《正大集团信息安全政策和指南》

正大集团信息安全政策和指南

修订记录

版本	负责部门	描述	审核人	批准人	批准日期
1					
2					

注: 本表仅供内部使用。

正大集团信息安全政策和指南

修订记录

事业线 / 公司名称

版本	负责部门	描述	审核人	批准人	批准日期
1					
2					

注: 本表仅供内部使用。

目录

《正大集团信息安全政策和指南》

1. 宗旨

正大集团意识到无论是纸质形式还是电子形式的信息，都是企业最有价值的资产之一。通过系统和信息技术存储、收集、处理和传输的信息应该受到保护，以防止未经授权的使用。这种保护包括但不限于防止未经授权的访问、披露、更改或破坏此类信息，以及防范网络威胁。出于以上原因，集团优先监管系统信息和网络安全，以确保它们高效、准确、完整且随时可用，从而保护公司的资产和信息，并将由安全漏洞导致的风险和损失降至最低。此外，集团通过风险管理来评估公司的风险承受能力，培养网络弹性以应对业务需求和整个供应链中内外部利益相关者的需求。

因此，集团制定了本政策和指南，旨在确保对信息安全和网络安全的风险进行管理、预防、监控、监督、审计和控制，以符合适用的法律、法规和标准要求。此外，本政策和指南倡导遵守保密性、完整性、可用性和安全性原则的商业实践。最终，集团将确保业务连续性和工作环境的安全，同时建立强大的信息安全文化，增加可持续的竞争优势。

2. 范围

《正大集团信息安全政策和指南》适用于正大集团（以下简称“集团”），该集团包括正大集团有限公司及其所有下属公司。下文中“公司”一词是指采用本《信息安全政策和指南》的公司。本文件应至少每年一次或视情况而修订。

3. 目的

3.1 为董事、管理层和员工提供信息安全指南。

3.2 确保信息资产的访问和使用安全，防范可能会影响公司业务运营的信息风险。

4. 角色和职责

4.1 董事会

4.1.1 考虑并批准本《信息安全政策和指南》。

4.1.2 监督业务运营及其对相关法律、法规、规章、政策和指南的遵守情况。

4.1.3 督促并确保本政策和指南执行。

4.2 管理层

4.2.1 根据公司的战略、政策和指导方针以及相匹配的业务环境，建立规章制度和程序。

4.2.2 确定公司架构和具有适当角色和责任的负责人。

4.2.3 制定信息和网络安全行动计划，包括业务连续性计划。

4.2.4 建立风险管理和内部控制制度。

4.2.5 传达本政策和指南，以提高各级管理人员和员工的意识。

4.2.6 管理并支持员工遵守相关规则、操作程序和标准。

4.2.7 建立举报和投诉渠道，以联系负责信息和网络安全违规事件的部门/负责人。

4.2.8 在整个公司中培养信息和网络安全文化。

4.2.9 定期评估信息和网络安全绩效报告以及需改进的地方。

4.3 相关责任部门/人员

4.3.1 在整个供应链中评估和管理涉及对信息资产、内部和外部利益相关者有威胁、漏洞、可能性和影响的风险。

4.3.2 根据本政策和指南建立信息和网络安全措施，包括相关操作程序和标准。

4.3.3 持续监管和维护信息资产，以确保其可操作性和安全性。

4.3.4 跟进相关法律、法规、规章和标准，以改进信息和网络安全措施，并定期监查对应措施的实施情况。

4.3.5 建立报告信息和网络安全漏洞的标准和程序。

4.3.6 提升意识，就信息和网络安全向员工以及整个供应链的内部和外部利益相关者提供建议。

4.3.7 准备信息和网络安全绩效报告。

4.4 工作人员

4.4.1 学习并遵守规则、法规、政策和指南。

4.4.2 采取行动并通过公司提供的渠道报告任何可能影响业务运营、与公司信息和网络安全相关的异常或事件。

4.4.3 就本政策和指南的任何实际或潜在不当行为提出投诉或举报。

5. 指南

5.1 评估和分析公司的信息和网络安全风险，以及与整个供应链的内部和外部利益相关者相关的风险。

5.2 制定信息和网络安全风险管理策略，与公司愿景、使命、目标和风险承受能力相一致。

5.3 确定信息和网络安全计划和措施，包括公司环境的识别、信息资产的保护、异常事件的检测、安全事件的响应以及信息资产的损坏恢复。

5.4 管理公司内部和外部各方运营的信息资产，确保系统/软件开发全生命周期各阶段的安全。

5.5 保护通过计算机系统和信息技术传输的信息和数据，包括员工、客户、供应商和第三方数据处理者的个人数据，防止未经授权的访问、使用、传输、调整、复制、更改、删除和销毁。

5.6 评估和管理计算机系统和信息技术中的漏洞，定期进行补丁管理。

5.7 监控和检测异常活动、违反信息和网络安全的行为，或可能影响业务连续性的活动，并审核相关措施以确保其持续有效。

5.8 建立信息和网络安全事件管理流程，以便及时、安全地控制、缓解、修复和恢复受到影响的部分，并恢复信息资产。此外，还需持续改进该流程。

5.9 在信息和网络安全方面与国内外私营/国营和政府部门的组织，包括民间社会相互支持并协作。

5.10 促进和支持员工、客户、供应商和业务合作伙伴以及整个供应链中的内部和外部利益相关者的信息和网络安全意识建设。

6. 培训

通过培训、会议或其他适当形式的活动向董事、高管、员工和外部利益相关方包括供应商、合作伙伴、合资企业交流和传达本《信息安全政策和指南》，并定期评估此类培训和交流的有效性。

7. 举报

一旦发现任何违反本《信息安全政策和指南》的行为，应根据《正大集团举报政策和指南》进行投诉举报。无论是在事件调查过程中还是之后，公司须全程保护投诉举报人，确保其不被报复和调动工作岗位，并保密其个人信息和投诉举报的内容。

8. 政策指导

如果您发现可能违反法律、法规和本《信息安全政策和指南》的行为，并有疑问，请在做出任何决定或采取任何行动之前，向您的主管、团队或负责监督信息安全的人员、合规部门或法务部门寻求指导。

9. 处罚办法

所有员工必须积极配合内部和外部的调查机构。任何直接和间接违反或不遵守本政策和指南的行为将一律按照公司的规定受到纪律处分。

10. 相关法律法规和政策

10.1 相关信息和网络安全法律

10.2 相关计算机犯罪法

10.3 相关个人资料保护法

10.4 相关电子交易法

10.5 ISO/IEC 27001 - 信息安全管理体系 (ISO: the International Organization for Standardization) 和国际电工委员会 (IEC: the International Electrotechnical Commission)

10.6 网络安全框架 (CSF: Cybersecurity Framework) 由美国国家标准与技术研究院 (NIST: the National Institute of Standards and Technology)

10.7 信息及相关技术控制目标 (COBIT: Control Objectives for Information and Related Technologies), 信息系统审计与控制协会的框架 (ISACA: Framework by the Information Systems Audit and Control Association) 和 IT 治理研究所 (the IT Governance Institute)

10.8 互联网安全中心 (CIS: the Center for Internet Security)

10.9 网络评估框架 (CAF: The Cyber Assessment Framework) 由英国国家网络安全中心 (NCSC: the United Kingdom's National Cyber Security Center)

11. 附录

本《信息安全政策和指南》附录:

附录一: 定义

附录一

定义

1. **控制 (Control)**

风险管理中的管理、操作或技术的功能，帮助公司根据相关标准监测和评估所关注的领域，实现目标和目的。

2. **安全性 (Safety)**

将与技术有关的风险降到最低的原则，在这种情况下，技术故障或恶意行为者的操纵会对个人和资产造成损害。

3. **安全性 (Security)**

任何过程和行动，如预防、严格、小心、谨慎使用和维护，目的是保护信息资产不被盗窃、破坏、损坏或被内部和外部各方干扰，从而损害公司的业务运作。安全原则如下：

- 保密性(Confidentiality): 保护信息资产的机密性，防止未经授权的访问和披露，包括属于公司专有的个人身份信息。
- 完整性 (Integrity): 确保信息资产不会被未经授权的人篡改、修改或销毁。
- 可用性 (Availability): 确保在线渠道和离线形式的信息资产能够及时和可靠地提供给授权用户。
- 责任性 (Accountability): 根据员工的角色和责任，对行动、命令、任务和决定的结果负责。

- 认证 (Authentication): 确保只有在成功认证后才允许访问信息资产。
- 授权 (Authorization):确保对信息资产的访问权只在一个主体完成其工作职能合法要求的情况下（最少的特权）给予（需要知道的基础）。
- 不可否认性 (Non-repudiation): 确保一个人不能否认执行了一个事务（操作）。

4. **安全系统/软件开发生命周期** (Secure System/Software Development Life Cycle)

在系统/软件开发生命周期的所有阶段实施信息安全流程、措施和要求，包括需求收集、设计、采购、开发、测试、运行、维护和退役。

5. **风险** (Risk)

不确定事件对实现公司的货币和非货币目的和目标的负面影响。

6. **网络** (Cyber)

因使用服务、计算机网络、互联网系统或电信网络而产生的信息和通信，包括卫星和类似网络的常规服务的一般连接。

7. **信息技术** (Information Technology)

利用计算机技术、电子设备和电信网络来搜索、储存、分析、处理、传输、分发、跟踪、收集和管理公司的信息。

8. **利益相关者（内部和外部）** (Stakeholder - internal and external)

受公司运营影响的个人、团体或实体。这可以分为内部利益相关者（由董事、管理层和员工组成）和外部利益相关者（由客户、消费者、供应商、商业伙伴、股东、投资者、社区、社会、政府、非政府组织、竞争对手和债权人组成）。

9. **员工 (Employee)**

由公司长期或临时雇用的低于管理层的人员，以及根据特别合同雇用的人员。

10. **信息和网络安全措施 (Information and Cyber Security Measures)**

信息和网络安全的措施有以下五个方面：

- 识别 (Identification) 包括治理、风险管理、合规、人员安全和供应链风险管理。
- 保护(Protection) 包括资产管理、访问控制、安全系统/软件开发生命周期、密码管理、操作安全、变更管理、能力和性能管理、物理和环境安全以及通信和网络管理。
- 检测 (Detection) 包括日志监控和威胁管理。
- 响应 (Response) 包括信息和网络安全事件管理。
- 恢复 (Recovery) 包括业务连续性管理和灾难恢复。

11. **系统 (System)**

一种资产，包括可以被指定、界定和管理的系统或网络，例如，计算机、工作站、笔记本电脑、服务器、路由器、交换机、防火墙、移动设备等。

12. **信息 (Information)**

公司经过处理、分析、计算或解释的数据，可以通过电子网络系统或电子数据处理技术进行访问、搜索或检索，以两种格式中的一种提供：

1. 储存在计算机系统中或通过使用服务和计算机网络、互联网系统、电信网络，包括卫星和类似的网络服务创造的电子信息，如电子文件、数据库、媒体或便携式驱动器和协作工具等。

2. 物理信息，如打印的文件等。

13. 信息资产 (Information Asset)

信息和系统，包括软件、应用程序、服务或其他支持商业运作并对公司有经济价值的信息资源。

14. 信息和网络安全事件（内部和外部）(Information and Cyber Security Incident - Internal and External)

通过未经授权的访问、破坏、披露、更改和/或服务中断，可能对公司、个人或其他组织拥有的运营和信息资产产生负面影响的任何情景或事件。