全球信息安全政策

本文件阐述了公司对信息技术安全问题的应对策略，符合公司的战略方向以及网络和信息安全方面适用的法律、法规[1]和合同要求。

本政策将根据现行法规要求并适应风险形势的变化，在出现针对企业信息的新类型威胁时，定期进行审查并在必要时予以更新。

原则

具体而言，本政策定义了保护组织信息资产的关键特征：

- **“保密性”**，即确保仅向经授权的个人或实体提供信息访问或披露的能力；
- **“完整性”**，指长期保障信息准确性和完整性的能力；
- **“可用性”**，指在授权个人或实体需要时，以其要求的方式提供、对信息进行访问和使用的能力。

这些原则为管理可能影响公司信息和资产（应用程序、服务、基础设施或其他信息处理组件）的风险提供了一个框架，以保护其免受任何来自内部或外部、故意或意外的威胁。

本政策要求倍耐力员工、供应商（及其分包商）、合作方以及任何管理集团数据、信息或信息系统的第三方遵守本政策以及适用的法律法规。

集团的安全保障基于持续风险评估、关键资源保护、人员培训和事件响应能力等关键原则。
为确保按照本政策的原则有效管理信息安全，倍耐力集团采用了稳健且结构完善的框架，并通过具体的内部操作程序和指导方针，明确了信息安全方面的职责、责任及操作方式。

治理、风险管理和持续改进

倍耐力股份有限公司董事会负责批准本信息安全与网络安全政策，确保其符合适用法规要求，包括《NIS2 指令》。

集团最高管理层在信息安全部门和其他相关公司职能部门的支持下，负责全面实施本政策，确保有效落实各项安全措施，并向董事会提供充分的信息流。

倍耐力集团的内部控制系统采用覆盖集团及重要第三方网络安全风险的管理流程，确保准确披露信息并充分控制集团所有活动，特别是关注潜在风险领域。倍耐力集团确定了必要的干预措施，以不断改进其安全状况、风险管理和与监管要求的一致性，并确保内部信息安全政策的实施。

安全事件监控、事件响应和危机管理

倍耐力集团采用结构化和集成化的安全管理方法，基于规范化的流程，持续进行事件监控、漏洞管理以及事件和危机响应。

具体而言，倍耐力集团识别、分析、确定对信息系统产生影响的漏洞的优先级及管理方式；监控安全事件并进行分析，以及时识别和管理可能危及信息保密性、完整性和可用性的威胁；并实施事件

[1] 因此，受欧盟（EU）2022/2555 号指令（NIS2）约束的倍耐力集团旗下各公司，在其由政策、标准、操作规程和指南组成的程序和运营框架内，制定、实施并监督相关适用要求。

响应计划，从威胁识别到采取必要的纠正措施，以减少此类事件的后续发生。 相关职责、沟通渠道和上报流程构成结构化和规范化的流程，其中还包括内部和外部的沟通信息流。

倍耐力集团建立了危机管理流程（包括重大事件），并将其纳入业务连续性计划，从而能够针对突发事件和/或特殊情况制定并实施快速有效的应对措施，以期在最短时间内恢复运营并将可能造成的损失降至最低。

信息安全综合控制体系

倍耐力集团制定并维护一套协调一致的技术、组织和人力资源措施，以完善其信息安全管理体系。为此，集团制定并保持针对员工和第三方（如适用）的培训和意识提升计划，实施信息分类和保护流程，并在资产的整个生命周期内对其进行安全管理，包括物理保护。

同时，集团采用结构化的数字身份管理和访问控制模型，旨在确保用户获得使用 IT 资源的授权，并且只能访问履行职责所必需的信息（“按需知密”），并遵循“最小权限原则”（“最小权限原则”）授予必要权限，保护其物理基础设施，并根据“安全设计”理念，将安全原则融入信息系统的整个生命周期。此外，企业网络和通信还通过技术防护和分段解决方案得到保护，以确保信息的保密性、完整性和可用性。

举报、保密、禁止报复以及违规后果

倍耐力集团鼓励本文件的适用对象本着诚信原则，举报（包括以匿名方式）任何由倍耐力内部人员、与倍耐力有业务往来的人员或代表倍耐力行事者所实施的任何作为或不作为，只要该行为构成或可能构成违反或诱使他人违反本政策所包含的原则。倍耐力公司举报政策以多种语言在公司网站 www.pirelli.com 发布，其中规定了举报程序、举报管理方式以及保密和禁止报复的保证。

若发生违反本政策的情况，无论该违规行为是通过举报程序还是其他方式被发现，倍耐力都将根据事件的严重程度采取适当措施，包括纠正措施（包括但不限于：与违规员工沟通、制定具体行动计划并委托主管经理执行等）和/或纪律处分（包括但不限于：口头和/或书面警告、绩效考核或评估结果不合格、解雇），所有措施均须符合适用的合同、纪律、法律和法规框架。

本政策相关文件

- 道德守则和行为守则
- 全球个人数据保护政策
- 知识产权政策
- 举报政策

2026 年 9 月

倍耐力股份有限公司

董事会