施。

第十条 参照《信息系统等级测评管理规定》对信息系统进行等级测评，并根据测评结果调整和修订安全保障体系的文件。

第五章　产品的采购和使用

第十一条 中国地质大学（北京）的安全产品、密码产品的采购按照政府采购清单完成，原则上须使用国产产品，安全产品和密码产品的使用必须符合国家的有关规定。

第十二条 对于新建信息系统的设备采购和安全产品主要由信息网络中心提出采购需求，采购中须完成对产品的选型测试，确定产品的候选范围等；产品采购主要按照国家政府采购提供的采购清单进行。

第六章　自行软件开发管理规定

第十三条 开发的方法和管理必须规范化、合理化、制度化。

第十四条 开发人员必须为专职人员，开发活动则受到限制、监视和

审查。

第十五条 开发人员根据安全设计方案进行系统安全开发，确保开发环境、编码及系统流程控制的安全。

第十六条 开发环境安全管理要求：

1、软件系统开发、测试不得在生产环境中进行；

2、开发环境中所使用的操作系统、开发工具、数据库等必须是正版软件；

3、开发环境中的开发用机应进行统一安全配置，及时进行系统补丁升级和漏洞修复。

第十七条 编码安全要求：

1、以安全设计方案为基础，确保所有设计能够被代码实现，当设计发生变更时，必须修改相关代码；

2、需保证设计文档和代码一致性，当代码的修改已经造成设计更改时，必须修订相应设计文档。

3、编码过程中，需考虑注入、跨站脚本、失效的身份认证和会话管理、不安全的直接对象引用、跨站请求伪造、安全配置错误、不安全的加密存储、URL 访问限制缺失、没有足够的传输层防护和未验证的重定向和转发等十个方面安全威胁；

4、根据模块、函数/单元/进程的复杂度、规模和在软件系统中的重要程度，选择重要的代码进行正规检视。

第十八条 开发过程中应对阶段性开发成果进行有效管理。

第十九条 开发人员不得超越其规定权限进行开发，不得在程序中设置后门或恶意代码程序。

第二十条 软件开发团队组织安全性检测，测试内容应包括代码的安全测试和安全功能测试。代码的安全测试是指识别代码的安全脆弱性。安全功能测试主要包括身份认证和访问控制等功能性测试。

第二十一条 应有专门的测试人员编制安全测试方案，构造安全测试用例。不得由开发人员兼任。

第二十二条 测试系统环境应模拟生产环境，并与生产环境进行安全隔离。

第二十三条 业务数据不得直接在测试环境中使用。

第二十四条 应对源代码的变更和版本发布进行统一控制，对程序资源库的任何修改、更新和发布都需经软件开发团队负责人授权和批准。

第二十五条 应指定专人妥善保管程序源代码及相关技术文档，对于源代码与技术文档实行授权访问。

第二十六条 对软件设计要出具相应的文档和使用指南，并对文档使用进行控制。

第七章 外包软件开发管理规定

第二十七条 系统软件外包开发时，中国地质大学（北京）应与软件开发单位签订协议（如软件开发协议和软件开发安全协议），明确知识产权的归属和安全方面的要求，规范软件开发单位的责任、开发过程中的安全行为、开发环境要求、软件质量、开发后的服务承诺等内容。

第二十八条 应根据协议的要求检测软件质量（如验收测试等）。

第二十九条 在软件安装之前检测软件包中可能存在的恶意代码，并保留相应的检测报告。

第三十条 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

第八章 工程实施管理

第三十一条 指定或授权专门的人员，按照工程实施方案的要求对工程实施过程进行进度和质量控制。

第三十二条 在系统进行建设前，应要求系统建设方提供详细的工程实施方案，并定期对执行情况进行审查；根据具体的系统建设实施情况，制定工程实施管理制度，在制度中，明确实施过程的控制方法和人员行为准则。

第三十三条 工程实施责任部门应与工程实施单位签订与安全相关的协议（如工程安全建设协议），约束工程实施单位的工程实施行为。

第九章 测试验收管理规定

第三十四条 测试环境主要用于生产环境发布前进行的集成测试。

第三十五条 为确保测试环境和生产环境的一致性，测试终端和发布终端需分开设置，原则上不得同时进行两项测试或发布。

第三十六条 完成集成测试之后，需清除所有测试数据。

第三十七条 系统测试时应履行的职责：

1、专人负责系统测试的管理，对测试过程（包括测试前、测试中和测试后）进行文档化要求和制度化要求，并按照管理制度的要求完成系统测试工作；

2、根据系统要求委托第三方测试机构根据设计方案或合同要求对信息系统进行独立的安全性测试，包括配置核查、后门查杀、管理制度执行情况的安全性测试验收报告。

第三十八条 系统验收时应履行的职责：

1、验收前根据设计方案或合同要求等制订验收方案，验收过程中详细记录测试验收结果，形成验收报告；

2、组织相关人员，对系统测试验收报告进行审定，没有疑问后由双方签字。

第十章 系统交付管理

第三十九条 系统交付时应履行的职责：

1. 向各个系统使用部门明确系统的交接手续,并按照交接手续完成交接工作。

2. 制定详细的交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

3. 要求系统建设方对系统使用方运维技术人员进行培训。

4. 要求系统建设方提交系统建设过程中的文档（如系统建设方案）和指导用户进行系统运行维护的文档（如服务器操作规程书）以及系统培训手册等文档。

5. 系统建设方应进行服务承诺，并提交服务承诺书，确保对系统运行维护的支持。

第十一章 等级测评管理

第四十条 信息网络中心按照国家相关部门的要求对信息系统进行等级保护测评工作。

第四十一条 若系统安全保护级别发生变化,应及时调整级别并完成所涉及的整改工作，使其满足等级保护要求。

第四十二条 应选择具有国家相关技术资质和安全资质的测评单位对其信息系统进行等级测评，并签订保密协议。

第四十三条 要求实施等级测评的单位在测评工作实施之前，出具资质证明，并介绍工作流程、说明测评所需准备材料及配合要求，提交等级测评方案。

第四十四条 测评单位应就检查结果出具书面报告，并以纸质材料和电子文档形式提交信息网络中心。

第十二章 附则

第四十五条 本规定由中国地质大学(北京)信息网络中心负责解释。

第四十六条 本规定自发布之日起执行。