www.genscriptprobio.cn

# 金斯瑞蓬勃生物数据安全白皮书

## 2024版

金斯瑞
蓬勃生物

# 目 录

# 1. 公司介绍

## 1.1 业务介绍

### 1.1.1 蓬勃生物——生物医药合同研发生产（CDMO）平台

蓬勃生物拥有一站式生物药研发生产平台，主要致力于为细胞和基因治疗(CGT)药物、疫苗、 抗体及重组蛋白药物等提供从靶点开发到商业化生产的端到端 CDMO 服务。 蓬勃生物在美国、荷兰、韩国、 中国（香港、上海、南京、镇江） 等地设有公司以服务全球客户。自 2017 年 10 月， 共助力美国、欧洲、亚太等区域客户获得 90 余个 IND 批件。

蓬勃生物的全面细胞与基因治疗（CGT）解决方案覆盖了质粒、病毒载体、 mRNA 疫苗和核酸药物的 IND 申报，以及临床和商业化生产。蓬勃生物为质粒和病毒载体提供了一体化的 CMC 解决方案，包括建库、工艺开发、表征和验证、分析方法开发和验证，以及稳定性研究，赋能细胞与基因治疗迈向下一个里程碑。

蓬勃生物的生物药开发解决方案涵盖生物药尤其是抗体药发现、抗体工程和和体内体外药理评价。在生物药 CDMO 服务方面，蓬勃生物为客户提供包括细胞系开发、宿主细胞商业化授权、上下游工艺开发、分析方法开发和临床样品及商业化生产等在内的一体化 CDMO 服务，并提供分批补料和灌流工艺以满足增长的抗体蛋白药的需求。 GMP 生产车间满足 FDA、 EMA 和 NMPA 监管要求。

蓬勃生物始终以“合作加速创新”为理念，致力于帮助客户缩短生物药进入临床的时间，显著降低客户的研发成本，加速医药转化，共创健康未来。

更多信息，请访问蓬勃生物官网 https://www.genscriptprobio.cn/

### 1.1.2 金斯瑞生物科技股份有限公司

蓬勃生物的母公司金斯瑞生物科技股份有限公司（HK.1548）是全球重要的生命科学研发与生产服务提供商。植根于坚实的 DNA 合成技术，金斯瑞现已建立四大主要业务单元：生命科学服务及产品业务单元、生物制剂合约开发及生产（CDMO）业务单元、工业合成产品业务单元、综合性全球细胞疗法公司。

金斯瑞成立于 2002 年，并于 2015 年在港交所主板挂牌上市，法人实体遍及美国、中国、日本、新加坡、荷兰、爱尔兰、英国、韩国、比利时及西班牙。业务运营范围覆盖全球 100 多个国家和地区，为 20 余万客户提供优质、便捷、可靠的服务与产品。

截至 2023 年 12 月 31 日，金斯瑞在全球拥有超过 6900 名员工，全球范围已有超过 87,700 篇经国际同业审阅的学术期刊文献引述了金斯瑞的服务及产品。金斯瑞拥有多项知识产权，其中包含超过 300 项授权专利与 900 多项专利申请，以及大量技术机密。

秉承“用生物技术使人和自然更健康”的企业使命，金斯瑞致力于成为全球“最受信赖的生物科技公司”。

更多信息，请访问金斯瑞官网 https://www.genscript.com.cn/

## 1.2 蓬勃生物安全合规认证

蓬勃生物遵守国际权威的安全标准及行业要求，并整合所有业务范围，将数据安全防护、监管、治理、保障制度融入每个流程中。蓬勃生物与数据安全领域专业、独立的第三方安全服务、咨询和审计机构进行合作，以外部专业权威机构的视角，对蓬勃生物数据安全的合规性进行评估，我们的认证和合规凭证如下所示：

### 1.2.1 ISO9001

ISO9001 标准是国际标准化组织颁发的一套具有质量管理及质量保证性质的国际标准，专门针对企业的质量管理。蓬勃生物提供抗体、蛋白药物分子发现及药理药效研究服务，抗体药物和蛋白药物临床前药学开发服务，临床前药学研究和临床样品制备服务，提供基因治疗与细胞治疗中质粒的开发与生产外包服务，提供基因治疗与细胞治疗中病毒的开发与生产外包服务，提供基因治疗、细胞治疗及预防性疫苗等领域中 mRNA 的开发与生产外包服务等均已通过 ISO9001 质量管理体系认证，是公司各项管理工作的规范化、标准化的全面检测，是对公司持续稳定健康发展的重要保证。蓬勃生物将严格执行质量管理体系及企业各项规章制度，严格按照标准进行生产作业，持续提升产品质量，更好的为客户提供优质产品和服务。

### 1.2.2 ISO27001

ISO27001 是一套获得业界广泛认可的信息安全管理体系标准，其一直被认为是国际最权威、最严格的信息安全体系认证标准，为各类组织建立并运行信息安全管理体系提供了最佳实践指导。蓬勃生物与金斯瑞生物科技股份有限公司的所有关联公司共享同一个综合的 IT 系统，该系统由金斯瑞生物科技股份有限公司的信息技术部门进行开发运维和支持。金斯瑞生物科技股份有限公司的信息技术部门通过此项认证意味着我们在信息安全管理领域已经与国际标准对标，具有充分的信息安全风险识别和控制能力，可以为全球客户提供安全可靠的服务。

# 2. 数据安全防护设计

## 2.1 数据安全防护目标

蓬勃生物为数据安全设计了全面可信的防御体系，有效保护数据在全生命周期过程中的安全，达到合法采集、合理利用、静态可知、动态可控的防护目标。

- 合法采集

利用大数据分拣技术，使企业在法律约束范围内合法采集敏感数据。

- 合理利用

通过建立数据模型，以及对数据的敏感级别进行划分，设立不同的访问层级，在数据被开发利用前做好防护措施，杜绝非法滥用。

- 静态可知

对存储中的静态数据进行扫描发现，并展示数据的分布。

- 动态可控

对流动的数据进行监控，防止数据在交互、共享中有意无意的泄露。

## 2.2 蓬勃生物数据安全体系建设方法论

蓬勃生物数据安全治理体系建设的步骤，结合数据安全治理框架，定义了数据安全建设的五个阶段，及业务梳理、分级分类、策略制定、技术管控、策略优化。

数据安全就是对数据的安全治理，是从制度到数据的全生命周期的监察与保护。

蓬勃生物结合公司业务的需求，以及对实际环境的调研，总结出了一套完整又科学的数据安全治理方法，即“知”、“识”、“控”、“察”、“行”。

- “知”

分析公司和行业制度、梳理业务及人员对数据的使用规范，定义敏感数据。

- “识”

根据定义好的敏感数据，进行数据定位、数据分类、数据分级。

- “控”

根据敏感数据的级别，设定数据在全生命周期中的可用范围，利用制度、管理平台对数据进行细粒度的权限管控。

- “察”

对数据进行监督监察，保障数据在可控范围内正常使用的同时，也对非法的数据行为进行了记录，为事后取证留下了清晰准确的日志信息。

- “行”

对不断变化的数据做持续性的跟踪，提供策略优化与持续运营的服务。

蓬勃生物将数据安全治理方法“知”、“识”、“控”、“察”、“行”应用于公司业务运营中，实时监督数据风险，对数据的可视化监控、风险点排除，及时预警、及时阻止对数据的非法使用行为，最后对数据安全进行持续运营，让数据始终处于被监控的安全状态，当有新的拓展业务时，蓬勃生物有能力根据此数据治理方法快速的实现新数据的全面安全管控。

## 2.3 多异地业务安全策略

蓬勃生物已建立全球化的数据存储中心，将根据客户所在国家和地区的合规要求，及客户选择，将客户数据存储于美国、新加坡、中国大陆的数据中心。同时按照数据分类，对企业、用户重要类别数据进行加密存储，提高重要类别数据的安全性。数据每日增量备份，每周全量备份，定期进行恢复测试，确保客户数据安全。目前不同数据中心业务数据安全管控策略如下：

| | 中国 IT 团队 | | | 美国 IT 团队 | | |
|---|---|---|---|---|---|---|
| 数据中心 | 应用开发 | 应用部署调试 | 底层环境调试 | 应用开发 | 应用部署调试 | 底层环境调试 |
| 中国数据中心 | √ | √ | √ | × | × | × |
| 美国数据中心 | √ | × | × | × | √ | √ |
| 新加坡数据中心 | √ | × | × | × | √ | √ |

# 3. 金斯瑞集团数据安全支持组织

## 3.1 风险管理和环境、社会及管治委员会

金斯瑞集团为适应全球化战略布局，管理经营过程中的各类风险、内部控制系统及 ESG 策略，高效支撑业务发展的需要，成立了风险管理和环境、社会及管治委员会，其主要职责包括：

- 检讨本集团的风险管理政策及标准、内部控制系统与环境、社会及管治（「ESG」）政策及指引，以及合规管理的基本概念及范围；
- 监督指导并牵头组织风险管理工作的开展；
- 定期审阅风险并将主要风险与战略计划相匹配；
- 持续识别、分析、评估、监控及汇报风险；
- 计划与实施风险管理措施来控制风险。

## 3.2 信息安全委员会

金斯瑞集团为建设集团信息安全体系，成立了集团的信息安全领导机构——信息安全委员会，主要职责包括研究决定信息安全工作涉及到的重大事项，审定集团信息安全方针、目标、工作计划和重要文件，为信息安全工作的有序推进和信息安全管理体系的有效运行提供必要的资源。集团的信息安全职能由信息安全部承担，其主要职责包括：

- 制订、落实信息安全工作计划；
- 对单位、部门信息安全工作进行检查、指导和协调；
- 建立健全企业的信息安全管理体系，保持其有效、持续运行。

## 3.3 数据合规委员会

金斯瑞集团为符合法律法规和行业监管机构对数据合规性的要求，成立了集团数据合规委员会，其主要职责包括：

- 明确数据合规建设工作目标；
- 组织落实数据合规建设要求，完成合规风险排查等各项工作；
- 及时跟踪法律法规政策等变化和业务需求的调整，定期评估数据合规管理情况，持续改进数据合规管理水平；
- 制定、审核相关制度规范，并监督落实情况。

## 3.4 生物安全委员会

金斯瑞集团为统筹集团生物安全相关事项，确保集团业务合规开展，保障实验室生物安全，成立了生物安全委员会，其主要职责包括：

- 制定和审核生物安全相关的政策方针；
- 对生物安全相关的重大事项进行决策；
- 监督指导 BU 子委员会履行生物安全管理要求，子委员会职责包括但不限于下列事项：

（1） 建立并落实实验室生物安全管理制度；

（2） 进行生物安全风险评估；

（3） 规划评估病原微生物、人类遗传资源的相关业务；

（4） 开展人类遗传资源研究利用的对外申报；

（5） 定期评估业务的生物安全合规性等。

## 3.5 特别说明

目前蓬勃生物作为金斯瑞集团的控股子公司，深入参与了集团上述所有的委员会，并且按照集团统一的标准和要求，建立信息防火墙，保障蓬勃生物自身的数据安全、持续良性运营。

# 4. 蓬勃生物数据生命周期安全管理

## 4.1 数据采集

在数据收集和产生阶段，蓬勃生物遵循国家法律法规、数据抽取汇聚流程的要求，对数据尤其是业务数据的采集和获取过程执行有效的安全控制，以保证对各类数据的合规收集，并对收集数据进行分类分级和质量控制。

### 4.1.1 数据分类分级管理

数据分类分级，本质上是对数据资产进行摸底，蓬勃生物对数据资产的业务属性，使用情况，权限状态，安全需求，使用分布等进行了全面的梳理，并按照一定的策略和方法进行分类和标识，在企业层面形成数据资产分类清单，明确数据安全主体责任及防护边界；在分类的基础上，蓬勃生物综合分析数据的保密性、完整性、可用性和可控性等属性遭到破坏后，对国家安全、公众权益、客户隐私、企业合法权益的危害程度，进行数据的逐类安全定级和标识，并明确各级别各类型的安全需求，配套相应保障措施，实现分类分级安全管理。

| 密级 | 定义 | 举例 |
| --- | --- | --- |
| 绝密 | 指极其保密的信息。任何不经许可的传播都会对公司的持续经营造成极其严重的威胁和损害。 | 如未经公告的公司业绩、专有技术资料、客户提供的基因质粒等具有知识产权的实物资产； |
| 秘密 | 指限定特定人群知晓的信息。不经许可的传播可能会对公司的正常经营造成威胁和损害。 | 如组织架构、订单信息、原始实验数据等； |
| 内部公开 | 指在公司范围内向全员发布，而无意向社会公开的信息。 | 如内部招聘启事、公司活动通知等； |
| 外部公开 | 指不受限制，可对外发布的信息。 | 如正式对外披露的公司年报、公司宣传材料等。 |

### 4.1.2 数据采集安全管理

蓬勃生物依照法律、行政法规的规定和与用户的约定，处理其相关数据，在满足相关法定规则的前提下，平衡数据应用和数据安全保护需求，建立一系列数据安全保护制度，明确数据采集的目的、用途、方式、范围、采集源、采集渠道等内容，对数据进行合法性和正当性的确认。

## 4.2 数据存储安全

在数据存储阶段，蓬勃生物对存储的介质、存储容器进行安全管理，并对存储的敏感数据加强安全保护措施，做好重要数据的备份与恢复措施，确保数据存储阶段的安全。

### 4.2.1 存储介质安全管理

数据存储介质即作为数据存储的媒介也作为数据过度传输的媒介，包含物理实体介质（磁盘/硬盘/光盘），虚拟存储介质（容器/虚拟盘）等，蓬勃生物在使用存储介质存储的时候规定了使用安全规范，避免不当使用而引发数据泄露风险。具体包括：

- 存储介质分类，例如物理实体介质（磁盘/硬盘/光盘），虚拟存储介质（容器/虚拟盘）等；
- 将存储介质进行分级，明确定义不同分级的存储介质对存储数据的要求；
- 介质使用规范，建立介质申请和使用人登记制度等；
- 存储介质使用审批和净化处理要求，例如对介质访问的身份识别，权限控制，以及数据清理或销毁等；
- 存储介质标记要求，例如标签及其有效期等；
- 存储介质使用审查，对介质定期检查，以防信息丢失。

### 4.2.2 逻辑存储安全管理

蓬勃生物针对存储容器和存储架构的安全要求，包括认证鉴权、访问控制、日志管理、文件防病毒等安全配置，以及安全配置策略，以保证数据存储安全。制定逻辑存储规范，包括：

- 逻辑存储系统和存储设备定义，如云存储对象、块存储、分布式存储等；
- 逻辑存储的安全配置规则，包括：认证鉴权、访问控制、安全策略等，以及配置变更和发布要求；
- 逻辑存储的多租户隔离、授权管理规范要求；
- 存储设备安全管理规范和操作规程，如标准操作流程、维护操作流程、应急操作流程等；
- 存储系统的账号和权限、日志管理、加密管理、版本升级等要求。

### 4.2.3 数据存储加密管理

为保障数据在存储中的机密性、完整性，蓬勃生物采用加密技术对数据进行加密存储，防止授权的数据被窃取、伪造和篡改等安全风险，保障数据在存储时的安全性。基于数据不同的类别和级别进行有针对性的加密保护，尤其对个人信息、重要数据等敏感数据采用加密存储，无论是内部还是外部、有意还是无意的泄露，蓬勃生物都可以保障敏感数据安全。

蓬勃生物根据国家法律法规的要求，结合自身业务数据对保密性和完整性的需求，在数据分类分级的基础上，确定需要加密存储的场景，凡是涉及到敏感业务数据或者其他对机密性和完整性要求较高的数据存储场景，都进行加密存储。

### 4.2.4 数据备份和恢复管理

灾难的发生往往是出乎人们意料的，在数据系统由于各种不可控因素崩溃的时候，没有数据备份就没法找到数据。为保障信息系统和数据高可用性，蓬勃生物定期执行数据备份和恢复验证测试，实现对存储数据的冗余管理。

## 4.3 数据传输安全

### 4.3.1 数据传输加密

蓬勃生物采用加密保护措施，防止数据在通过不可信或者较低安全性的网络进行传输时，发生数据被窃取、伪造和篡改等安全风险，保障数据在传输过程中的安全性，例如采用 TLS 协议保障传输链路的加密、VPN 设备建立加密隧道等。

### 4.3.2 数据传输泄露防护

蓬勃生物利用数据传输防泄漏工具对传输过程中的数据进行泄露防护和审计，保障数据在传输过程中的安全，尤其是对非结构化数据的传输和外发。

## 4.4 数据处理安全

在数据开放、共享、分析等处理过程中，蓬勃生物为了防止内部敏感数据尤其是业务机密数据被损坏、丢失或窃取，建立数据处理的环境安全保护机制，并对使用的权限以最小化原则进行梳理和控制，同时对其敏感数据的开放、共享、分析等特定场景进行脱敏处理，以此达到数据处理过程中的保障数据安全的目的。

### 4.4.1 数据分析安全管理

蓬勃生物通过在数据分析过程采取适当的安全控制措施，防止数据处理过程中有价值信息和机密信息泄露的安全风险，并防止复原匿名化数据，进而识别特定客户或者项目，获取有价值的业务信息或敏感数据，制定数据分析过程中数据资源操作规范和实施指南，明确各种分析算法可获取的数据来源和授权使用范围，并明确相关的数据保护要求。

### 4.4.2 数据开放安全管理

蓬勃生物建立数据开放管理制度，在数据分类分级的基础上，针对可对开放的数据进行开放前、开放中、开放后安全管理过程，包括开放前的数据内容、开放范围等审核，开放中对定期审查，以及开放后可能出现不良影响的应急处理机制。

### 4.4.3 数据共享安全管理

蓬勃生物在数据分类分级的基础上，基于数据自身的业务属性定义共享级别及相对应的保护措施，明确共享数据的类型、数据内容、数据格式及共享的场景和范围。建立数据共享审核流程，明确共享的用途等，并定期审核。

### 4.4.4 数据接口安全管理

蓬勃生物制定数据接口安全开发规范，在明确数据接口调用的目的、用途等内容的前提下，对接口的安全开发设计进行统一的定义和要求。

### 4.4.5 数据脱敏管理

蓬勃生物利用脱敏工具对敏感信息按脱敏要求进行脱敏处理，保障生产数据尤其是客户、项目信息数据在分析过程和结果输出是安全的，针对业务信息的脱敏以无法复原和定位具体客户、订单、项目为原则，对唯一标识信息（订单等）必须脱敏处理。

- 数据脱敏规则

通过脱敏技术实现对数值和文本类型的数据脱敏，支持多种脱敏方式，包括不可逆加密、区间随机、掩码替换等。

- 脱敏数据转发

满足多重数据脱敏转发方式，蓬勃生物设计的脱敏场景多样性，支持广泛的数据脱敏分发方式，脱敏后的数据可以实时的上传到目标数据库或文件服务器，也可以保存在脱敏服务本地，按需转发实现一次脱敏多次使用。

- 数据对比校验

蓬勃生物具备脱敏前后数据校验功能，从数据库结构、数据对象、表数量、表内数据量等维度对比分析源库数据和目标库数据的差异。

### 4.4.6 数据传输加密管理

蓬勃生物利用传输加密设备对传输过程中的数据进行保护，防止接口传输数据被篡改、伪装等，保护接口调用数据的完整性和保密性，同时对接口调用的人员身份认证和审计。

### 4.4.7 数据销毁安全管理

蓬勃生物通过建立对存储数据销毁的规程，包括数据及存储介质的销毁申请、审批和销毁的流程和要求等，防止因存储数据丢失、被窃或未授权的访问而导致的存储媒体中的数据泄露的安全风险。

制定数据销毁的审批流程及管理办法，包含数据销毁和介质销毁。包含：

- 明确销毁的场景：什么场景下需要做数据销毁，结合业务和数据重要性需要；
- 审批：建立符合数据销毁策略和管理制度的销毁审批机制，对销毁进行严格审批。

- 销毁：在销毁审批后，以不可逆的方式销毁数据内容。
- 记录：对数据销毁处理过程操作做进行记录，以满足安全审计要求。

# 5. 访问控制措施

## 5.1 安全访问管理

为明确蓬勃生物信息访问的控制要求，防止未经授权的访问，加强对远程工作的管理，确保在远程工作场地访问、处理或存储公司信息的安全性，根据相关法律法规及监管要求，并结合公司业务情况，制订了蓬勃生物安全访问管理流程。

### 5.1.1 认证与登录

#### 5.1.1.1 账号分类

在系统中建立的账号分为以下类别：用户账号、管理员账号、应急账号、系统服务账号、系统默认账号；

- 用户账号：给予用户进行应用系统中业务操作；
- 管理员账号：给予管理员建立、更改信息系统参数配置，建立、更改、删除用户账号，激活、重置账号密码等操作；
- 应急账号：日常操作不应使用的账号，仅在紧急情况（如用户账号、管理员账号均异常）下临时使用；
- 系统服务账号：用于系统与系统间的连接，系统服务的启停；
- 系统默认账号：指系统或应用初始安装使用时即已构建在操作系统、应用系统上的账号；
- 临时账号：特指为了满足某项临时性或一次性工作，特殊开设的临时账号，通常该账号有效期不超过 3 天，该类账号禁止增、删、改权限。

#### 5.1.1.2 认证标准

认证数据是指在认证方式中用于确认用户身份的信息，包括但不限于密码、动态口令、交易认证信息如 PIN、CVV2 等；蓬勃生物所有保存秘密及以上级别信息的系统，相应人员均以密码认证或强效认证来鉴别用户身份，保护信息的保密性、完整性和可用性；所有认证数据，包括但不限于密码、动态口令、PIN、CVV2 等，在储存、传输中都加以保护，如采用有效的加密保护，以防泄露或被未获授权的修改；所有高风险系统（如资金管理系统、财务系统）的访问，蓬勃生物均使用强效认证，包括但不限于双因素认证、生物识别认证等。

用户一旦发现其账号有异常活动，将立即修改密码，如有必要可通知信息安全部进行协助调查，如调查为账号被盗、撞库、暴力破解等攻击行为或信息安全事件，则报备至信息安全管理者代表。

#### 5.1.1.3 登陆标准

蓬勃生物内部的信息系统在登陆方面，有以下安全管控措施：

- 内部信息系统在登录系统前，会显示恰当的登录警告语或安全建议
- 信息系统的登录功能禁止默认显示明文密码，能够通过日志记录成功与失败的登陆信息；
- 登陆失败时不显示原始的登陆失败原因，如因为账号不存在或密码错误的登陆失败，均显示为“账号密码不匹配”或“登陆认证失败”；

- 设置合适的登陆失败控制措施，如一定时间内连续 5 次登录认证失败锁定当前尝试登陆的账号或 IP 地址，一定时间内不得允许成功登录；
- 配置开启会话超时，当系统空闲超过 30 分钟自动断开连接或自动注销当前的用户登录，如果系统没有空闲超时控制，有其它措施来辅助实现，如 Windows 的屏幕保护程序；
- 对单个系统的最大并发会话连接数进行限制；
- 对单个账户的多重并发会话连接数进行限制。

### 5.1.2 账号管理

账号是一个信息平台进行准入的最重要、使用最频繁的凭证，而各个业务系统同时也是数据的载体，蓬勃生物为保证数据安全，针对账号管理，通过以下措施保障账户相关的安全管理：

#### 5.1.2.1 账号标准

- 所有账号有指定的拥有人；
- 所有账号使用实名制，确保所有账号可以精确到使用人，原则上不允许多人共用同一账号；
- 在特殊情况下如确需多人共用同一账号，必须经过信息安全管理者代表批准且做好账号的使用管理记录，以便可以对账号的使用情况进行跟踪审查。
- 账号拥有人负责所持有账号的安全使用，因自己使用不当或保管不当造成账号被他人使用而产生的违反公司信息安全规定、损害公司或他人利益的一切不良后果均由账号拥有人自行承担；
- 如用户账号连续 90 天没有产生使用记录，该账号将被禁用或限制登陆。

#### 5.1.2.2 账号管理策略

- 所有账号的建立及权限增加通过申请相关流程，并获得部门领导或其委托者的批准，账号管理员审核申请人访问该信息系统在业务上的必要性并确认只授予申请人最小限度的系统权限；
- 业务部门或账号管理员每半年复核用户账号的必要性及权限的适当性，一旦发现不适当的系统访问权限将立即作出相应的修正。账号复核修正只限于账号及权限的删除，账号建立和权限增加禁止以账号复核替代账号审批流程；
- 当人员离职时，账号将在离职当日被禁用；
- 账号被禁用或被锁定，必须经账号管理员确认用户身份后或经公司信息安全部核准的自动解锁／密码重置设施，方能恢复账号和解除锁定；
- 系统服务账号是系统底层账号，只能用于系统与系统间的通讯或启停系统服务，禁止被用作系统管理、维护等其它用途；
- 系统默认账号必须被禁用、锁定、更改或作适当的配置，防止被使用，任何系统及设备账号的默认密码，在系统配置完成后将立即更改；
- 应急账号在紧急情况使用时，必须在两个获授权人员互相监督下使用，并确保没有一个人员独自知悉完整账号密码；

- 对于特权工具的特殊权限尽力控制在最小的范围内，对特殊权限的授权有经信息安全部批准后才可实施，信息安全部定期对特权账号进行评审。

#### 5.1.2.3 密码管理

密码作为账户信息中最敏感的内容，一旦泄露，将造成严重的后果，为此蓬勃生物通过以下措施对密码进行严格管控：

- 密码长度必须大于等于 8 位；
- 密码必须包含大写字母、小写字母、数字和符号中的三种或三种以上元素；
- 密码不可包含用户帐户名称的全部或部分文字；
- 启用账号风险告警，一旦检测到账号存在风险即强制要求修改密码，新设定密码不能与最近 6 次使用过的密码相同。
- 员工不得在计算机或纸张上以无保护的形式记录密码；
- 员工必须避免在不同环境使用同一密码；
- 禁止通过传真等明文方式传送密码，通过邮件传送账号和密码时，必须将账号和密码分次传送，并在传送完毕后通过非邮件的方式与接收人确认是否已接收；
- 员工忘记密码时，管理员在对该用户进行适当的身份识别后才能向其提供临时密码或协助重置密码。

## 5.2 授权管理

数据权限是蓬勃生物控制数据访问、变更、销毁的依据，根据“最小化授权”原则，蓬勃生物指定数据授权管理方法如下：

### 5.2.1 授权原则

- 权限必须以角色的形式授予账号，各角色的权限根据角色的职能授予；
- 授权必须细化到每个功能，每个行动可以分开授予，如信息资产的读、写、修改、删除、执行等行动分别授予权限；
- 授权请求必须基于合理的工作目的，并经过部门主管及信息拥有人或其指定管理人的确认；
- 信息访问的授权必须遵循“权限最小化”原则，每个用户分配的权限以完成本岗位工作最低标准为准；
- 信息访问的授权必须遵循职责分离的要求，禁止存在冲突的授权。

### 5.2.2 访问管理

- 公司所有信息系统必须具备访问控制功能，所有存储有保密信息的信息资产设置有访问控制策略；
- 访问策略中清晰定义每个用户或每组用户的访问控制规则及拥有的权限；
- 当用户持有的账号、权限不适用（如异动、离职）时，及时删除或禁用相关账号、权限。

### 5.2.3 网络及网络服务访问控制管理

- 对网络和网络服务进行管控，确保用户只能访问已获授权的网络和网络服务；
- 采用防火墙技术和虚拟局城网（VLAN)技术实现网络域的逻辑分离，并保证各个网络域之间只有授权的信息流交换；
- 保持严格的分离控制措施，保证跨边界的网络访问安全；
- 防火墙策略设计遵守“默认拒绝”原则，只允许必须的信息流通过网络，阻止未授权 IP 地址访问；
- 外部连接用户访问内部网络或系统使用 VPN 加密或远程桌面等安全方式进行连接；
- 对日常工作不需要使用的信息处理设施的远程诊断和配置端口进行严格控制，默认设置成禁用，需要时再进行开启；
- 外部访客原则上只可以接入公司的访客网络，未经信息技术部部门负责人或信息安全管理者代表授权不得接入公司办公网络；
- 定期对网络访问控制策略进行复审，防止访问控制策略不适宜或不正确。

# 6. 物理安全

## 6.1 物理安全区域划分

蓬勃生物对物理安全区域进行划分，做到分级管理、分类管控，具体的划分原则如下：

- 业务优先原则：在保障业务正常运行和运行效率的基础上建立防护体系；
- 结构简化原则：便于设计防护体系，安全区域尽可能简化；
- 等级保护原则：每个安全区域的信息资产价值相近，具有相同或相近的安全等级、安全环境、安全策略等；
- 逐步细化原则：每个安全区域的安全防护措施会随着实际情况不断调整和细化。

根据以上原则，蓬勃生物以各部门区域所拥有的信息资产最高保密级别（参考《信息安全管理制度》中密级分类方法、ISO22301 业务连续性管理中 BIA 业务影响分析方法）为依据判断业务影响级别（Business Impact Level，BIL），同时综合考虑可能面临的威胁及风险进行划定各部门安全区域。划分考量因素如下：

- 资产价值平均值考量：根据各部门使用的资产价值平均值判定安全等级，其中如包含高安全等级的特殊资产可在部门内部划分子安全领域，该子安全领域可根据高安全等级领域的安全措施进行管理，其中密级划分可参考公司《信息安全管理制度》：
  - 包含大量 “绝密”文件（≧5 份）为“极高”资产价值；
  - 包含一定数量“绝密”文件（2≦份数<5）为“较高”资产价值；
  - 包含少量“绝密”文件（<2）为“高”资产价值；
  - 包含大量“秘密”文件（≧5 份）但没有“绝密”文件为“中”资产价值；
  - 仅有少量“秘密”文件（<2 份）为“低”资产价值。
- 风险等级考量：针对各部门实际存在的信息风险等级和威胁严重程度，可以考虑增加其安全等级防护措施（风险等级评定依据《信息安全风险评估管理细则》风险评估测评结果分为极高、较高、高、中、低五种），其中“极高”风险安全等级必须立即停止业务进行风险处置。
- 法规标准考量：参考各部门在经营中所依据的国内外法律、法规、标准以及公司制定的制度等要求，可适当增加高等级的安全措施。

基于以上划分原则，目前将蓬勃生物物理区域划分为四级安全等级，最高为四级，最低为一级。典型物理安全区域划分具体如下：

| 安全区域等级 | 划分因素等级 | 典型区域 |
| --- | --- | --- |
| 一级 | 资产价值和风险等级均为“低”，且无法规要求 | 接待室、停车场、食堂大厅 |

| | | |
|---|---|---|
| 二级 | 资产价值和风险等级至少有一个为“中”但没有“较高”等级 | 一般办公区域（不包括机房、档案室以及财务、人事、投资者关系部、采购、市场、内审、IT 等部门）以及进出口部的交接区等 |
| 三级 | 资产价值和风险等级至少有一个为“较高”但没有“极高” 等级，法规有一定要求 | 所有生产区域、员工宿舍<br>办公区域中的财务、人事、采购、市场、内审、IT、高管（VP 以上级别）办公室等 |
| 四级 | 资产价值和风险等级至少有一个为“极高”，或法规有明确要求 | 研发部门重点实验室、核心机房、档案室、投资者关系部（IR）资料室、消防监控室、消防泵房、配电房、食堂后厨等。 |

## 6.2 物理安全控制

蓬勃生物作为生物科技领先企业，着力为每一个客户提供安全、稳定、持续、可靠的服务，依据数据中心相关的国际标准和监管要求，建立了一套全方位的安全管理体系，从制度策略，到流程管理，并配合严格的监察审计，通过持续改进来保证业务环境的物理安全。

蓬勃生物在公司物理环境入口和边界部署相应的安全控制措施，防止未经授权进入公司受保护区域。公司依据不同安全区域的等级制定物理安全、访问控制、安全管理等三个方面安全措施，原则上同级别物理区域所采取的物理措施要求一致。具体安全措施清单如下：

| 安全区域 | 安全措施 | 一级 | 二级 | 三级 | 四级 |
|---|---|---|---|---|---|
| 物理安全措施 | 建筑标准 | × | × | × | 专用标准房间 |
| | 监控区域 | 出入口 | 出入口 | 对角线监控 | 全方位监控 |
| | 门禁系统 | 门锁 | 门锁 | 门锁/门禁 | 门禁/指纹 |
| | 报警系统 | × | × | × | 入侵报警系统 |
| | 安全标识 | × | × | 醒目标识 | 重点标识（隐藏名称） |
| 访问控制 | 访问人员 | 访客\一般员工 | 访客\一般员工 | (部门）员工陪同 | 专职管理员工 |

| | | | | | |
|---|---|---|---|---|---|
| | 身份鉴别 | 员工证 | 员工证 | （部门）员工证 | 专职管理员工证\指纹识别 |
| | 访问管理 | × | × | × | 访问记录 |
| 安全管理 | 安全审计 | 日常巡查 | 日常巡查 | 日常巡查季度审计 | 日常巡查季度审计 |
| | 经验教训培训学习 | × | 通告学习 | 季度培训 | 季度培训 |

## 6.3 物理安全防护措施

### 6.3.1 环境安全控制

蓬勃生物在环境安全控制上，遵守以下原则：

- 安全区域的选址充分考虑火灾、水灾、地震、雷电、爆炸、骚乱等自然和人为灾难，并采取额外的控制措施加以保护；
- 安全区域的建设满足国家相关要求且部署充分的防火、防水、防潮、防盗等措施；
- 安全区域供电充分考虑其可用性，确保日常工作不受异常电力中断的影响；
- 安全区域消防管理满足国家消防要求，并经过当地消防局的检查，机房及档案室使用气体消防系统；
- 机房区域设置温湿度自动调节设施，并对关键设备或关键区域实施电磁屏蔽。

### 6.3.2 建筑安全标准

蓬勃生物对物理建筑安全标准进行严格把控，原则如下：

- 核心机房依据《数据中心设计规范》(GB50174-2017)B 级数据中心建设；
- 公司档案室参考《档案馆建筑设计规范》（JGJ25-2010）、《企业数字档案馆（室）建设指南》等标准建设；
- 研发部门实验室可依据世界通用生物安全水平标准、《生物安全实验室建筑技术规范》（GB50346-2011）等相关法规标准建设；
- 重要部门（投资者关系部资料室、财务部门资料室等）房间按照 ISO27001 标准建议，设置接待区域，且保管的重要资产放入加锁文件柜、保险箱或信息系统中；
- 各区域电缆设计均规范合理，电力电缆与通信电缆相隔离，不同供电电压与频率的电力电缆也相互隔离，防止发生干扰。

### 6.3.3 监控区域

对于机房监控、安防管理，蓬勃生物制定安全管理规定如下：

- 三级以下安全区域仅需在出入口及关键通道上设置监控设备，监控录像保存 30 天及以上；
- 三级安全区域需在内部安装监控设备，监控录像保存 30 天及以上；
- 四级安全区域需在内部 360 度无死角监控，监控录像保存 90 天及以上。

### 6.3.4 门禁系统

蓬勃生物数据中心、办公大楼等场地门禁安全管控政策如下

- 四级以下安全区域需在出入口安装门锁或电子门禁，门锁钥匙、门禁权限由专人负责；
- 四级安全区域须安装门禁系统和指纹识别系统，出入记录保存 180 天以上。

### 6.3.5 报警系统

蓬勃生物告警系统管理标准如下：

- 三级以下安全区域除厂区界线有红外对射报警系统外，可不再加装其他报警系统；
- 四级安全区域须加装入侵防范报警系统，防止未授权人员非法闯入。

## 6.4 人员访问管理

所有进入蓬勃生物公司安全区域的人员都必须经过授权，所有员工必须佩戴员工证，外部访客进入公司安全区域必须登记且得到授权才能进入，公司南门和东门岗亭为访客交接区域。

### 6.4.1 外来访问人员要管控

针对外来访问人员要求，蓬勃生物规定如下：

- 三级以下安全区域凭访客证/员工证可以进入，外部访客由公司员工陪同进入；
- 三级安全区域须经过 OA 上的“AM06-来宾接待申请流程”申请后，由该区域员工陪同方可进入；
- 四级安全区域原则上仅专职工作人员进入，其他员工或特殊访客须向主管部门申请后由公司专职管理人员陪同进入，并进行人员进出和工作内容登记，记录保存 90 天以上；
- 清洁人员和保安人员应统一着装且佩戴统一的身份标识，清洁人员或保安人员进入四级安全区域应有该区域员工在场陪同。

### 6.4.2 身份鉴别管控

对于人员身份鉴别，蓬勃生物规定如下：

- 在公司各安全区域内活动的人员都应佩戴公司员工证或访客证，员工不得将自己的员工证转借他人，如果员工证遗失，应尽快与人力部门联系；
- 三级以下安全区域使用公司员工证即可通行；
- 三级安全区域须在员工证上开通该安全区域权限方可进入；
- 四级安全区域须在员工证和指纹上同时开通该安全区域权限方可进入。

### 6.4.3 访问管理管控

对于人员访问，蓬勃生物制定标准如下：

- 三级以下安全区域无须单独申请权限；
- 三级以上安全区域需根据员工实际岗位需求单独授权；
- 员工离职时应将员工证交还给部门助理，部门助理将员工证交给人力部门，同时取消其所有访问权限。

### 6.4.4 设备进出安全区域要求

设备作为数据的可能载体，蓬勃生物同样对设备进行管控，并制定标准如下：

- 未经许可严禁将安全区域内信息设备搬离，安全区域内的信息设备搬离应事先由设备所属部门负责人签字，向信息技术部获取书面批准后，才能搬离；
- 进入安全区域搬卸设备的外来人员应参照访客人员管理要求提前获取授权，公司员工应全程陪同。

### 6.4.5 人员检查、培训和考核

蓬勃生物针对各安全区域的信息设备进行定期进行预防性维护，并明确维护人员的责任、维护过程的监督控制，每年至少对机房和档案室的相关设施进行一次全面检查，并组织人员培训、考核，具体做法如下：

- 一级和二级安全区域通过日常巡查的方式检查安全措施，三级和四级安全区域通过日常巡查和季度审计的方式检查安全措施；
- 三级以下安全区域工作人员可根据实际情况通过信息安全通告和信息安全部组织的专项培训学习信息安全事件经验；
- 三级以上安全区域工作人员每年应参加信息安全部组织的信息安全培训与考核，学习总结国内外发生的信息安全案例，减少未来该类事件发生的可能性和影响。

# 7. 运行安全

## 7.1 终端安全

企业内部终端会存储、处理、交换大量敏感数据，一方面终端环境的复杂、多变等都给终端数据安全管控带来更多的挑战，另一方面在不同人员角色、复杂使用场景及跨系统的数据流动下，给数据安全带来更多的威胁。对于以上问题，蓬勃生物建立相关管理和技术的终端保护措施来保证数据可用性和安全性。

### 7.1.1 桌面安全管理

对终端计算机的桌面行为监控、审计和管理。系统对终端计算机上的文件访问、上网行为、程序使用、端口通信、网络共享、打印等行为进行审计和管理，同时也对终端计算机进行桌面消息通知、远程计算机操作、远程协助、远程控制、流量管理等管理操作。桌面安全管理包括桌面安全及审计和桌面管理与运维两个部分。

### 7.1.2 桌面安全及审计

- 桌面用户、权限和密码管理
- 终端计算机端口管理
- 防病毒软件管理
- 终端用户变化审计
- 文件访问审计与管理
- 上网行为审计与管理
- 程序使用审计与管理
- 即时通讯程序审计与管理
- 网络端口通信审计
- 网络共享审计与管理
- 终端用户屏幕审计
- 打印行为审计与管理

### 7.1.3 桌面管理及运维

- 进程运行管理
- 软件和启动组管理
- 桌面消息通知
- 远程计算机管理
- 系统设置管理

- 网络连接与流量管理
- 终端运行统计

### 7.1.4 存储、外设管理

外设与接口管理主要指对终端计算机上各种外设和接口的使用进行管理。蓬勃生物制定规则禁用终端计算机的各种外设和接口，防止用户非法使用。对于移动存储设备，在禁止使用通用移动存储设备的同时，允许使用经过认证的移动存储设备。

- 存储设备禁用
- 设置移动存储设备只读
- 移动存储设备认证
- 外设和接口禁用
- 在线/离线策略管理

### 7.1.5 安全准入与非法外联

蓬勃生物建立数据安全监控平台，主要用于发现和管理内部人员非法建立通路连接互联网或非授权网络的行为。通过对非法外联的监控管理，防止人员非法访问互联网或非信任网络资源，并防止引入安全风险或导致信息泄密。

- 在线主机监测
- 主机授权认证
- 非法主机网络阻断
- IP 和 MAC 绑定管理
- 终端非法外联行为监控
- 终端非法外联行为阻止

### 7.1.6 补丁分发管理

补丁分发管理主要完成对终端计算机的系统补丁检测和补丁分发安装，增强终端计算机的健壮性。蓬勃生物内部的安全管理员也可以自定义软件分发，完成员工应用系统的软件和补丁管理。

- 终端计算机漏洞自动分析
- 补丁分发
- 补丁分发策略管理
- 补丁完整性和兼容性测试
- 补丁管理
- 流量控制

## 7.2 网络安全

### 7.2.1 安全防护设备

安全防护设备是企业整体安全防护的基本单元，蓬勃生物为综合、全面地保护内部信息资产，从网络、主机、应用、数据层面，部署了相应的安全防护设备。

目前蓬勃生物在内网中的安全设备部署、防护概况如下：

- Firewall
- Web Application Firewall
- Intrusion Prevention System
- Intrusion Detection System
- Internet Behavior Management System
- Secure Mail Gateway

## 7.3 日志管理

### 7.3.1 日志级别划分

蓬勃生物将企业内部日志级别划分为 Fatal、Error、Warn、Info、Debug 等级别，对于生产环境日志级别必须在 info 及以上级别，禁止出现 debug 级别日志；同时也按照日志类型，将日志分为系统日志，应用日志，中间件日志和数据库日志四大类。

对于不同类型的日志，蓬勃生物的定义以及安全管理措施如下：

- 系统日志由操作系统（包含虚拟化系统等）、数据库管理系统生成，内容包括系统登录、系统事件、错误信息等；
- 应用日志由应用软件产生，内容包括用户登录、数据业务操作、错误信息、警告信息等；应用日志主要包括以下几大类型：错误、警告、业务审计、程序追踪、业务数据操作、访问日志；
- 中间件日志由各个中间件产生，内容包括数据业务操作、错误信息、警告信息以及缓存数据信息等；
- 数据库日志由数据库产生，包括数据库文件日志和数据库表日志，由各数据库管理方自行管理；
- 各类日志的命名必须统一，比如 pafa 日志，spri 日志，acc 日志，gc 日志等等。

### 7.3.2 日志接入策略

针对日志的搜集过程，蓬勃生物制定管理规定如下：

- 本策略涉及日志收集备份监控等操作，默认为标装环境下各类日志。如果项目需要运行非标装环境，涉及到日志路径、收集、备份以及监控审计等事项，开发部门需在首次部署前与运维部门确定日志管理方案，待方案确定之后再做首次部署工作；

- 新提接入请求需清晰，至少包含需要接入的主机、接入路径、接入日志管理平台的 tag 以及后续管理员 um 权限信息等要素，审批方对接入请求的合理性进行评估，默认新系统首次部署上线后需要提接入日志管理平台请求，时限为 2 个工作日；
- 接入管理平台审批方需要审批接入的具体服务器、日志路径等信息，确认正确合规，接入管理平台审批方应沟通协调、跟踪接入实施过程，默认审批结果反馈时限为 1 个工作日；
- 接入过程中不涉及修改原有需求的问题，在此阶段可以进行修改操作（比如分配账号查看日志格式异常等，在此阶段可以协调修改），如果涉及新的需求则需更新，默认实施操作时限为 2 个工作日，如果有特殊情况需要延期需要提前邮件通知请求方。

### 7.3.3 日志权限管理

针对蓬勃生物内部平台、主机、服务器、业务系统收集的日志内容，公司制定政策标准如下：

- 生产环境主机日志文件查看下载等权限，禁止除运维人员之外人员持有，生产日志必须在日志管理平台查看；
- 外部实施地需要在主机上查看日志的情况，须提服务请求申请服务器日志查看账号，此账号应只具有日志查看权限；
- 日志管理平台针对各个系统配置管理员角色账户，其他人员需要查看日志可向各子系统管理员申请，各部门应依据公司相关要求做好管理员账号的管理；
- 生产环境日志文件如果需要下载，需要请求方提交服务申请，由于公司统一日志管理平台的最短延迟时间等原因，不能满足某些特殊事件处理、问题分析等需求，需要在生产主机实施操作的，须提交日志查询例外申请，审批通过之后由运维同事协助实施；
- 日志查看方后期使用过程中，遇到的问题（包括但不局限于日志切割格式，日志收集新增删除路径等）须及时反馈至接入管理平台审批方，并由接入管理平台审批方协调跟进修正。

### 7.3.4 日志审计策略

关于各类日志安全审计相关策略，蓬勃生物规定如下：

- 日志审计监控方通过日志管理平台对日志进行审计，审计内容包括但不局限于违规操作、异常日志出现频率及期限等，如果发现违规行为，应能够进行告警响应；
- 默认日志审计工具为日志管理平台，后续如有需求会接入日志管理平台以外的供日志管理所使用的日志审计分析工具，确保符合相关法律法规、监管机构及公司的信息安全要求。

# 8. 业务连续性

为了保障蓬勃生物业务的连续性、可靠性，建立信息安全事件报告、响应、评价和惩戒机制，加强和改进信息安全事件管理，在发生信息安全事件后，能够分析事故原因及影响、反馈处理结果、吸取事故教训，同时满足突发情况下信息系统保障和信息系统恢复工作需要，提高应对突发事件的组织管理能力和应急处置能力，有效防范信息系统风险，保障信息系统的稳定运行，将事件和故障造成的损害降到最低程度，蓬勃生物制定了详细的安全应急预案体系。

## 8.1 应急事件分级

蓬勃生物按照各类事件的严重程度、影响范围、响应需求，将应急事件分为以下等级。

| 级别 | 说明 |
| --- | --- |
| 特别重大安全事件（Ⅰ 级） | 涉及公司核心业务的关键信息系统或相关设备设施受到损害，恢复系统/设备功能需要 5 小时或以上时间，造成部门与部门之间、个人与个人之间的信息交流和情报传递极其不通畅；<br>公司绝密信息被泄露、破坏且无法追回或恢复；<br>负面消息引起政府部门或监管机构的高度关注并展开调查，或者引起公众媒体极大关注并呼吁采取行动，对企业声誉造成无法弥补的损害。产生特别重大社会影响乃至损害品牌形象。 |
| 重大安全事件（Ⅱ级） | 公司的关键信息系统或相关设备设施受到损害，恢复系统/设备功能需要大于或等于 3 小时，且小于 5 小时。造成部门与部门之间、个人与个人之间的信息交流和情报传递不通畅；<br>公司秘密信息被泄露或破坏且无法追回或恢复；<br>负面消息在行业内广泛流传，或者被全国性媒体报道，对企业声誉造成重大损害。产生重大社会影响。 |
| 一般安全事件（Ⅲ级） | 关键信息系统/设备设施受影响，恢复系统/设备功能需要大于或等于 1 小时，且小于 3 小时，<br>部门与部门之间、个人与个人之间的信息交流和情报传递受到一定阻碍；<br>内部公开信息 被泄露或破坏且无法追回或恢复；<br>对公司声誉基本没有影响或造成的声誉影响能在短时间内恢复。 |
| 轻微事件（Ⅳ级） | 对营运影响微弱，未导致关键生产系统中断或中断后的恢复时间小于 1 小时，部门与部门之间、个人与个人之间的信息交流和情报传递受到轻微阻碍；<br>信息未被泄露或破坏；<br>不影响企业声誉。 |

## 8.2 应急事件响应流程

为快速响应各类安全事件，及时恢复业务的可用性、机密性、完整性，蓬勃生物制定应急响应流程如下。

### 8.2.1 事件发现

对于观察到的或怀疑的任何系统或服务的信息安全弱点，公司员工必须及时报告给信息安全部，经分析及判断后交由相关的技术人员进行处置，并由信息安全部备案记录在《信息安全事件台账》。

由蓬勃生物信息安全部负责跟踪已备案的信息安全弱点处置情况。

事件、故障、薄弱点在报告受理人到来处理之前，发现人禁止改变现状。未经信息安全部允许，公司员工和外部人员禁止利用测试等方法证明未经证实和确认的信息安全弱点。测试弱点视为对系统可能的滥用，可能导致信息系统和服务的损坏。

### 8.2.2 事件报告

蓬勃生物规定公司全体员工具有责任和义务将已发现的或可疑的事件、故障和薄弱点及时上报。信息安全事件报告采取“谁发现，谁报告”的原则，由发现信息安全事件的人员第一时间上报本部门信息安全代表或通过专用邮箱将事件报告给信息安全部。信息安全部初步分析和判断事件类型及级别，并通知相关负责人处理。

如果发生Ⅰ级或Ⅱ级信息安全事件，信息安全部应及时向流程 IT 部负责人报告，由流程 IT 部负责人向公司风险管理委员会报告，并视情况向外部相关机构报告。

### 8.2.3 事件响应

信息安全事件发生部门、信息安全部根据所发生的信息安全事件的性质、对公司商业活动影响的程度，会同有关部门在第一时间内采取有效措施处理信息安全事件，尽可能减少由于信息安全事件而引发事故所造成的损失。

信息安全部对安全事件做最初响应，原则如下：

- 采取恰当的方式，联系相关机构；
- 采集并保存有效证据，尤其关注牵涉到内部员工的场景；
- 考虑以对本公司信息安全产生最小影响的方式来进行调查，可能需要寻求外部专家的支持。

事件响应及处理者在处理安全事件时应考虑以下优先次序：

- 保护人员的生命与安全；
- 保护敏感的设备和资料；
- 保护重要的数据资源；
- 防止系统被损坏；
- 将公司遭受的损失降至最小。

### 8.2.4 信息收集与调查

信息安全部接到信息安全事件的报告后，在初步判断基础上，将进一步收集相关信息，对事件进行深入的调查，为事件分析、评估与响应策略确定奠定基础。

调查内容包括但不限于：

- 网络设备日志（包括路由器、交换机等日志）；
- 安全设备日志（防火墙、入侵检测系统、防病毒系统日志）；
- 服务器和应用系统日志；
- 监控系统日志；
- 系统正在运行的进程与服务（特别是可以提供远程访问的进程与服务）；
- 可疑的用户账户（特别是非授权账户）；
- 不寻常的隐藏文件；
- 初次发现信息安全事件/迹象的时间和表现形式；
- 事件涉及的系统、用户。

### 8.2.5 分析与评估

基于对事件相关信息的收集与调查，蓬勃生物信息安全部给出对事件的初步判断，进行分析并明确信息事件类型并评估信息安全事件等级。信息安全事件分级会在事件控制和处理过程中结合不断获得的详细信息进行调整。

### 8.2.6 信息安全事件总结

蓬勃生物信息安全部组织开展对信息安全事件处理总结工作，总结事件发生原因，事件处理过程各个阶段的经验教训，并讨论后续的处理意见(包括事件通报、落实整改等)。所有信息安全事件均应填写《信息安全事件台账》，并依据事件处理过程中形成的记录、事件评估结果、事后的调查及经验总结等情况，由信息安全部编写《信息安全事件调查总结报告》，其中Ⅱ级及以上信息安全事件必须编制调查总结报告，Ⅱ级以下信息安全事件根据需要编制该调查总结报告。

### 8.2.7 奖惩

对于所有的信息安全事件，蓬勃生物采取严格审查、严肃处理的态度，制定相应规定如下：

- 为减少信息安全事件的发生，提高信息安全事件处理效率，保证业务连续性，对于在信息安全事件处理中做出贡献的先进部门和个人给予奖励；
- 对于未遵照或不配合前述规程要求的，造成不良影响及损失的个人或部门应给予处罚；

- 具体奖惩措施依据公司《员工奖惩制度》，结合事件的严重程度、造成的损失、产生的原因对违规者进行处罚。

## 8.3 应急演练

为了加强自有业务安全管理，梳理和完善自有业务系统遇到突发事件后应急处理流程，缩短系统中断时间，全力保障业务系统安全，蓬勃生物针对业务系统在运行过程中或者操作过程中可能出现的紧急安全问题，定期进行模拟应急演练，演练科目包括：

- DDoS 攻击防护演练
- 黑客攻击入侵反制演练
- 数据丢失恢复演练
- 数据灾备切换、恢复、处理演练
- 数据中心防火、防涝演练
- 钓鱼事件演练
- 外来人员防泄密演练
- 员工办公主机防病毒演练
- 新型漏洞攻击防护演练
- 数据异常外发告警演练

在演练活动中，蓬勃生物员工通过公司监控、管理、防护平台，快速定位、并进行针对性的分析与处理，并及时将情况报告给信息安全部。

通过定期开展各项安全事件应急演练，使得蓬勃生物时刻能够保持对信息安全事件处理的及时性，同时能够不断加强内部组织、部门、员工相应的安全意识，形成牢固的安全规范，持续保障蓬勃生物客户的数据安全。

# 9. 外部审计

金斯瑞集团定期聘请第三方外部审计机构对集团开展审计，最近审计开展为 2023 年第四季度聘请 BSI 对集团的信息安全管理体系进行审计，聘请德勤对集团的信息安全风险管理进行审计，审计结果良好。

www.genscriptprobio.cn

Email:infosec@genscriptprobio.com

金斯瑞
蓬勃生物