通威股份有限公司信息安全与隐私保护政策

一、政策声明

通威股份有限公司（以下简称“通威股份”或“公司”）高度重视信息安全与隐私保护工作，严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规及相关规定要求，结合我司已经完成贯标的ISO/IEC 27001、ISO 37301，并参考GB/T 22239-2019等信息安全与合规标准要求，积极推进信息安全管理体系建设，严格落实信息及数据安全保护工作。公司制定本政策旨在规范信息处理行为、保障信息安全、维护相关方合法权益。

二、适用范围

本政策适用于通威股份及旗下分子公司的各项业务与运营活动，涵盖信息的收集、存储、处理、传输、使用及销毁等全流程。同时，公司要求与公司有业务往来的供应商、承包商、合作伙伴和其他相关利益相关方积极遵守本准则，共同构建安全可靠的信息环境。

三、责任部门

公司明确信息部为信息安全与隐私保护的主要责任部门，负责统筹协调信息安全与隐私保护工作，包括政策的制定、修订、执行监督、培训宣传以及隐私问题的接收、调查与处理等。各部门负责人为本部门信息安全与隐私保护的第一责任人，确保本部门人员严格遵守相关规定。

信息安全与隐私保护是所有工作人员必须共同承担的责任，基于本公司信息系统的现状，已建立信息化与网络安全领导小组和工作组，构建由二者共同组成的信息安全管理机构。在

信息化与网络安全领导小组的统一领导下，各部门须履行自身信息安全工作职责，协同保障本企业信息系统的信息安全。

四、信息安全与隐私保护政策

（1）风险管理：公司承诺不断推进信息安全管理体系完善、升级，将信息安全管理政策与相关工作的实施整合融入全公司范围的风险与合规管理环节，公司将定期对信息安全与隐私保护风险进行识别、评估和分析，针对可能存在的风险点制定相应的防控措施和应急预案。此外，公司信息部通过多种渠道（包括但不限于安全漏洞发布平台、信息安全专业网站、行业内部信息、安全公司订阅情报等）监控和收集各类信息安全威胁情报，并对所收集的威胁情报实施评估与分析。对于经评估判定为高风险且可能对公司信息安全造成实际影响的威胁，信息部应当及时制定内部应对措施，并通过邮件等方式及时向内部发布预警通知。

（2）信息安全管理体系：在信息化与网络安全领导小组的领导下，信息部依照计划、执行、检查和行动的过程建立并管理信息安全管理体系。公司每年开展信息安全管理体系审核，审核工作旨在确定该体系的控制目标、控制措施、过程及程序是否符合相关标准和法律法规的要求，是否符合已识别的信息安全要求，是否得到有效实施和维护，以及是否按管理层期望执行。公司通过对各项监测活动结果的分析，采集内外部与信息安全管理有关的信息，为体系的持续改进提供支撑；公司亦通过管理评审，识别管理体系改进的需求、偏离信息安全目标的原因或现行体系在适应环境方面的差距，制定改进的具体措施并明确具体的改进计划；此外，公司实施改进措施并验证其结果，并保留实施过程和结果的相关记录。

（3）信息与数据安全：为确保信息及数据的保密性、完整性、可用性，公司强化信息传输全流程安全管控，通过部署加密技术、访问控制机制等手段，防止信息及数据被非法篡改、泄露或破坏。

（4）零容忍政策：公司对违反信息安全与隐私保护规定的行为持零容忍态度。一经发现，将根据情节轻重根据公司相关管理制度对相关责任人进行处理，包括但不限于警告、降职、撤职、解除劳动合同等；若行为触犯法律法规，将依法移交司法机关处理，追究其法律责任。

（5）内外部审计：为确保信息安全与隐私保护政策的有效执行，公司每年将开展一次信息安全内部审核，对各部门信息安全与隐私保护工作的落实情况进行全面检查与评估。同时，公司将定期邀请具备资质的第三方机构开展外部审核，针对审核中发现的问题及时进行整改，

持续提升信息安全与隐私保护水平。

（6）合作伙伴管理：公司要求合作伙伴（包括供应商等）积极配合信息安全与隐私保护相关制度与要求。在与重点供应商确立合作之前，公司积极开展信息安全相关尽职调查，确保不存在重大风险。同时，要求合作伙伴签署保密协议，明确双方保密责任和义务。此外，定期评估和监督合作伙伴信息安全措施的有效性，以降低合作过程中的信息安全风险。

（7）隐私信息收集与使用管理：公司尊重客户的知情权，充分告知其以下隐私保护相关问题。

- 所获取信息的性质：包括但不限于客户的名称、属性、联系方式、 基本介绍、特别注意事项等。
- 信息收集的用途：包括但不限于建立客户档案、日常联系、提供个性化产品和服务、改善产品与服务质量等。
- 信息保存的期限：承诺始终按照法律的规定在合理必要期限内存储客户个人信息。超出上述期限后，公司将删除客户的个人信息或对个人信息进行匿名化处理。如公司停止运营，公司将及时停止收集个人信息的活动，将停止运营的通知以逐一送达或公告的形式通知客户，并对所持有的个人信息进行删除或匿名化处理。
- 信息处理权利：客户有权访问、查阅、复制、更正、注销用户信息，法律法规规定的例外情况除外。
- 信息保护的措施：努力采取各种符合行业标准的安全措施来保护客户的个人信息以最大程度降低个人信息被毁损、盗用、泄露、非授权访问、使用、披露和更改的风险。公司将积极建立数据分类分级制度、数据安全管理规范、数据安全开发规范来管理规范个人信息的存储和使用，确保未收集与公司提供的服务无关的个人信息。

（8）供应商信息安全管理：公司对供应商实施全流程信息安全管理，明确供应商在信息资产访问环节的安全责任与操作规范。针对供应商可访问的信息资产，公司应通过签订安全协议、划定访问权限范围、建立访问日志审计机制等方式进行严格保护，防止供应商以未经授权的方式获取组织资产；同时，公司对供应商的授权流程进行规范化管控，通过定期审查授权合理性、动态调整授权范围等措施，避免因授权不当导致敏感信息泄露，确保组织信息资产的安全性与保密性。

（9）第三方披露政策：公司承诺在将相关数据分享、转移或提供给第三方时，严格遵守相关法律法规和隐私保护准则，以确保数据转移活动符合法律规定并尊重数据主体的权利。

数据转移的目的和范围不能超出收集时所声明的目的和范围。高影响数据的传输须采用安全传输通道或加密后传输。数据输出者必须获得接收者的明确承诺。如涉及数据的跨境传输，需遵从当地法律法规的要求。

（10）业务连续性管理：公司围绕信息安全保障需求，在业务影响分析和风险分析中，依据多方面因素识别支撑信息安全的关键系统，并每年进行至少一次面向信息系统的安全风险评估，对安全风险相关影响及可能性进行实际分析；根据保障信息安全的管理目标及策略，公司从多方面分类制定应急演练预案并输出信息安全连续性演练计划，涵盖信息安全各环节检验，并定期开展业务连续性信息安全培训，使相关人员熟悉信息安全保障目标。此外，公司每年开展突发事件信息安全风险防范措施及应急响应工作的全面评估审计，将信息安全保障纳入全面风险管理体系，建立长效机制以保证信息安全管理工作的持续性和有效性。

CEO：刘舒琪

通威股份有限公司

2025 年 7 月

备注：

1、公司鼓励并支持供应商及合作伙伴在遵循本政策的前提下，采纳和执行额外的原则与政策，但这些额外原则和政策都不得与本政策产生冲突。

2、公司业务开展严格遵循所在地法律法规要求，若当地无明确法律法规要求时，执行本准则。

3、该文件由通威股份有限公司解释和修订，公司会适时根据国内外政策、监管要求和行业发展情况对文件进行更新，当文件中英文版有冲突时，请以中文版为准。