

ICS 65.020.40
B 65

LY

中华人民共和国林业行业标准

LY/T 2170—2013

林业信息系统安全评估准则

Security evaluation criterion of forestry information system

2013-10-17 发布

2014-01-01 实施

国家林业局 发布

目 次

前 言	III
引 言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 林业信息系统安全等级保护	1
4.1 林业信息系统安全保护等级	1
4.2 不同等级的安全保护能力	1
4.3 基本安全要求	2
4.4 基本技术要求的三种类型	2
5 第一级基本要求及应对措施	2
5.1 技术要求及应对措施	2
5.1.1 物理安全	2
5.1.2 网络安全	3
5.1.3 主机安全	4
5.1.4 应用安全	4
5.1.5 数据安全及备份恢复	5
5.2 管理要求及应对措施	5
5.2.1 安全管理制度	5
5.2.2 安全管理机构	5
5.2.3 人员安全管理	6
5.2.4 系统建设管理	6
5.2.5 系统运维管理	7
6 第二级基本要求及应对措施	9
6.1 技术要求及应对措施	9
6.1.1 物理安全	9
6.1.2 网络安全	11
6.1.3 主机安全	12
6.1.4 应用安全	13
6.1.5 数据安全及备份恢复	14
6.2 管理要求及应对措施	15
6.2.1 安全管理制度	15
6.2.2 安全管理机构	15
6.2.3 人员安全管理	16
6.2.4 系统建设管理	16
6.2.5 系统运维管理	18
7 第三级基本要求及应对措施	21

7.1	技术要求及应对措施	21
7.1.1	物理安全	21
7.1.2	网络安全	23
7.1.3	主机安全	25
7.1.4	应用安全	27
7.1.5	数据安全及备份恢复	29
7.2	管理要求及应对措施	29
7.2.1	安全管理制度	29
7.2.2	安全管理机构	30
7.2.3	人员安全管理	31
7.2.4	系统建设管理	32
7.2.5	系统运维管理	34
8	第四级基本要求及应对措施	38
8.1	技术要求及应对措施	38
8.1.1	物理安全	38
8.1.2	网络安全	40
8.1.3	主机安全	42
8.1.4	应用安全	44
8.1.5	数据安全及备份恢复	46
8.2	管理要求及应对措施	47
8.2.1	安全管理制度	47
8.2.2	安全管理机构	48
8.2.3	人员安全管理	49
8.2.4	系统建设管理	50
8.2.5	系统运维管理	52
9	第五级基本要求	56
	附录 A(规范性附录) 关于林业信息系统整体安全保护能力的要求	57
	附录 B(规范性附录) 林业重要信息系统安全要求的选择和使用	58
	参考文献	59

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国林业信息数据标准化技术委员会(SAC/TC 386)提出并归口。

本标准起草单位:国家林业局信息中心、中科信息安全共性技术国家工程研究中心有限公司。

本标准主要起草人:杨新民、乌日根、李淑芳、温战强、白莹、张洋、裴少亮、薛征宇。

引 言

本标准依据国家信息安全等级保护管理规定制定。林业具有信息化程度高、业务持续性要求高、对信息系统的容量和处理能力要求高的特点。本标准从林业实际情况出发,对《信息安全技术 信息系统安全等级保护基本要求》(GB/T 22239—2008)的有关要求进行了明确、细化和调整,提出和规定了林业不同等级信息系统的安全要求,并针对不同等级的安全要求提出了技术和管理方面的应对措施,适用于指导林业按照等级保护要求进行安全建设、测评和监督管理。

本标准文字中,明确、细化和调整的内容以楷体字表示。

林业信息系统安全评估准则

1 范围

本标准规定了林业不同安全保护等级信息系统的基本保护要求,包括基本技术要求、基本管理要求及应对措施。

本标准适用于指导林业分等级信息系统的安全建设、整改、测评和监督、管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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。

GB/T 5271.8 信息技术 词汇 第8部分:安全

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 22240 信息安全技术 信息系统安全等级保护定级指南

GB 50016 建筑设计防火规范

GB 50174—2008 电子信息系统机房设计规范

3 术语和定义

GB/T 5271.8 和 GB 17859 界定的以及下列术语和定义适用于本文件。

3.1

安全保护能力 security protection ability

系统能够抵御威胁、发现安全事件以及在系统遭到损害后能够恢复先前状态等的程度。

4 林业信息系统安全等级保护

4.1 林业信息系统安全保护等级

林业信息系统根据其在国家安全、经济建设、社会生活中的重要程度,遭到破坏后对国家安全、社会秩序、林业市场稳定、公共利益以及投资者、法人和其他组织的合法权益的危害程度,由低到高划分为五个等级,定级划分定义见 GB/T 22240。

4.2 不同等级的安全保护能力

不同等级的信息系统应具备的基本安全保护能力如下:

第一级安全保护能力:应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾害,以及其他相当危害程度的威胁所造成的关键资源损害,在系统遭到损害后,能够恢复部分功能。

第二级安全保护能力:应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾害,以及其他相当危害程度的威胁所造成的重要资源损害,能够发现重要的安全