**雅砻江流域水电开发有限公司**

**数字档案馆系统安全与保密管理办法**

**2021年7月**

**雅砻江流域水电开发有限公司数字档案馆系统安全与保密管理办法**

1. 总 则
2. 为了规范雅砻江流域水电开发有限公司（以下简称“公司”）数字档案馆的建设、运行使用与运维管理，加强安全保密管控，确保国家秘密和公司商业秘密安全，根据《档案信息系统安全等级保护定级工作指南》（档办发〔2013〕5号）、《档案信息系统安全保护基本要求》（档办发〔2016〕1号）、《保密管理办法》（YLJ-GM-16）等要求，结合公司实际，制定本办法。
3. 本办法中的数字档案馆是指公司运用现代信息技术固化档案工作业务流程，对公司电子档案或其他数字资源进行收集、整理、保存，并通过网络提供档案信息服务和共享利用的集成管理系统平台。
4. 本办法主要以公司数字档案馆系统包含的基础设施、电子档案管理系统和数字档案资源为对象，从管理和技术方面对数字档案管理系统安全与保密工作提出具体要求。

本办法中的基础设施包含数字档案馆系统运行需要的机房、网络设施、硬件设备、基础软件和其他设施等。

1. 公司数字档案馆安全与保密工作实行积极防范、突出重点、依法管理的方针，坚持安全引领、管理科学、保障有力的原则，具体要求如下：

（一） 建立公司数字档案馆要树立“安全第一”的思想，不安全、宁不建，凡已建、必安全，要同步规划、同步建设、同步运行档案信息安全防护体系。

（二） 按照“谁运行谁管理、谁负责”的要求，建立数字档案馆系统安全管理机制，明确领导责任和岗位职责，以档案数据为核心，按照不同安全级别实行区别管理，以预防为主，制定应急预案，定期开展应急演练。

（三） 建立数字档案馆系统经费投入机制，配备数字档案馆系统安全管理人员，定期开展安全培训。

1. 公司数字档案馆安全等级保护为第三级，即监督保护级，除应满足《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239）安全等级保护三级要求以外，还应按照档案行业要求采取相应的安全保密防护措施。
2. 机构及职责
3. 公司保密领导小组是数字档案馆安全与保密工作的领导机构，主要职责如下：

（一）负责审定公司数字档案馆系统安全等级保护级别及等级变更事项。

（二）审核、签发公司数字档案馆系统安全保密策略与管理制度。

（三）审批公司数字档案馆系统平台的建设与废止申请。

（四）指导和处理公司数字档案馆系统的建设、使用、维护等过程中涉及保密工作的重大事项和重大安全事件。

（五）负责对公司数字档案馆系统“三员”进行任命。

1. 公司保密工作小组是数字档案馆系统安全与保密工作的管理机构，主要职责如下：

（一）负责监督公司数字档案馆系统的安全与保密管理工作。

（二）负责组织公司数字档案馆系统安全保密检查，并对违规行为进行处罚和整改检查。

（三）负责确定数字档案馆系统保护等级，组织编制定级报告，并向上级单位申请组织信息安全保护等级专家组进行评审工作，评审工作完成后，办理备案手续及等级变更工作。

（四）承办其他有关数字档案馆系统安全与保密工作事项。

1. 信息管理部是公司数字档案馆系统建设、运维工作具体实施部门，主要职责如下：

（一）负责公司编制数字档案馆系统安全保密策略、管理制度和操作规程等组成的安全保密管理体系文件。

（二）负责公司数字档案馆系统的规划、建设和运行维护管理工作，制定运行维护工作制度和操作规程，建立健全工作记录和日志文档，并妥善保存。

（三）负责组织数字档案馆系统安全审计和检查，组织开展系统安全风险评估，形成文档报保密办，并组织整改，不断优化完善系统安全保密防护体系。

（四）负责组织系统管理员、安全保密管理员和安全审计员（以下简称“三员”）开展数字档案馆系统的日常运行维护、安全策略的执行，对系统安全状态进行监控和系统故障处理，组织系统“三员”进行运维技术培训和保密培训。

（五）承办上级保密管理部门和本单位领导交办的其他数字档案馆系统安全与保密工作事项。

1. 档案室是数字档案管理系统业务归口部门，主要职责如下：

（一）参与数字档案馆系统规划、建设工作，提出档案业务需求。

（二）负责配合总经理工作部、信息管理部开展数字档案馆系统日常使用管理和安全保密管理工作，定期开展自查和整改。

（三）负责数字档案馆系统中全宗和人员增加、修改、删除等操作的审批及审核工作。

（四）负责数字档案馆中档案信息资源的导入、修改、删除等操作的管理和审核等工作。

（五）负责制定数字档案馆系统中档案信息资源利用范围和权限设置规则，控制数据访问权限。

（六）负责制定数字档案馆系统数据移交、接收和销毁等流程和规范。

（七）联合总经理工作部、信息管理部制定档案数据备份方案，负责档案数据的离线备份及离线备份载体的保管工作。

（八）承办上级保密管理部门和本单位领导交办的其他数字档案馆系统安全与保密工作事项。

1. 公司各部门负责配合信息管理部、档案室开展数字档案馆系统的建设、管理和运维和安全保密工作，主要职责如下：

（一）按照安全与保密要求，利用数字档案馆系统负责本部门档案数据的收集、整理和归档等工作。

（二）指定本部门专兼职档案员为本部门信息安全员，落实本规范和公司数字档案馆系统操作规程的有关事项。

（三）按照要求组织本部门人员进行数字档案馆系统使用培训和安全保密培训。

（四）承办上级保密管理部门和本单位领导交办的其他数字档案馆系统安全与保密工作事项。

1. 各二级单位是公司数字档案馆系统建设和管理的主要参与单位，负责本单位系统的安全与保密工作，主要职责如下：

（一）落实公司数字档案馆系统安全与保密办法，开展本单位系统使用培训和安全保密培训工作。

（二）负责制定本单位访问控制和档案数据权限规则，并按照规则严格执行。

（三）负责本单位档案数据离线备份及存储载体的安全与保密工作。

（四）负责开展本单位系统的保密检查工作，及时处理所发生的失泄密事件，对发生的失泄密事件进行查处，对泄露国家秘密和商业秘密采取补救措施，并及时向本单位保密委、主要负责人和上级保密工作管理部门报告。

（五）承办上级保密管理部门和本单位领导交办的其他数字档案馆系统安全与保密工作事项。

1. 管理员职责与基本要求
2. 公司数字档案馆系统应配备系统管理员、安全管理员和安全审计员，分别负责系统的运行维护、安全保密和安全审计相关工作，具体要求如下：

（一） 系统管理员至少配备一名专职人员，由信息管理部负责数字档案馆系统的运维人员担任，主要负责数字档案馆系统日常运行管理和维护，相关参数的制定、配置与监控管理。

（二） 安全管理员至少配备一名人员，由信息管理部或档案室档案人员担任，应为专职不可兼任，主要负责数字档案馆系统的安全策略、安全评估、用户权限设置等日常安全保密管理。

（三） 安全审计员至少配备一名人员，应由总经理工作部保密人员担任，主要负责对数字档案馆系统管理员、安全保密管理员的操作行为进行审计、跟踪、分析和监督检查，以便及时发现违规行为。

1. “三员”按照涉密人员管理，其配备和权限设置按照“相互独立、相互制约、最小授权”的原则，对承担的工作职责进行严格分工，管理员角色不得兼任，不可交叉替代。
2. “三员”不能以其他用户身份登陆系统，不能查看和修改任何业务数据库中的信息，不能删改日志内容。
3. “三员”应定期对数字档案馆系统进行审核和检查，主要工作如下：

（一）每月对数字档案馆系统进行常规检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

（二）应每年进行一次全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

（三）制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

1. 全宗和超出权限范围的档案数据的增加、删除、修改及相关参数的配置等操作应经过档案室领导审批后，系统管理员方可在系统内执行操作，审批记录应存档备查。
2. “三员”上岗前，应按公司保密办法履行人员审查程序，对被录用人员的身份、安全背景、专业资格或资质等进行审查，确保政治可靠，应当参加保密工作培训，具备岗位所要求的专业能力。一旦录用，被录用人应签署保密协议。
3. “三员”人员离岗应及时终止离岗人员数字档案馆系统所有访问权限，按照公司保密办法办理调离手续，并承诺调离后的保密义务后方可离开。“三员”人员信息及工作内容信息应至少保留一年以上。
4. 系统建设管理
5. 信息管理部和档案室共同负责数字档案馆系统的规划和建设管理工作，在方案设计、工程实施、系统测评、系统审批、日常管理、测评与检查、系统废止等阶段中，按照档案信息系统安全保护要求开展。
6. 总经理工作部负责数字档案馆系统明确数字档案馆系统的边界和安全保护等级，形成书面报告，报公司保密领导小组审核和批准，并组织有关安全技术专家对数字档案馆系统定级结果的合理性和正确性进行论证和审定。
7. 信息管理部对数字档案馆系统的安全建设进行总体规划，制定安全建设工作计划。
8. 公司数字档案馆系统厂商应将按照系统安全等级安全要求纳入系统建设方案中，经专家论证和审定，才能正式实施。
9. 公司电子档案管理系统开发单位应提供软件设计的相关文档、使用指南和软件源代码，审查软件中可能存在的后门，在软件安装之前检测软件包中可能存在的恶意代码。
10. 数字档案馆系统厂商应制定详细的实施方案、实施方面管理制度，明确说明实施过程控制方法和人员行为准则，经档案室、信息管理部审查通过后，方可实施。
11. 信息管理部负责数字档案馆系统工程实施过程的管理，档案室负责提供数字档案馆系统权限分配、各类参数设置等档案业务要求，监督、指导实施单位完成系统各类业务定制工作。
12. 数字档案馆系统实施完毕后，信息管理部应委托第三方测试单位对系统进行安全性测试，并出具安全性测试报告。对系统测试验收的控制方法和人员行为准则进行书面规定。
13. 公司成立系统验收小组负责数字档案馆系统测试验收工作和系统交付工作。数字档案馆系统承建单位应制定交付清单，并根据交付清单对所交接的设备、软件和文档进行清单，并对系统使用人员、专兼职档案人员进行相应的技能培训。
14. 系统运行管理
15. 公司数字档案馆系统运行维护工作由信息管理部和数字档案馆厂商共同负责，包括机房和办公环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、密码管理、备份与恢复管理、安全事件处置等，应按照《雅砻江流域水电开发有限公司档案信息系统运行维护管理办法》相关要求执行。
16. 档案数据存储介质应统一管理，建立采购、使用、检测和销毁的全过程记录，应根据介质存放情况由信息管理部和档案室分别保管。信息管理部负责存放在机房内的存储介质的管理，档案室负责档案数据离线存储介质的管理。
17. 存储介质需要销毁的，应按照《电子文件归档与电子档案管理实施细则》（YLJ-IM-28）、《档案管理规定》（YLJ-IM-15）要求执行，在送出销毁前对数据进行消除操作，并将待销毁介质编号登记，以便销毁时查对。
18. 档案数据需进行本地和异地备份，备份与恢复应按照《电子文件归档与电子档案管理实施细则》（YLJ-IM-28）要求执行，应规范备份信息的备份方式、备份频度、存储介质和保存期等。
19. 机房建设、网络安全管理
20. 信息管理部为数字档案馆系统及相关设备提供运行场所，机房建设和管理按照公司相关要求执行。
21. 数字档案馆系统网络架构、通信传输及可信验证应按照《信息安全技术 网络安全等级保护基本要求》（GB/T 22239）第三级安全要求建设和管理，保障系统网络技术安全。
22. 数字档案馆系统网络设备应封闭不需要的端口，关闭不需要的服务，建立网络设备运维、管理人员身份数据库，根据职责分配用户名，设置组合密码，分配访问权限。
23. 访问控制
24. 信息管理部负责制定访问安全控制策略，应包含并注意以下几点与用户身份标识和访问控制相关的内容：

（一）对数字档案馆系统的服务器、用户终端以及应用程序的系统登录进行用户身份鉴别，安全保密设备的配置操作等应进行用户身份鉴别。

（二）用户身份标识符由系统管理员统一生成，并确保身份标识在此系统生命周期中的唯一性；

（三）系统管理员应对系统内身份标识符加强管理、维护，确保身份标识符列表不被非授权地访问、修改和删除；用户标识符应与安全审计相关联，保证系统内安全事件的可核查性。

（四）对涉密信息、重要信息和主体进行分类分级并对主体访问涉密信息和重要信息采用分类分级的强制访问控制策略。

（五）应按照主体类别、客体类别进行涉密信息和重要信息的访问控制。涉密信息和重要信息的访问控制，主体应控制到单个用户，客体应控制到信息类别。

1. 数字档案馆系统管理员应根据管理用户的角色分配权限，仅授予管理用户所需要的最小权限。用户角色分为普通用户、档案管理员、领导三类，权限设置规则如下：

（一）普通用户具有查看公开、部门公开档案条目的权限，查阅不公开档案需按照《档案管理规定》（YLJ-IM-15）、《档案利用办法》（YLJ-IM-21）要求，经相关领导审批后可查阅。普通用户可在数字档案馆系统内增加数据，拥有对归档前本用户增加数据的修改、删除、归档、查阅的权限。

（二） 公司档案管理员角色具有查看本角色管理范围内公司电子档案管理系统内全部档案数据条目和电子档案的权限。具有对已归档档案数据进行审查和修改的权限。

（三） 领导角色具有查看业务主管部门或本部门档案数据条目和电子档案权限，具有审批档案数据利用流程权限。

1. 数字档案馆系统访问用户应以人力资源部正式下发或提供的人员名单为准，新增用户的访问权限设置和开通，应由本人申请，信息管理部审批，系统管理员负责开通。员工离职后，系统管理员应根据人力资源部提供的离职信息应及时删除账户。
2. 禁止单一账户多人使用，禁止使用默认账户及默认口令，账户密码应由字母、数字等组成，并定期更换。
3. 档案数据安全与保密
4. 涉密档案数据严禁上线。
5. 数字档案馆系统档案数据的输入输出方式主要包括：利用存储设备对电子档案拷贝输入输出；利用扫描仪等识别设备将纸介文件转换为电子文件输入；利用打印机将电子档案转换为纸质文件输出等。
6. 信息管理部负责档案数据输入输出环境的安全策略配置，档案数据导入过程中，须经过中间机进行计算机病毒、木马程序、恶意代码和间谍软件的查杀；中间机不允许处理与信息导入无关的业务工作，禁止进行除单向导入以外的任何导出操作。
7. 档案数据利用时应按照《档案利用办法》（YLJ-IM-21）要求，严格执行利用审批流程，档案数据在打印、刻录、拷贝等输出操作时，应当确保输出后的载体具有与源信息涉密等级相同的密级标志或同等安全等级标志。
8. 信息管理部、厂商应对系统内重要档案数据输出（如打印、拷贝、下载等）操作采取水印、限制利用次数等技术措施，进行严格控制。
9. 数字档案馆系统与其他安全等级系统或涉密系统互联互通时应经过公司总经理工作部审批并明确系统之间的边界划分、采取有效的边界防护和访问控制措施，防止超出系统安全等级数据流向系统。
10. 信息管理部负责对档案数据输入与输出行为开展日常审计检查和技术管控；总经理工作部负责档案数据输入与输出过程的保密监督检查，会同信息管理部定期开展检查；各部门负责本部门档案数据自查；对于信息输入与输出过程中发现的高密低出、审批不严、操作不合规等安全隐患和违规行为，按照公司保密办法有关要求进行处理。
11. 信息管理部负责对数字档案馆系统内传输和存储的涉密信息进行完整性检测，及时发现涉密信息被篡改、删除、插入等情况，并生成记录日志。在信息完整性校验中发现异常情况的应立即中止当前数据操作，并对异常信息进行重校验，若依然发生异常的，应按照应急响应管理相关要求执行应急响应处理。对完整性被破坏的信息采取有效的信息恢复补救措施，采取措施后，应对数据进行完整性检测。
12. 信息公开和发布
13. 档案室应通过公司数字档案馆系统或档案网站发布档案工作相关信息，公开符合规定的档案信息资源。
14. 档案信息公开和发布应坚持真实、可靠、及时、准确、服务公司及便于开展档案工作为原则。严禁发布影响或可能影响公司形象、利益的信息；严禁发布与公司无关的虚假、无效、过时信息。
15. 应充分利用公司档案信息发布形式，主动发布应当让公司员工知晓的各类信息，最大限度地为公司各类管理工作服务。
16. 公司发布的档案信息如下：

（一）档案工作法规规章、规范性文件及公司制定的各类档案规章制度、业务政策解读等;

（二）公司档案接收、利用、保管等业务统计数据；

（三）公司档案工作规划、年度计划、总结；

（四）公司及各子公司档案工作机构概况、领导班子、联系方式等；

（五）公司重要档案工作动态；

（六）根据库藏编制的可公开的各类档案专题、文件汇编；

（七）法律、法规、规章规定应当公开的其他档案信息。

1. 公司档案信息发布涉及下列内容的，不予发布：

（一）公司规定的秘密和法律、法规、规章规定的工作秘密；

（二）仍在保密期限内的国家秘密和商业秘密信息；

（三）保密期限届满但不适宜公开的国家秘密和商业秘密信息；

（四）依法受到保护的个人隐私；

（五）正在调查、讨论、审议过程中的档案信息公开后可能影响公司、个人利益的；

（六）法律、法规、规章规定不予向发布的其他档案信息。

1. 公司信息发布和公开应按照公司信息公开保密审查程序执行，任何人未经许可不得以公司的名义发布档案信息。
2. 信息发布不当的责任，按“谁批准谁负责，谁发布谁负责”的原则追究。
3. 附 则
4. 本办法由档案室、信息管理部负责解释和修订。
5. 本办法自印发之日起施行。