ICS 35.080
CCS L 70

团　　体　　标　　准

T/XXX XXXX—2024

自然资源应用系统安全日志规范

Specification for security logs of natural resource application systems

（征求意见稿）

广东省土地学会

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

广东省土地学会　　发 布

目　　次

广东省土地学会

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东省土地学会提出并归口。

本文件起草单位：广东省国土资源技术中心、广东省信息安全测评中心、数字广东网络建设有限公司、广州智臣信息科技有限公司。

本文件主要起草人：暂略。

广东省土地学会

自然资源应用系统安全日志规范

1 范围

本文件规定了自然资源应用系统日志设计、日志记录、日志存储、日志审计等相关要求。

本文件适用于自然资源应用系统相关的日志能力建设和日志管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GA/T 911-2010 信息安全技术 日志分析产品安全技术要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术—个人信息安全规范

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

日志 log

为保障应用系统的安全稳定运行而由应用系统在某种情况下按时间记录的有序数据集合，包括应系统运行、操作、故障等信息。

3.2

日志审计 log audit

对自然资源应用系统的运行（故障）、用户操作行为和接口服务等应用系统日志信息进行监测、采集及存储，以备倒查追踪。

3.3

运行 operation

应用系统启动、运行过程产生的事件。

3.4

接口服务 application programming interface

应用系统通过接口调用方式为其它应用系统提供数据资源共享的服务，包括但不限于数据服务目录接口、数据操作服务接口等。

3.5

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用就有可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：个人敏感信息包括公民身份号码、个人生物特征信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下(含)儿童的个人信息等。

注 2：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露，非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，也属于个人敏感信息。开展业务时产

广东省土地学会

生的用户的个人信息以及房产相关的信息等。
[来源:GB/T 35273-2020,3.2]

3.6

响应码 response status code
每类请求处理结果的状态码。

4 缩略语

下列缩略语适用于本文件。
UFT-8：8位元（Universal Character Set/Unicode Transformation Format）

5 设计要求

5.1 设计原则

在应用系统规划和设计前期，应根据应用系统具体的业务场景设计应用系统的日志记录方案，日志记录设计基本要求如下：

从网络安全和数据保护的角度出发，根据应用系统承载的业务数据设置合理的日志记录要求，包括但不限于以下原则：

——完整性：在保障应用系统稳定运行的前提下，日志记录应完整，采用国密校验算法定期验证日志完整性，并且确保日志不被非法篡改；
——机密性：日志记录中对于敏感信息应做脱敏处理、加密或通过适当访问权限控制，避免因日志分析导致业务敏感数据泄密；
——安全性：应对日志程序进行保护，防止非授权用户对日志程序进行强制停止、退出、删掉、重启等非法操作；
——可用性：日志应可供应用系统管理员定位故障问题、发现异常等，应每周进行一次全量备份日志，每年开展一次恢复测试，对备份日志有效性进行验证；
——分级分类：日志应分级分类分别记录；
——时效性：日志应被实时、有序记录，记录应及时，同时要确保日志、系统时间与 NTP 服务器同步；
——合规性：日志保留期限应满足法律法规要求。

5.2 内容要求

记录必要的程序执行过程和状态，以便于问题跟踪和排查、系统监控、流程恢复及数据分析参考等。由于业务场景不同，日志记录会有所不同，日志记录基本内容要求如下。

a) 支持应用系统运维。
   1) 监控告警：应反映系统运行状态；
   2) 问题定位：为快速、准确地定位线上问题提供足够数据支撑；
   3) 容量预警：反映应用系统性能瓶颈，预警系统潜在风险，为优化系统性能、或者根据日志信息调整系统行为等提供数据支撑。
b) 为业务流程回放、恢复等提供数据支撑。
c) 日志应当满足反映出安全攻击行为，如登录错误、异常访问等。

6 分类要求

根据日志数据的产生场景，分为系统类日志、业务类日志。

a) 系统类日志，包括应用系统运行日志和管理日志。
b) 业务类日志，一般包括用户行为日志、业务行为日志和接口服务调用日志。
c) 每一类日志记录中都应记录以下基本内容：
   1) 事件发生的日期和时间；

广东省土地学会

2） 事件发生的服务器信息，如机器 IP；
3） 事件定位信息，如事件发生的完整路径信息；
4） 事件描述；
5） 操作者信息(如有)；
6） 操作结果状态(如有)；
7） 事件级别。

7 分级要求

日志级别从高到低至少应分为五档，从高到低各日志各级别说明如下：

表 1 日志数据分级

级别值	说明
1	紧急（emergency）：该类错误可导致整个应用系统的功能无法使用，甚至导致应用系统瘫痪、关闭和退出等，如磁盘空间满或 I/O 负载高、数据库或储存连接失败等。
2	警报（alert）：该类错误可导致整个应用系统的超过一半的功能无法使用，不会影响系统本身运行，只对部分业务处理有影响。该级别表示虽然发生错误事件，但系统仍可正常运行，错误需尽快修复。一般用来记录程序中发生的异常错误信息，或者记录业务逻辑出错。例如请求超时、程序关闭、接口报错。记录该级别日志时，应包括异常发生的堆栈信息、详细的异常信息、异常发生的出处信息等。
3	警告（critical）：表明会出现潜在错误的情形，不影响应用系统正常运行，但需要引起注意的警告信息。比如内存或 CPU 不足、批量查询、导出数据、登录失败、程序重启、少部分功能无法使用等。
4	信息（info）：应用系统运行的关键时点的操作信息以及应用系统运行的关键步骤等信息，一般用于记录业务日志。这个级别记录了应用系统日常运转中产生的事件，但同时也应该有足够的信息以用于业务追踪、业务监控及异常排查等。比如程序启动、登录、退出、业务办理等。
5	调试（debug）：指出细粒度信息事件，用于程序调试和测试。调式信息主要便于开发人员进行错误分析和定位，一般记录一些运行中的细粒度的事件，比如记录某个操作具体步骤信息。

8 字符集要求

日志数据统一采用UFT-8字符集记录和存储。

9 传输要求

遵循RFC5426系统日志传输协议，通过SYSLOG或服务接口协议传输日志数据。

10 存储要求

应在保障日志数据安全前提下做好日志存储工作，日志的存储应满足下列条件：
——应将日志记录与业务数据逻辑隔离；
——日志保存的时限不应少于 6 个月，对已另有安全管理规定的日志存储工作，应遵守《互联网政务应用安全管理规定》《自然资源领域数据安全管理办法》等规定；
——涉及重要数据和核心数据的应用日志应采取加密机制保证日志数据保密性，加密机制应符合《GB/T 39786-2021 信息安全技术应用系统密码应用基本要求》；
——日志应采取校验机制进行日志数据完整性保护，保证日志数据完整性，校验机制应符合《GB/T 39786-2021 信息安全技术应用系统密码应用基本要求》；
——严格控制日志的访问权限，确保日志的授权访问；
——应具有使用 SQL 语句进行审计日志查询的功能，能够根据事件的主体、客体、类型、级别、时间和日期等属性进行查询；
——具备备份和恢复能力；
——与统一的标准时间源保持同步。

广东省土地学会

11 审计要求

各应用系统应指定专人定期开展日志审计，审计内容包括但不限于以下内容：
——应用系统日志的准确性、完整性、安全性情况；
——应用系统运行情况；
——安全保密员和系统管理员日常操作情况；
——重要用户行为、异常操作和重要系统命令的使用等情况。

广东省土地学会

附 录 A
（资料性）
日志内容及格式要求

A.1 运行日志

运行日志内容及格式见表A.1。

表 A.1 运行日志内容及格式

序号	名称	数据项标识	字段类型	长度	描述
1	记录标识	Id	长整型	32	用于唯一标识应用系统产生的日志数据中的一条记录，在日志记录产生时生成，其格式和产生方式由各应用系统系统自行决定。
2	运行状态	State	整数型	1	应用系统运行状态，0：启动；1：停止；2：重启。
3	程序名称	Mod	字符型	10	应用系统程序名称、线程名称。
4	时间	Date	字符型	14	日志产生的日志，采用格式YYYYMMDDhhmmss，24 小时制格式。
5	结果	Result	布尔型	1	用户管理操作的结果记录，包括成功/失败，1:成功；0：失败。
6	风险等级	Pri	整数型	1	日志风险等级，1：紧急；2：警报；3：警告；4：信息；5：调试。
7	类型	Logtype	整数型	1	日志类型，1：运行日志；2：管理日志；3：业务日志。

A.2 管理日志

管理日志内容及格式见表A.2。

表 A.2 管理日志内容及格式

序号	名称	数据项标识	字段类型	长度	描述
1	记录标识	Id	长整型	32	用于唯一标识应用系统产生的日志数据中的一条记录，在日志记录产生时生成，其格式和产生方式由各应用系统系统自行决定。
2	用户标识	User	字符型	10	应用系统管理员用户名。
3	客户端登录IP	From	可变长字符型	40	终端标识为 IP 地址。
4	操作类型	Type	整数型	1	管理员具体操作类型，0：登录；1：查询；2：新增；3：修改；4：删除；5：启动；6：停止；7：重启；8：导入；9：导出。
6	时间	Data	字符型	14	执行各类日志管理操作的时间，采用格式 YYYYMMDDhhmmss，24 小时制格式。
7	操作内容	Condition	可变长字符型	——	记录执行日志管理操作的 SQL 语句。

广东省土地学会

表 A.2 管理日志内容及格式（续）

序号	名称	数据项标识	字段类型	长度	描述
8	结果	Result	布尔型	1	用户管理操作的结果记录，包括成功/失败，1:成功；0：失败。
9	风险等级	Pri	整数型	1	日志风险等级，1：紧急；2：警报；3：警告；4：信息；5：调试。
10	类型	Logtype	整数型	1	日志类型，1：运行日志；2：管理日志；3：业务日志。

A.3 用户行为日志

用户行为日志内容及格式见表A.3。

表 A.3 用户行为日志内容及格式

序号	数据项名称	数据项标识	类型	长度	采用标准及说明
1	记录标识	Id	长整型	32	用于唯一标识应用系统产生的日志数据中的一条记录，在日志记录产生时生成，其格式和产生方式由各应用系统系统自行决定。
2	时间	Data	字符型	14	日志产生的日志，采用格式 YYYYMMDDhhmmss，24 小时制格式。
3	应用系统名称	Dname	可变长字符型	100	产生日志的应用系统名称，采用格式 XXX 或 XXX-xxx（XXX 表示平台名称，xxx 表示子系统名称）。
4	*单位名称	Organization	可变长字符型	100	用户所属单位的名称，省统建或跨单位使用的应用系统建议使用。
5	用户标识	Name	可变长字符型	30	用户登录操作时的名称，使用证书、粤政易、粤省事等方式进行身份鉴别的，记录用户真实姓名，使用应用系统自身的身份鉴别的，记录应用系统分配的用户名，其格式和产生方式由各应用系统系统自行决定。
6	客户端登录 IP	From	可变长字符型	40	用户操作时所使用的信息处理终端的 IP,填写其网络 IP 地址，如：19.16.240.5。
7	客户端代理 IP	Client_Http_Proxy	可变长字符型	40	客户端 HTTP 代理列表(x_forwarded_for)。
8	客户端请求操作时间	Client_Rq_Time	字符型	14	用户请求时的系统日期时间，采用格式 YYYYMMDDhhmmss，24 小时制格式。
9	请求 Host	Rq_Host	可变长字符型	40	记录请求的主机，如 https://ythpt.nr.gdgov.cn/ythpt-tymh/am-portal/login?redirect=%2Fhome，其对应的 Rq_host 为 https://ythpt.nr.gdgov.cn。
10	客户端请求 URL	Rq_Url	可变长字符型	200	客户端请求 URL, 如 https://ythpt.nr.gdgov.cn/ythpt-tymh/am-portal/login?redirect=%2Fhome，其对应的 Rq_Url 为 /ythpt-tymh/am-portal/login?redirect=%2Fhome。
11	客户端请求方法	Rq_Http_Method	字符型	10	客户端请求 HTTP METHOD，如 OPTION、PUT、DELECT、TRACE、CONNECT 等。
12	客户端操作类型	Operate_Type	整数型	1	用户具体操作类型代表，0：登录；1：退出；2：查询；3：新增；4：修改；5：删除；6：上传；7：下载。
13	服务端响应时间	Rq_ Prov_Time	字符型	14	从请求到响应的时间，采用格式 xxms。
14	服务端返回响应码	Resp_Code	整数型	5	服务端返回响应码。
15	操作结果	Operate_Result	字符型	1	用户操作的结果，包括成功/失败。1:成功；0：失败。

广东省土地学会

序号	数据项名称	数据项标识	类型	长度	采用标准及说明
16	功能模块名称	Mod	可变长字符型	30	操作类型为0-登录时，置空；使用中文描述的模块名称。

表 A.3 用户行为日志内容及格式（续）

序号	数据项名称	数据项标识	类型	长度	采用标准及说明
17	操作详情	Operate_Condition	可变长字符型	200	操作类型为0-登录、1-退出时，置空；可识别的操作内容，如上传了一个XX文件、将a修改为b等，不能是sql语句等，例如含有select的语句。
18	风险等级	Pri	整数型	1	日志风险等级，1：紧急；2：警报；3：警告；4：信息；5：调试。
19	类型	Logtype	整数型	1	日志类型，1：运行日志；2：管理日志；3：业务日志。

注：标有“*”号的数据项在条件允许时可考虑采集，其他没有标“*”号的数据项必须采集。

A.4 业务行为日志

业务行为日志内容及格式见表A.4。

表 A.4 业务行为日志内容及格式

序号	数据项名称	数据项标识	类型	长度	采用标准及说明
1	记录标识	Id	长整型	32	用于唯一标识应用系统产生的日志数据中的一条记录，在日志记录产生时生成，其格式和产生方式由各应用系统系统自行决定。
2	时间	Data	字符型	14	日志产生的日志，，采用格式YYYYMMDDhhmmss，24小时制格式。
3	业务名称	Bname	可变长字符型	50	记录业务的名称
4	耗时	Btime	字符型	6	从请求到响应的时间，采用格式xxms。
5	结果	Result	字符型	1	处理结果，包括成功/失败。1:成功；0：失败。
6	风险等级	Pri	整数型	1	日志风险等级，1：紧急；2：警报；3：警告；4：信息；5：调试。
7	类型	Logtype	整数型	1	日志类型，1：运行日志；2：管理日志；3：业务日志。

A.5 接口服务调用日志

接口服务调用日志内容及格式见表A.5.

表 A.5 接口服务日志内容及格式

序号	数据项名称	数据项标识	类型	长度	采用标准及说明
1	记录标识	Id	长整型	32	用于唯一标识应用系统产生的日志数据中的一条记录，在日志记录产生时生成，其格式和产生方式由应用应用系统自行决定。
2	时间	Data	字符型	14	日志产生的日志，，采用格式YYYYMMDDhhmmss，24小时制格式。
3	应用系统名称	Dname	可变长字符型	100	产生日志的应用系统名称，采用格式XXX或XXX-xxx（XXX表示平台名称，xxx表示子系统名称）。

广东省土地学会

4	接口名称	Interface_Name	可变长字符型	50	被调用的接口的具体名称。
5	请求方名称	Requester	可变长字符型	50	请求方的应用系统或客户端名称。

A.5 接口服务日志内容及格式（续）

序号	数据项名称	数据项标识	类型	长度	采用标准及说明
6	请求方 IP	From	可变长字符型	40	请求方的 IP。
7	*用户标识	User	字符型	18	触发接口调用行为的用户信息，涉及重要数据、个人敏感信息的数据共享建议使用。
8	*用户使用 IP	Terminal_IP	可变长字符型	40	触发接口调用行为的用户 IP(NAT 前的 IP)，涉及重要数据、个人敏感信息的数据共享建议使用。
9	*单位名称	Organization	可变长字符型	100	用户所属单位的名称，省统建或跨单位使用的应用系统建议使用。
10	接口服务响应时间	Interface_Time	字符型	14	服务端收到请求的第一个字节起，至响应最后一个字节发出止所花费的时间，采用格式 xxxms。
11	请求参数	Interface_Parameters	可变长字符型	--	记录接口服务的接口参数值。
12	结果	Result	字符型	1	服务执行结果，包括成功/失败。1:成功；0：失败。
13	*图层名称	layerName	可变长字符型	50	调用图层的名称。
14	*服务类型	Servicetype	可变长字符型	40	服务类型(3DTiles、I3S、S3M 等)。
15	*文件路径	Path	可变长字符型	100	文件路径(B3DM、SLPK、S3M 等)。
16	*叠加操作	Operation	可变长字符型	20	叠加操作枚举值： CLIP，ERASE，INDENTITY，INTER SECT，UNION，UPDATE，XOR。
17	Token	Token	可变长字符型	100	认证 token。
18	风险等级	Pri	整数型	1	日志风险等级，1：紧急；2：警报；3：警告；4：信息；5：调试。
19	类型	Logtype	整数型	1	日志类型，1：运行日志；2：管理日志；3：业务日志。

注：标有“*”号的数据项在条件允许时可考虑采集，其他没有标“*”号的数据项必须采集。

广东省地学会

参 考 文 献

[1] 互联网政务应用安全管理规定》
[2] 《自然资源领域数据安全管理办法》
[3] JR/T 0233—2021 证券期货业经营机构内部应用系统日志规范
[4] YD/T 3496-2019 Web 安全日志格式及共享接口规范

广东省土地学会