

（供学术交流使用）

《老挝人民民主共和国网络安全法》

编译：西北政法大学涉外刑事法治与国别检察司法
研究中心

本件法律由西北政法大学涉外刑事法治与国别
检察司法研究中心组织编译，如需详细法律查明，
请与中心联系。

单位：西北政法大学涉外刑事法治与国别检察
司法研究中心

联系电话：029-88182613

目录

老挝人民民主共和国主席令	1
老挝人民民主共和国国会决议	1
老挝人民民主共和国网络安全法	2
第一编 总则	2
第 1 条 目的	2
第 2 条 网络安全	3
第 3 条 用语解释	3
第 4 条 国家网络安全政策	5
第 5 条 网络安全工作原则	6
第 6 条 适用范围	6
第 7 条 国际合作	6
第二编 网络安全要素	7
第 8 条 网络安全要素	7
第 9 条 保密	7
第 10 条 完整性	7
第 11 条 可用性	7
第 12 条 身份验证与访问控制	8
第 13 条 电子证据与责任	8
第三编 国家重要信息基础设施	8
第 14 条 国家重要信息基础设施	8
第 1 章 国家重要信息基础设施部门	9
第 15 条 国家重要信息基础设施部门	9
第 16 条 国家重要信息基础设施部门的认定条件	9
第 2 章 国家重要信息基础设施单位的保护	9
第 17 条 国家重要信息基础设施单位的认定	9
第 18 条 实体保护与访问控制	10
第 19 条 对供应商和第三方服务提供商的管控	10
第 20 条 报告、预警与评估	10

第 21 条 国家重要信息基础设施单位的责任	11
第 3 章 国家网络安全执行体系	11
第 22 条 国家网络安全执行体系	11
第 23 条 与国家网络安全执行体系的连接	12
第四编 网络安全措施	12
第 1 章 防范措施	12
第 24 条 防范措施	12
第 25 条 风险评估	13
第 26 条 访问控制	13
第 27 条 数据的安全加密	13
第 28 条 网络的安全维护	13
第 2 章 突发事件的应对措施	13
第 29 条 突发事件的应对措施	13
第 30 条 网络安全突发事件的监测与分析系统	14
第 31 条 网络安全突发事件的处置与应对	14
第 3 章 发生突发事件时的措施	14
第 32 条 发生突发事件时的措施	14
第 33 条 紧急状态的宣布	15
第 34 条 专门委员会的成立	15
第 35 条 对提供服务的限制和暂停	15
第 4 章 系统恢复措施	15
第 36 条 系统恢复措施	15
第 37 条 突发事件的应急处置	16
第 38 条 数据的备份与恢复	16
第 5 章 报告与数据交换	16
第 39 条 数据报告	16
第 40 条 事件报告	16
第 41 条 数据交换	17
第 42 条 数据交换中的保密	17
第 43 条 侦查调查中的合作	17

第 44 条 年度报告	17
第 45 条 数据跨境交换	18
第 6 章 宣传教育与培训	18
第 46 条 宣传教育与培训	18
第 47 条 网络安全宣传教育	18
第 48 条 网络安全培训	19
第五编 网络安全经营	19
第 49 条 网络安全经营业务的类别	19
第 50 条 网络安全经营许可的申请	20
第 51 条 网络安全经营许可的条件	20
第 52 条 网络安全经营许可的申请材料	20
第 53 条 网络安全经营许可证的审批	21
第 54 条 网络安全经营许可证	21
第 55 条 网络安全经营者的权利	22
第 56 条 网络安全经营者的义务	22
第 57 条 网络安全经营的暂停	23
第 58 条 网络安全经营许可证的吊销	24
第六编 网络安全备案	25
第 59 条 网络安全备案	25
第 60 条 应当备案的对象	25
第 61 条 应当备案对象的信息	25
第 62 条 备案的审议	26
第七编 禁止性规定	26
第 63 条 一般禁止性规定	26
第 64 条 对网络安全经营者的禁止性规定	27
第 65 条 对服务使用者的禁止性规定	27
第 66 条 对有关公务员和主管人员的禁止性规定	27
第八编 网络安全工作的管理与检查	28
第 1 章 网络安全工作的管理	28
第 67 条 网络安全工作主管机关	28

第 68 条 技术与通信部的权利和义务	28
第 69 条 万象市、各省技术与通信厅的权利和义务	30
第 70 条 各县、市技术与通信办公室的权利和义务	31
第 71 条 有关部、机关和地方政权机关的权利和义务	32
第 2 章 网络安全工作的检查	32
第 72 条 网络安全工作检查机关	32
第 73 条 检查的内容	32
第 74 条 检查的形式	32
第九编 对有功人员的政策和对违法人员的措施	33
第 75 条 对有功人员的政策	33
第 76 条 对违法人员的措施	33
第十编 附则	33
第 77 条 经费	33
第 78 条 组织实施	33
第 79 条 生效	34

老挝人民民主共和国主席令

关于颁布《网络安全法》

第 144/ປະທານ 号

万象市，2025 年 8 月 6 日

- 根据《老挝人民民主共和国宪法》（国会第 77/ສພຊ 号，2025 年 3 月 20 日）第 68 条第 1 款；
- 根据国会 2025 年 6 月 25 日第 163/ສພຊ 号关于通过《网络安全法》的决议；
- 根据国会常务委员会 2025 年 7 月 23 日第 41/ຄປຈ 号建议函。

老挝人民民主共和国主席兹颁布主席令如下：

第 1 条 兹颁布《网络安全法》。

第 2 条 本主席令自签署之日起生效。

老挝人民民主共和国主席

（签名并盖章）

通伦·西苏里（ທອງລຸນ ສີສຸລິດ）

老挝人民民主共和国国会决议

关于通过《网络安全法》

第 163/ສພຊ 号

万象市，2025 年 6 月 25 日

- 根据《老挝人民民主共和国宪法》（国会第 77/ສພຊ 号，2025 年 3 月 20 日）第 54 条第 1 款；

– 根据《国会法》（国会第 56/ສພຊ号，2024 年 6 月 28 日）第 11 条第 1 款。

国会第九届第九次常会对《网络安全法》的内容进行了广泛而深入的审议研究，并于 2025 年 6 月 23 日的会议议程上予以审议，于 2025 年 6 月 25 日下午的议程中予以通过。

国会决定：

第 1 条 以出席会议的国会议员半数以上赞成票通过《网络安全法》。

第 2 条 本决议自签署之日起生效。

国会主席

（签名并盖章）

赛宋蓬·丰威汉（ບອ ໄຊສົມພອນ ພົມມະວິຫານ）

老挝人民民主共和国网络安全法

（国会第 87/ສພຊ号，2025 年 6 月 25 日通过；主席令第 144/ປະທານ号，2025 年 8 月 6 日公布）

第一编 总则

第 1 条 目的

本法规定网络安全工作的管理与监督检查的原则、规则和措施，使上述工作高效并取得实效，旨在维护国家安全、社会安宁和社会秩序、数据信息安全、国家重要信息基础设施，保护国家、组织和

自然人的权利与利益，能够与区域和国际接轨，为保卫和建设国家作出贡献。

第 2 条 网络安全

网络安全，是指防止通信技术、数据、信息系统遭受网络攻击，或者遭受网络威胁造成的损害，包括维护系统和网络的完整性，以及保障上述系统的可用性。

第 3 条 用语解释

本法中使用的用语，含义如下：

1、网络（Cyber），是指由计算机网络、信息技术基础设施、控制系统、连接设备，以及全部在线活动构成的通信技术、数据、信息系统；

2、国家重要信息基础设施单位（Critical Information Infrastructure, CII），是指拥有、运营或者管理对国家具有重要意义的系统的法人、组织或者机关；上述单位停顿或者被破坏，将对老挝人民民主共和国的稳定、经济社会造成严重影响¹；

3、计算机突发事件应急响应单位（CERT），是指负责处置和防范网络安全事件的专业团队²；

4、网络威胁（Cyber threat），是指在网络空间可能对系统、网络或者数据产生的危险或者风险，例如网络攻击、恶意软件或者个人数据泄露；

¹ 老挝法称 ໂຄງລ່າງພື້ນຖານ ຂໍ້ມູນ ຂ່າວສານ ທີ່ສໍາຄັນຂອງຊາດ，字面为“国家重要信息基础设施”；我国《网络安全法》第 31 条称“关键信息基础设施”（CII）。两者的实质标准相近，但认定主体与程序不同：老挝法由技术与通信部牵头、会同有关部门复核评估后报政府核准（见本法第 17 条），我国则由国务院制定认定规则、保护工作部门负责认定并通知运营者。

² 老挝文 ໜ່ວຍງານຕອບໂຕ້ເຫດສຸກເສີນທາງຄອມພິວເຕີ 直译为“计算机突发事件应对单位”，国际通行简称 CERT（Computer Emergency Response Team）。我国相近机构为国家计算机网络应急技术处理协调中心（CNCERT/CC），但隶属关系与法定职权不同，故保留英文简称并加注。

5、网络空间（Cyberspace），是指由系统、网络、电子数据，以及通过通信技术连接的全部使用者之间的交互构成的数字环境；

6、网络攻击（Cyber attack），是指具有破坏、干扰目的，或者未经授权访问系统、网络或者数据的任何行为，例如阻断式攻击、入侵系统、计算机系统漏洞；

7、防火墙（Firewall），是指跟踪和管控数据进出流量、防止未经授权的访问和互联网威胁的网络安全系统；

8、分布式拒绝服务攻击（Distributed Denial of Service attack, DDoS），是指利用控制大量设备向目标系统发出大量数据请求的网络攻击，致使该系统瘫痪或者无法正常提供服务；

9、云（Cloud），是指通过互联网利用远程计算机资源存储和处理数据的系统；

10、硬盘（Hard disk），是指用于在计算机内部存储数据的电子设备，用于记录和大量保存数据；

11、个人数据（Personal data），是指可用于直接或者间接识别个人身份的任何数据³；

12、恶意软件（Malware），是指被设计用于破坏、干扰计算机系统运行或者窃取数据的软件；

13、勒索软件（Ransomware），是指对使用者文件加密、实施诱骗勒索，并以解密数据为交换条件索取赎金的一类恶意软件；

14、计算机系统漏洞（Vulnerability），是指程序或者软件不完善和 / 或未获更新升级的缺陷，使入侵者得以利用其实施破坏系统、窃取数据、篡改数据等行为；

³ 老挝文 ຂໍ້ມູນສ່ວນບຸກຄົນ 直译为“个人数据”（Personal data），与我国《个人信息保护法》上的“个人信息”范围大体相当而表述不同；本译本依原文统一作“个人数据”。

15、网络（Network），是指能够交换数据信息的计算机和电子设备互联系统；

16、数据库（Database），是指能够系统性检索和访问的、用于保存和管理数据的系统；

17、控制系统（Control System），是指用于控制、跟踪和管理设备、机械或者各种工艺过程的运行，使之自动化工作的系统，例如工业控制系统、空调系统、飞机飞行控制系统；

18、人工智能（Artificial Intelligence, AI），是指使机器能够像人一样思考、学习和决策的技术；

19、促进安全数字生态系统发展（Secure Digital Ecosystem），是指营造安全、可信的数字环境，包括发展安全的网络基础设施、保护个人数据、培养人才队伍、制定适当的法规并安全地开展国际对接，以促进数字经济；

20、第三方服务提供商（Third-party Service Provider），是指提供信息技术、数据信息、云服务、系统维护或者其他网络安全服务，可能访问或者处理单位数据的外部自然人、法人或者组织。

第4条 国家网络安全政策

国家将网络安全作为国防和公安工作、经济社会发展、科学、技术和对外事务中的优先事项。

国家重视网络安全工作，通过提供预算和必要的物资设备，建设基础设施，培养、培训和配备专业人力资源，研究采用现代技术，使上述工作高效并取得实效。

国家鼓励国内外的自然人、法人和组织相互合作，共同参与防范危害国家重要信息基础设施和社会秩序的网络安全危险。

国家鼓励和促进自然人、法人和组织进行研究、投资，开发用于网络安全防范的技术、产品和服务。

第5条 网络安全工作原则

网络安全工作应遵循以下原则：

- 1、符合路线、政策、宪法、法律、战略规划和国家经济社会发展规划；
- 2、保障国家安全、社会安宁和社会秩序；
- 3、保障国家、自然人、法人和组织的数据信息安全；
- 4、保障法律面前人人平等，保护使用者的权利和利益；
- 5、保障与各部、机关、地方行政机关和其他有关方面的协调配合；
- 6、符合老挝人民民主共和国为缔约方的公约和有关国际条约⁴。

第6条 适用范围

本法适用于在老挝人民民主共和国境内开展和涉及网络安全工作的国内外自然人、法人和组织。

第7条 国际合作

国家鼓励与外国、区域和国际在网络安全工作方面发展关系和开展合作，通过交流经验教训、信息、技术、工艺、创新，提高工作人员的专业水平、知识和业务能力，开发人力资源，履行老挝人民民主共和国为缔约方的公约义务和有关国际条约。

⁴ 老挝文 ສັນທິສັນຍາ 指多边公约，ສັນຍາສາກົນ 指国际条约；二者在本法中并列使用，本译本分别作“公约”“国际条约”。

第二编 网络安全要素

第8条 网络安全要素

网络安全要素如下：

- 1、保密；
- 2、完整性；
- 3、可用性；
- 4、身份验证与访问控制；
- 5、电子证据与责任⁵。

第9条 保密

保密，是指保护数据免受未经授权的访问或者披露；数据保密包括数据加密、访问控制、数据分类等。

第10条 完整性

完整性，是指数据的正确性和原有完整状态在数据的整个使用期限内得到保持，所采用的技术包括电子签名、数据正确性校验、变更控制、数据备份、恢复等。

第11条 可用性

可用性，是指保障系统内数据和资源的供应处于就绪状态，包括持续发展规划、数据备份、灾难恢复、系统维护，以及对有需求的自然人或者经授权的系统进行承载能力管理。

⁵ 本条所列五项要素，大体对应信息安全的保密性、完整性、可用性三项基本属性，另加身份验证与访问控制、电子证据与责任两组制度性要素。老挝文 ການຮັກສາຄວາມລັບ 字面为“保守秘密”，本译本依本法用语作“保密”（第9条同）。

第 12 条 身份验证与访问控制

身份验证，是指审核自然人、法人或者组织与从有关组织数据库中调取并据以指认该自然人、法人或者组织的数据和特征之间的关联是否正确过程。

访问控制，是指确保仅经授权的自然人或者系统方可依据其访问权限和访问必要性访问数据或者技术资源，并对访问实行系统审核的机制。

第 13 条 电子证据与责任

电子证据，是指以电子工具记录并保存在系统中或者处于发送、接收过程中的数据，能够证明某一行为或者事件确实发生。

责任，是指致害人必须对其行为承担的义务，包括恢复名誉、赔礼道歉、教育、警告、纪律处分、罚款、承担民事损害赔偿、刑事处罚⁶。

第三编 国家重要信息基础设施

第 14 条 国家重要信息基础设施

国家重要信息基础设施，是指对老挝人民民主共和国的稳定、安宁、安全、经济社会、科学、技术和对外事务具有重大意义的系统、财产、便利设施和网络；上述信息基础设施停顿或者被破坏，将给国家造成严重危害⁷。

⁶ 老挝文 ກອບກຸ້ຍງດຮັກສີ 字面为“恢复名誉”，指致害人以一定方式弥补对受害人名誉的损害，我国《民法典》上的相应责任形式为“消除影响、恢复名誉”。本条将民事、行政、刑事以及纪律责任形式并列，与我国法律责任分类体例不完全对应。

⁷ 原文此句末作 ສົ່ງຜົນກະທົບຮ້າຍແຮງໂດຍກົງຕໍ່ປະເທດຊາດ，其中 ໂດຍກົງ 非规范搭配（识读稿另录作 ໂດຍກົງປະເພດຊາດ），疑为 ໂດຍກົງຕໍ່ປະເທດຊາດ（“直接针对国家”）之排印讹误；本译本按后者之义译出。

国家重要信息基础设施，分别按部门、单位保护和国家网络安全执行体系作出规定。

第 1 章 国家重要信息基础设施部门

第 15 条 国家重要信息基础设施部门

国家重要信息基础设施部门如下：

- 1、国防和公安；
- 2、技术与通信；
- 3、财政和银行；
- 4、能源；
- 5、商业、交通运输和物流；
- 6、其他部门。

第 16 条 国家重要信息基础设施部门的认定条件

国家重要信息基础设施部门按以下条件认定：

- 1、对人民生活的重要性；
- 2、国家发展；
- 3、遭受网络攻击或者其他灾害的风险；
- 4、停顿或者服务被破坏的影响。

第 2 章 国家重要信息基础设施单位的保护

第 17 条 国家重要信息基础设施单位的认定

国家重要信息基础设施单位的认定，按以下规定执行：

- 1、识别并分类可能成为国家重要信息基础设施的单位；
- 2、评估可能发生的风险和影响；

3、确定单位的优先次序；

4、确定并核准国家重要信息基础设施单位名单。

技术与通信部牵头协调有关各部、机关和地方行政机关，每年一次，或者在数据信息技术发生重大变化时，对国家重要信息基础设施单位进行复核和评估，并报政府审议核准⁸。

第 18 条 实体保护与访问控制

国家重要信息基础设施单位必须具备以下实体保护和访问控制措施：

- 1、严格的实体安全防护系统；
- 2、将重要区域与一般区域隔离，并限制仅经授权人员方可进入；
- 3、严格的身份验证与访问控制系统；
- 4、每次进出的记录与跟踪。

第 19 条 对供应商和第三方服务提供商的管控

对供应商和第三方服务提供商的管控，按以下规定执行：

- 1、必须通过基础审查，并取得技术与通信部门的认可；
- 2、必须严格控制供应商和第三方服务提供商的访问；
- 3、必须严格按照网络安全规定通过检查。

第 20 条 报告、预警与评估

在报告、预警和评估方面，国家重要信息基础设施单位应按以下规定执行：

- 1、建立网络安全报告和预警系统；

⁸ 老挝法由技术与通信部牵头、会同有关部门复核评估后报政府核准名单；我国《关键信息基础设施安全保护条例》则规定由保护工作部门按照认定规则负责认定并通知运营者，报国务院公安部门备案，认定主体与程序不同。

2、在国家重要信息基础设施遭受网络威胁时，必须立即向负责网络安全工作的机关报告突发事件；

3、必须建立针对国家重要信息基础设施可能发生的威胁的预警系统；

4、由负责网络安全工作的机关对国家重要信息基础设施单位的准备情况定期进行检查和评估；

5、必须立即向政府报告检查和评估结果。

第 21 条 国家重要信息基础设施单位的责任

国家重要信息基础设施单位负有以下责任：

1、执行负责网络安全工作的机关发布的各项规定；

2、制定保障连续运行的发展和完善计划，并规定发生网络威胁时的处置办法；

3、建立主系统瘫痪时可以使用的备份系统；

4、定期进行风险评估和网络安全检查。

第 3 章 国家网络安全执行体系

第 22 条 国家网络安全执行体系

国家网络安全执行体系，是国家网络威胁监测、分析和应对中心。该体系隶属技术与通信部，承担全国范围内的信息基础设施、数据信息和互联网的管理职责，以持续监测和分析网络威胁，协调和应对网络安全突发事件，交换和预警威胁信息，提供技术咨询和援助，组织培训并建设工作人员的能力⁹。

⁹ 我国无同名机构：网络安全工作由中央网络安全和信息化领导机构统筹协调、国家网信部门负责，应急处置的技术支撑由国家计算机网络应急技术处理协调中心（CNCERT/CC）等承担，未设统揽监测、分析、应对的单一体系；老挝则将上述职能集中于隶属技术与通信部的国家网络安全执行体系。

国家网络安全执行体系由现代化工具和专业人才组成，二十四小时不间断运行，运用大数据分析技术和人工智能侦测和应对威胁；此外，还协调国家与私营部门的其他单位，以保障国家网络安全工作。

第 23 条 与国家网络安全执行体系的连接

与国家网络安全执行体系连接，国家重要信息基础设施单位应按以下规定执行：

- 1、必须与国家网络安全执行体系连接；
- 2、执行技术与通信部各时期规定的连接技术规程和标准；
- 3、保障连接的安全性和可信性；
- 4、对通过系统交换的数据保密；
- 5、测试和维护连接。

第四编 网络安全措施

第 1 章 防范措施

第 24 条 防范措施

网络安全防范措施如下：

- 1、风险评估；
- 2、访问控制；
- 3、数据的安全加密；
- 4、网络的安全维护；
- 5、认为有必要的其他网络安全防范措施。

关于网络安全防范措施的步骤和方法，另行规定。

第 25 条 风险评估

自然人、法人和组织，必须对重要的系统、数据和数字资产开展网络安全风险评估；上述评估必须至少每年进行一次。

网络安全风险评估结果必须用于改进安全计划，并向上一级报告¹⁰。

第 26 条 访问控制

自然人、法人和组织，必须采取有效的系统访问控制措施，实行最小权限、职责分离和多因素身份验证。

第 27 条 数据的安全加密

自然人、法人和组织，必须对存储的和正在通过网络传输的重要、敏感数据采取数据的安全加密措施；数据的安全加密必须采用强加密方法。

第 28 条 网络的安全维护

自然人、法人和组织，必须采取网络的安全维护措施，即安装防火墙和入侵检测与防御系统，同时对网络作适当的分域隔离，以保障网络系统的安全¹¹。

第2章 突发事件的应对措施

第 29 条 突发事件的应对措施

突发事件的应对措施如下:

¹⁰ 原文此句末作 *ລາຍງານຕໍ່ຂັ້ນເທິງທັດຖິນ*，其中 *ທັດຖິນ* 非标准老挝语词，疑为 *ທັນທີ*（“立即”）之排印讹误；本译本按“向上一级报告”译出。

11 老挝文 ພຣັດ 为英文 Firewall 之音译，本法第 3 条第 7 项定义为“跟踪和管控数据进出流量、防止未经许可的访问和互联网威胁的网络保护系统”，本译本作“防火墙”。又 ວະບົນກອດຈັບປ້ອງກັນການບຸກລຸກ 字面为“侦察并防止入侵的系统”，本译本作“入侵检测与防御系统”；我国《网络安全法》第 21 条将“防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施”列为网络安全等级保护义务之一，未点明具体系统名称。

- 1、网络安全突发事件的监测与分析系统；
- 2、网络安全突发事件的处置与应对；
- 3、认为有必要的其他应对措施。

第 30 条 网络安全突发事件的监测与分析系统

自然人、法人和组织，必须采用有效的网络安全突发事件监测与分析系统，该系统由入侵检测与防护工具、技术、用于数据分析并确定目标事件优先次序的人工智能¹²组成，具备清晰的报告和预警程序，同时保障全天候不间断运行，并配备专家团队值守，以及针对发生突发事件情形的应急预案¹³。

第 31 条 网络安全突发事件的处置与应对

自然人、法人和组织，必须处置和应对网络安全突发事件，为此应制定并实施网络安全突发事件应对预案；该预案必须规定详细、明确的响应步骤、网络安全工作机关的职责、损害限制措施，以及报告程序，并规定与相关各方的协调配合。

关于网络安全突发事件应对的步骤和方法，另行规定¹⁴。

第 3 章 发生突发事件时的措施

第 32 条 发生突发事件时的措施

发生突发事件时的措施如下：

- 1、宣布紧急状态；
- 2、成立专门委员会；

¹² 老挝文 ປັນຍາປະດິດ 即英文 Artificial Intelligence (AI)，本法第 3 条第 18 项定义为“使机器能够如人类一样思考、学习和决策的技术”，本译本作“人工智能”，保留英文原文 AI 于译名之后。

¹³ 本编各条所称 ຕູດກາງສຸກເສີນທາງໄຊເຊີ ວີ，字面为“网络紧急事件”，指需要即时处置的网络安全突发事件，本译本作“网络安全突发事件”，与本法固定用语 ອຸປະຕິຕູດທາງໄຊເຊີ ວີ（网络安全事件）相区别。

¹⁴ 老挝文 ໄດ້ກຳນົດໄວ້ໃນລະບຽບການຕ່າງຫາກ 字面为“已在专门法规中规定”，指本法之外的专门法规另行规范，本法全篇多次使用此种指引性表述，本译本统一作“另行规定”。

- 3、限制或者暂停提供服务；
- 4、认为有必要的其他措施。

第 33 条 紧急状态的宣布

政府是网络安全紧急状态¹⁵的宣布机关，在发生严重并给国家经济社会发展造成重大影响的网络安全突发事件时，依技术与通信部的提议宣布之。

第 34 条 专门委员会的成立

在发生严重并给国家经济社会发展造成重大影响的网络安全突发事件时，政府必须成立专门委员会，由相关部门、机关和方面的代表组成，以开展对该事件的应对。

第 35 条 对提供服务的限制和暂停

专门委员会必须采取限制或者暂停提供服务的措施，如全部或者部分停止提供电信、互联网和通信服务，以防止由网络安全突发事件产生的威胁扩散。

在管控和暂停提供服务的过程中，专门委员会必须与相关部门、机关、地方政权机关和有关方面协调配合，以阻止扩散、减少影响、恢复系统和采取认为有必要的其他措施。

第 4 章 系统恢复措施

第 36 条 系统恢复措施

系统恢复措施如下：

- 1、突发事件的应急处置；

¹⁵ 老挝文 ພາວະສຸກເສີນທາງໄຊຕ໌, 本译本作"网络安全紧急状态", 指依本条、第 34 条、第 35 条启动的特别处置程序。我国《网络安全法》设监测预警与应急处置制度（第五章），但未设由国务院宣布紧急状态的程序。

- 2、备份与系统恢复；
- 3、认为有必要的其他措施。

第 37 条 突发事件的应急处置

自然人、法人和组织，必须规定突发事件的应急处置步骤和方法，以及时评估、控制和限制网络威胁，然后报告专门委员会和技术与通信部。

第 38 条 数据的备份与恢复

自然人、法人和组织，必须将数据备份于服务器和 / 或硬盘，并将备份数据多地点存放，以便在发生突发事件时能够恢复所备份的数据。

第 5 章 报告与数据交换

第 39 条 数据报告

数据报告如下：

- 1、事件报告；
- 2、数据交换；
- 3、数据交换中的保密；
- 4、侦查调查中的合作；
- 5、年度报告；
- 6、数据跨境交换；
- 7、认为有必要的其他数据报告。

第 40 条 事件报告

自然人、法人和组织，必须报告将会给自身造成损害和 / 或扩散至其他方面的网络安全事件，必须在发现该事件后立即报告网络

安全负责机关；同时必须报告必要的的数据，如勒索软件（ຮາບຊອມແລວ）、恶意软件、分布式拒绝服务攻击，以便及时评估影响并作出应对¹⁶。

第 41 条 数据交换

国家重要信息基础设施各部门的网络安全负责机关，必须与有关的自然人、法人交换关于网络威胁和安全漏洞的数据。

自然人、法人的网络安全负责机关，必须与技术通信部的网络安全工作机关协调配合并交换关于网络安全的数据和信息。

第 42 条 数据交换中的保密

自然人、法人和技术通信部的网络安全工作机关，必须确保所报告和所交换的事件数据按已规定的密级予以保密。

第 43 条 侦查调查中的合作

自然人、法人和组织，必须与有关的侦查调查机关合作，如提供数据、证据、为侦查调查所必要的系统访问权限，以应对构成犯罪的网络安全违法行为。

第 44 条 年度报告

自然人、法人和组织，必须于每年 1 月内向技术与通信部提交年度报告网络安全状况和工作执行情况。

年度报告由以下内容组成：

- 1、已实施的网络安全措施；
- 2、所发生的网络安全事件或者威胁及其解决办法；

¹⁶ 原文作 ຄຣາບຊ້າງແລວ (ransomware 之音译)，与本法第 3 条第 13 项定义 ransomware 时所用 ຄຣາບຊ້າງແລວ 用字不一，本译本并注英文 Ransomware，作“勒索软件（ຮາບຊອມແລວ）”。又 ມາລວແລວ 为 Malware 之音译，本译本作“恶意软件”；ການໂຈມຕີແລບບຕິດຕໍ່ 字面为“连续攻击”，即分布式拒绝服务攻击（Distributed Denial of Service attack, DDoS），本译本作“分布式拒绝服务攻击”。

- 3、执行网络安全计划的进展；
- 4、所发现的计算机系统安全漏洞及其解决办法；
- 5、网络安全方面的宣传教育和培训；
- 6、下一年度的计划安排。

技术与通信部必须在三十日内汇总、分析并向政府报告结果。

第 45 条 数据跨境交换

关于网络安全的跨境数据交换如下：

- 1、关于计算机系统威胁和安全漏洞的数据；
- 2、对网络威胁的分析和应对技术；
- 3、开展网络安全工作的经验教训；
- 4、认为有必要的其他数据。

技术与通信部主管网络安全的跨境数据交换，应确保安全、保守秘密，并符合老挝人民民主共和国为缔约方的公约和有关国际条约。

第 6 章 宣传教育与培训

第 46 条 宣传教育与培训

宣传教育与培训如下：

- 1、网络安全宣传教育；
- 2、网络安全培训。

第 47 条 网络安全宣传教育

网络安全工作主管机关、自然人、法人和有关方面，必须经常、持续地开展网络安全宣传教育，如关于网络威胁的认识、国家重要

信息基础设施的防护方法等，以在本单位和全社会树立牢固的网络安全文化¹⁷。

第 48 条 网络安全培训

网络安全工作主管机关、自然人、法人和有关方面，必须如下开展网络安全培训：

- 1、建立对网络安全的基本认识；
- 2、培养报告和应对网络威胁的技能；
- 3、开展网络安全突发事件应急处置的实操演练；
- 4、更新知识技能，以适应技术和网络威胁的发展。

网络安全培训必须经常、持续地进行，并对培训步骤、技术和方式进行评估和改进，以使网络安全培训具有效力和实效。

第五编 网络安全经营

第 49 条 网络安全经营业务的类别

网络安全经营业务如下:

- 1、网络安全咨询；
- 2、安全系统的开发和安装；
- 3、渗透测试¹⁸；
- 4、事件应对；
- 5、培训；
- 6、标准符合性审查；
- 7、培训与监测服务；

¹⁷ 老樹文 ວັດທະນະທຳດ້ານຄວາມປອດໄພໄລເບີ 字面为“网络安全文化”，本译本作“网络安全文化”。

¹⁸ 原文作 ကာကတိနဆပကာကအးလးပိပ, 其中 အးလး 于老挝语无相应义项, 疑为排印错字, 本译本按“渗透测试”(Penetration Test)译出。

- 8、数据与系统恢复；
 - 9、安全服务；
 - 10、与网络安全有关的其他业务。
- 关于各类网络安全经营业务，另行规定。

第 50 条 网络安全经营许可的申请

有意开展网络安全经营业务者，必须依《企业法》的规定向工业与商业部门备案登记企业；取得企业登记证后，向技术与通信部申请经营许可¹⁹。

第 51 条 网络安全经营许可的条件

网络安全经营许可的条件如下：

- 1、持有企业登记证；
- 2、在老挝人民民主共和国设有合法、固定的办公场所；
- 3、具有至少二年信息技术或相关领域工作经验的管理人员；
- 4、拥有信息技术或者相关专业高等教育以上学历的技术人员；
- 5、财务状况稳健，并经有关部门确认；
- 6、未曾因故意违法犯罪被法院判处剥夺自由刑；
- 7、拥有保障业务开展的技术系统；
- 8、认为有必要的其他条件。

第 52 条 网络安全经营许可的申请材料

网络安全经营许可的申请材料如下：

- 1、技术与通信部规定格式的申请书；
- 2、企业登记证的复印件；

¹⁹ 老挝文 ດຳລັງຂຶ້ນທະບຽນວິສາຫະກິດ，字面为“申报企业登记”，指依《企业法》办理企业设立登记并按企业类型确定经营范围、取得企业登记证，故译“登记”；本法第六编称的 ການຂຶ້ນທະບຽນຄວາມປອດໄພໄຊເຕີ 为向技术与通信部办理的“网络安全备案”，二者不同，本译本分别作“登记”“备案”以相区别。

- 3、企业内部规章；
- 4、合营合同（如有）；
- 5、设立人的简历；
- 6、财务状况证明；
- 7、经济技术分析报告和 / 或经营计划；
- 8、其他必要的材料。

第 53 条 网络安全经营许可证的审批

技术与通信部必须在收到正确、完整的申请书和申请材料之日起十五日内，会同其他有关行业部门审批发放网络安全经营许可证²⁰；在不能发放网络安全经营许可证的情形下，也必须在前述期限内以书面形式将理由通知申请人。

第 54 条 网络安全经营许可证

网络安全经营许可证的有效期为一年，可以续期。

经营许可证不得交付、转让、出租或者交由其他自然人、法人或者组织使用。

申请续展许可证的，必须在许可证有效期届满之日前至少三十日向技术与通信部²¹提交申请书，并必须附送下列文件：

- 1、续展许可证申请书；
- 2、经营许可证副本；
- 3、完税、缴纳手续费和服务费的凭证副本；
- 4、以往经营情况报告。

²⁰ 本条第二句"ອອກໃບອະນຸຍາດດຳເນີນທຸລະກິດຄວາມປອດໄພໄຊບີ"较本条首句少 ກ່ຽວກັບ（关于）一词，指同一许可证，本译本按首句用语统一译出，未逐处注明。

²¹ 老挝文 ກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ 直译为"技术与通信部"，为老挝主管科技、邮电通信和信息化工作的部门，本法第六编、第八编的多项职权均由该部行使，本译本统一作"技术与通信部"。又本条第三款原文作 ກະຊວງການເຕັກໂນໂລຊີ，于 ກະຊວງ（部）后多一 ການ 字，本法其他各处均无此字，疑为原件排印衍字，姑按机关名称译出。

技术与通信部必须自收到正确、完整的申请书和附送文件之日起十日内，审议许可证续展事宜。

第 55 条 网络安全经营者的权利

网络安全经营者享有下列权利：

- 1、按照所获许可提供网络安全服务；
- 2、安全、保密地保存服务使用者的数据，且仅用于网络安全服务，法律另有规定的除外；
- 3、按照所获许可的业务类别，生产、进口、出口、销售和安装网络安全设备；
- 4、依法使用场地和其他便利条件开展经营；
- 5、申请使用电信运营商的电信基础设施；
- 6、对不缴纳服务费或者违法的服务使用者，暂停或者取消提供服务；
- 7、依法获得权利和合法利益的保护；
- 8、向有关方面提出防范和解决安全问题的措施建议；
- 9、与其他服务提供者和有关机关交换网络威胁数据；
- 10、申请服务标准认证；
- 11、申请暂停或者注销本人的经营许可证；
- 12、行使法律规定的其他权利。

第 56 条 网络安全经营者的义务

网络安全经营者负有下列义务：

- 1、制定本单位的网络安全经营计划，使之符合国家网络安全发展战略和国家数字经济发展规划；

2、向技术与通信部门的公务员²²和本单位工作人员传授经营服务中所使用的技术知识；

3、保障本单位的技术系统能够与其他电信运营商的技术系统相连接；

4、在提供网络安全服务方面给予国家机关优先；

5、具有本法规定的发生灾害、突发事件时的网络安全系统恢复预案；

6、与国家网络安全运行单位²³合作；

7、接收、研究和解决网络安全服务使用者的意见；

8、依照法律和有关法规的规定，履行关税、赋税、手续费和服务费义务；

9、按照各时期工作的需要，提供与国家网络安全技术系统的连接；

10、按照技术与通信部的规定，建立服务使用者数据的存储和保护系统，防止数据泄露；

11、为与本单位安全系统有关的其他服务提供者提供便利；

12、解决和赔偿因本单位提供服务所产生的影响和损害；

13、向网络安全负责机关年度报告本单位的网络安全状况；

14、履行法律规定的其他义务。

第 57 条 网络安全经营的暂停

网络安全经营在下列情形下将被暂停：

1、由经营者提出暂停，或者有关组织提出建议的；

²² 老挝文 ພະນັກງານ-ລັດຖະກອນ 指在党政机关、军队、警察和国营单位任职的公职人员，范围宽于我国“公务员”，本译本作“公务员”。

²³ 老挝文 ຫວ່ອຍງານປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ，指运行本法第 23 条所称国家网络安全运行系统（ລະບົບປະຕິບັດການຄວາມປອດໄພໄຊເບີແຫ່ງຊາດ）的单位；原件 ຫວ່ອຍ 系 ຫນ່ວຍ 之异写。

- 2、未按照所获许可的宗旨和目标开展经营的；
- 3、未向有关机关报告安全违法行为的；
- 4、未依照法律和有关法规缴纳赋税、手续费和服务费的；
- 5、法律规定的其他情形。

在暂停网络安全经营之前，技术与通信部必须通知经营者改正和解决。

如发生严重网络威胁，危及国家重要基础设施、信息数据，以及社会稳定和秩序，必须立即吊销经营许可证，无需事先通知。

第 58 条 网络安全经营许可证的吊销

网络安全经营许可证在下列情形下将被吊销²⁴：

- 1、不按照责令改正通知改正、解决的；
- 2、由经营者提出，或者有关组织提出建议的；
- 3、将许可证交由其他自然人、法人或者组织使用、出租或者转让的；
- 4、严重违法违反法律、法规，对国家经济社会、国防和公安工作以及公民合法权益造成重大损害的。

技术与通信部必须自吊销经营许可证之日起五个工作日内，以书面形式将吊销网络安全经营许可证的情况通知工业和贸易部，并通过新闻媒体向社会公布。

²⁴ 本条标题原文作 ການຖອນໃບອະນຸຍາດການດຳເນີນທຸລະກິດ，导言及第 2 项同此，均作 ດຳເນີນ；本法其他条文均作 ດຳເນີນ，系原件拼写不一，本译本统一作“经营”。

第六编 网络安全备案

第 59 条 网络安全备案

在老挝人民民主共和国境内通过互联网系统提供服务、分发、供应和传播信息的自然人、法人和组织，必须向技术与通信部办理网络安全备案，以保障安全和透明²⁵，旨在保护重要系统和数据，保护自然人、法人和组织的数据，促进安全数字生态系统的发展。

网络安全备案的手续费和服务费，按照各时期公布的手续费和服务费规定执行。

第 60 条 应当备案的对象

应当办理网络安全备案的对象如下：

1、通过互联网系统提供服务、分发、供应和传播信息而不以营利为目的的自然人、法人和组织，如提供数据库服务、提供网络安全系统服务；

2、提供网络安全方面的服务，如提供网站托管服务、提供数字支付系统服务、提供电信服务。

第 61 条 应当备案对象的信息

应当备案对象的信息如下：

- 1、自然人、法人和组织的名称和地址；
- 2、网络安全负责人的联系信息；
- 3、关于数据保存和处理的信息；
- 4、提供、分发、传播服务的类别；
- 5、认为有必要的其他信息。

²⁵ 原文作 ຄວາມປອດໄພ, 疑为 ຄວາມໂປ່ງໃສ (透明) 之异写, 本译本按"透明"译出。

第 62 条 备案的审议

通过互联网系统提供服务、分发、供应和传播信息的自然人、法人和组织，必须向技术与通信部提交网络安全备案申请。

技术与通信部在收到备案申请和应当备案对象的信息后，必须核查上述信息的准确性，以在三十日内审议发放备案证明。如信息不齐全，必须通知备案申请人在十五日内补充提供信息。

在已备案的信息发生变更的情况下，该备案人必须自信息变更之日起十五日内，以书面形式将上述信息变更情况告知技术与通信部。

第七编 禁止性规定

第 63 条 一般禁止性规定

禁止自然人、法人和组织有下列行为：

- 1、未经许可开展网络安全经营；
- 2、未经许可侵入或者访问系统、网络、程序和数据；
- 3、制作、分发、使用恶意软件、病毒或者其他危害数字系统的程序；
- 4、未经许可截取、篡改、隐匿或者毁坏他人个人数据；
- 5、妨碍或者干扰系统、网络的运行；
- 6、未经许可进口、出口、使用网络安全设备或者技术；
- 7、未经许可买卖或者交换他人个人数据；
- 8、拒绝或者回避与国家有关机关合作侦查调查网络安全威胁事件；
- 9、有其他违法行为。

第 64 条 对网络安全经营者的禁止性规定

禁止网络安全经营者有下列行为：

- 1、不按照所获许可的宗旨开展经营；
- 2、未经许可披露、使用服务使用者的数据；
- 3、忽视遵守网络安全标准；
- 4、隐匿或者忽视向国家有关机关报告网络安全违法行为；
- 5、无充分理由拒绝提供服务或者区别对待服务使用者；
- 6、向国家有关机关提供或者报告不准确、不齐全的网络安全信息；
- 7、有其他违法行为。

第 65 条 对服务使用者的禁止性规定

禁止网络安全服务使用者有下列行为：

- 1、以不合法的方式使用网络安全服务；
- 2、不按照服务合同遵守使用条件；
- 3、不遵守网络安全经营者关于网络安全的指导意见；
- 4、披露网络安全经营者计算机系统安全漏洞的信息；
- 5、有其他违法行为。

第 66 条 对有关公务员和主管人员的禁止性规定

禁止有关公务员和主管人员有下列行为：

- 1、利用职权、职责、职位为自己、家庭、亲属和自己所在党派谋取利益，给自然人、法人、组织或社会造成损害；
- 2、未经许可披露国家机密或者经营者的数据；
- 3、拖延、伪造网络安全文件；
- 4、忽视遵守网络安全步骤和标准；

- 5、不按照本人的权利和职责，访问所负责的数据或者系统；
- 6、在履行职责中使用未经许可的设备或者软件；
- 7、有其他违法行为。

第八编 网络安全工作的管理与检查

第 1 章 网络安全工作的管理

第 67 条 网络安全工作主管机关

政府在全国范围内统一、集中管理网络安全工作，责成技术与通信部直接负责，并作为主要协调者，与有关部门、机关和地方政权机关协调配合。

网络安全工作主管机关由下列机关组成：

- 1、技术与通信部；
- 2、万象市、各省技术与通信厅²⁶；
- 3、各县、市技术与通信办公室。

为保障网络安全工作有效、高效开展，网络安全工作主管机关可以按照各时期的规定，委托乡行政管理委员会²⁷协助管理网络安全工作。

第 68 条 技术与通信部的权利和义务

在网络安全工作管理中，技术与通信部享有下列权利和义务：

- 1、研究、制定和修改关于网络安全工作的方针政策、法律、战略规划和法规，提交政府审议；

²⁶ 老挝文 ນະຄອນຫຼວງ 指首都万象市，为部级以下、省级建制的地方行政单位，本译本作“万象市”；下同。

²⁷ 老挝文 ຄະນະການປຶກສາລາຍງານ ກ່ຽວກັບ ຕາແລງ (乡) 一级的行政管理机关，原件 ປຶກສາລາຍງານ ກ່ຽວກັບ ຕາແລງ 之异写，本译本作“乡行政管理委员会”。

2、将关于网络安全工作的方针政策、法律、战略规划和法规分解为计划、方案、项目和组织实施；

3、宣传、传播关于网络安全工作的方针政策、法律、战略规划和法规；

4、发布关于网络安全工作的决议、命令和指导意见；

5、制定和发展网络安全标准；

6、管理、跟踪和检查网络安全工作的组织实施，并解决全国范围内发生的问题；

7、建设和管理国家网络安全防护系统，配备专家人员和现代化设备；

8、向政府提议宣布网络安全紧急状态；

9、研究和审议网络安全备案；

10、发放、暂停或者吊销网络安全经营许可证；

11、研究国家重要信息基础设施单位的确定、评估或者复审，以提交政府各时期审议；

12、培养、提高、升级和发展网络安全工作的人员；

13、研究、开发和应用网络安全技术；

14、向社会树立网络安全工作的意识和认识；

15、接收、研究和解决自然人、法人或者组织关于网络安全工作的意见；

16、与有关部门、机关、地方政权机关和有关方面就网络安全工作进行协调配合；

17、与外国、区域和国际就网络安全工作进行联系和合作；

18、经常总结和向政府报告网络安全工作的开展情况；

19、行使法律规定的其他权利和履行其他职责。

第 69 条 万象市、各省技术与通信厅的权利和义务

在网络安全工作管理中，万象市、各省技术与通信厅在本机关的职责范围内享有下列权利和义务：

- 1、组织实施关于网络安全工作的方针政策、法律、战略规划和法规；
- 2、宣传、传播关于网络安全工作的方针政策、法律、战略规划和法规；
- 3、制定关于网络安全工作的计划和项目，以组织实施；
- 4、管理、跟踪和检查网络安全工作的组织实施，并解决发生的问题；
- 5、与有关部门、办公室和有关方面就网络安全工作进行协调配合；
- 6、促进和支持网络安全工作的人员发展；
- 7、提出培养、升级和发展网络安全工作的人员；
- 8、接收和研究网络安全备案申请和网络安全经营许可证申请；
- 9、提出网络安全备案；
- 10、提出发放、暂停或者吊销网络安全经营许可证；
- 11、收集和报告关于网络安全状况的信息；
- 12、在发生网络安全突发事件时，与计算机突发事件应对单位协调配合；
- 13、提供关于网络安全工作的咨询和技术援助；
- 14、向社会树立网络安全工作的意识和认识；
- 15、接收、研究和解决自然人、法人或者组织关于网络安全工作的意见；
- 16、跟踪和评估网络安全项目的实施结果；

17、按照授权与外国就网络安全工作进行联系和合作；

18、经常总结和向技术与通信部以及万象市、省级行政管理委员会报告网络安全工作的开展情况；

19、行使法律规定的其他权利和履行其他职责。

第 70 条 各县、市技术与通信办公室的权利和义务

在网络安全工作中，各县、市技术与通信办公室在本机关的职责范围内享有下列权利和义务：

1、组织实施关于网络安全工作的方针政策、法律、战略规划和法规²⁸；

2、传播关于网络安全工作的方针政策、法律、战略规划和法规；

3、向社会树立网络安全工作的意识和认识；

4、跟踪、检查关于网络安全工作的情况并作出报告；

5、就网络安全工作提供指导意见；

6、收集和提供服务提供者关于网络安全工作的信息；

7、提出网络安全工作中人员培养、升级和发展的计划；

8、接收、研究和解决自然人、法人或者组织关于网络安全工作的意见；

9、与有关部门、办公室和有关方面就网络安全工作进行协调配合；

10、经常总结和向万象市、各省技术与通信厅以及县、市级行政管理委员会报告网络安全工作的开展情况；

11、行使法律规定的其他权利和履行其他职责。

²⁸ 原文作 ກຽວກັບອາການຄວາມປອດໄພໂຊດີ, 其中 ອາການ 疑为 ວຽກງານ (工作) 之讹, 本条下文及本法其他条文均作 ວຽກງານ, 本译本按"工作"译出。

第 71 条 有关部、机关和地方政权机关的权利和义务

有关部、机关和地方政权机关，在本机关的角色和职责范围内，享有与同级技术与通信部门、国防和公安部门共同管理、跟踪、参与和协调配合网络安全工作的权利和义务。

第 2 章 网络安全工作的检查

第 72 条 网络安全工作检查机关

网络安全工作检查机关由下列机关组成：

- 1、内部检查机关，即与本法第 67 条规定的网络安全工作主管机关为同一机关；
- 2、外部检查机关，即国会、省级人民议会、各级国家检查机关、国家审计机关、老挝建国阵线、老挝退伍军人联合会、群众组织和新闻媒体²⁹。

第 73 条 检查的内容

网络安全工作的检查内容如下：

- 1、关于网络安全工作的方针政策、法律、战略规划和法规的组织实施情况；
- 2、网络安全工作的服务提供情况；
- 3、有关公务员和主管人员行使权利和履行职责的情况；
- 4、认为重要和必要的其他内容。

第 74 条 检查的形式

网络安全工作的检查以下列三种形式进行：

²⁹ 老挝 ສະພາແຫ່ງຊາດ 为国会，ສະພາປະຊາຊົນຂັ້ນແຂວງ 为省级人民议会，ອົງການກວດກາລັດ 为各级政府序列内的国家检查机关，ອົງການກວດສອບແຫ່ງລັດ 为国家审计机关，ອົງການຈັດຕັ້ງມະຫາຊົນ 为群众组织；老挝不设人民代表大会，其国家权力机关的监督、行政监察与审计的机关分工与我国不同。

- 1、常规计划检查，即按照计划定期进行并有确定期限的检查；
 - 2、事先通知的检查，即认为有必要时进行的计划外检查，必须事先通知被检查人³⁰；
 - 3、突击检查，即不事先通知被检查人的紧急检查。
- 在网络安全工作的检查中，必须严格遵守法律。

第九编 对有功人员的政策和对违法人员的措施

第 75 条 对有功人员的政策

在组织实施本法中成绩突出的自然人、法人或者组织，将依照规定受到表彰或者享受其他政策待遇。

第 76 条 对违法人员的措施

违反本法的自然人、法人或者组织，将依照法律受到教育、警告、纪律处分、罚款³¹、赔偿民事损害或者刑事处罚。

第十编 附则

第 77 条 经费

网络安全工作的经费，包括国家预算、电信和数字化转型发展基金、国内外自然人、法人和组织的援助和捐助，以及其他合法收入。

第 78 条 组织实施

老挝人民民主共和国政府是本法组织实施机关。

³⁰ 原文作 ການກວດກາບອກແຜນການ ແລະ ຕັ້ງຄົງຄວາມ, 其中 ອກ、ຕັ້ງ 疑分别为 ນອກ（外）、ເຖິງ（见、认为）之讹，本译本分别按“计划外”“认为”译出。

³¹ 原文作 ປັບໃຫມ, 疑脱 ໃຫມ 的声调符号（ປັບໃຫມ），本译本按“罚款”译出。

第 79 条 生效

本法自 2025 年 9 月 1 日起生效，即在老挝人民民主共和国国家主席发布公布令并在政府公报上登载之后。

国会主席

（签名并盖章）

赛宋蓬·丰威汉（ບໍ ໄຊສົມພອນ ພົມວິຫານ）