

ProcessMind 灾难恢复、业务连续性与事件响应

生效日期：2026 年 9 月 14 日

本文件提供 ProcessMind B.V. 针对其云服务的灾难恢复 (“DR”)、业务连续性 (“BCP”) 和安全事件响应程序的高级摘要。本文件补充[安全措施](#)、[SaaS 托管政策](#)、[服务级别协议](#)和[数据处理附录](#)。

本文件说明我们当前采用的方法，不会在适用协议、DPA 或 SLA 明确规定的范围之外，另行设立合同恢复时间目标、恢复点目标、数据持久性保证、通知期限、服务级别或责任标准。

1. 目标和范围

ProcessMind 维护这些程序，以便：

- 在发生中断事件期间保护客户数据的机密性、完整性和可用性
- 在 ProcessMind 控制的系统发生故障后恢复关键生产服务组件
- 在服务中断期间继续进行事件管理、客户沟通和运营决策
- 使用成文程序和受源代码控制的基础设施定义，从基础设施、部署、应用程序或数据层故障中恢复
- 识别和评估安全事件、遏制威胁、根除根本原因、恢复受影响的系统、按要求进行沟通并总结经验教训

这些程序适用于生产环境中的 ProcessMind 云服务，以及涉及子处理器或云服务的安全事件，但仅限于这些事件影响服务且在 ProcessMind 合理调查和管理能力范围内的情形。开发和测试环境彼此隔离，不被视为面向客户的生产承诺所对应的恢复目标。

2. 弹性策略

****2.1 区域设计。****生产服务托管于 AWS EU（德国法兰克福，eu-central-1）。该架构依赖该区域内的 AWS 托管服务，而 AWS 在多个可用区之间运营这些服务。

Aurora 集群目前运行单个写入实例，因此数据库恢复依赖自动备份和时间点恢复，而非区域内备用实例。ProcessMind 目前不运营第二个活跃的客户数据区域。

****2.2 托管式和无服务器服务。** **ProcessMind 依赖 AWS Lambda、Amazon API Gateway、Amazon CloudFront、Amazon Aurora PostgreSQL、Amazon S3、Amazon SQS、Amazon SNS 和 Amazon CloudWatch。这减少了对客户管理的长期运行服务器的依赖，并支持从源代码重建应用程序和静态组件。

****2.3 环境分离。** **生产环境和开发环境在不同的 AWS 账户中运行，并使用不同的数据库和基础设施堆栈。这降低了开发活动影响生产恢复操作的风险。

****2.4 监控和检测。** **CloudWatch 警报、仪表板、死信队列警报、集中式日志记录和合成服务监控支持事件检测、分类和升级。潜在事件也可能通过支持请求受理、员工报告、供应商通知或其他调查触发因素被识别。

3. 恢复优先级

在重大事件期间，ProcessMind 的恢复优先级通常为：

1. 保护客户数据完整性并防止进一步损害。
2. 遏制事件并稳定受影响的系统。
3. 恢复核心生产访问路径和关键工作流。
4. 在宣布恢复完成前，验证服务行为、数据完整性和监控。
5. 沟通状态更新、客户影响和后续行动。

具体顺序可能因事件性质而异，包括事件是否影响数据完整性、客户访问、异步处理或支持性基础设施。

4. 灾难恢复程序

****4.1 事件声明和协调。** **重大服务中断和安全事件通过事件响应程序进行分类。

ProcessMind 指定事件负责人，将响应参与范围限制在获授权人员内，评估严重程度和范围，协调技术响应人员，并持续跟踪恢复行动，直至事件得到解决或降级。

****4.2 遏制。** **ProcessMind 在开始更广泛的恢复之前，采取商业上合理的努力来停止或减少持续影响。根据故障模式，遏制措施可能包括回滚近期变更、停用受影响的路径、隔离发生故障的组件、在执行完整性检查期间暂停后台处理、撤销或轮换凭证，或阻止滥用活动。

****4.3 根除。****在即时影响得到稳定后，ProcessMind 致力于移除根本原因或促成条件。这可能包括应用代码或配置修复、移除恶意构件、轮换机密、恢复可信配置或关闭暴露的访问路径。

****4.4 数据库恢复。****Aurora PostgreSQL 持续执行自动备份，保留期限为七（7）天，并支持时间点恢复。如果数据库级故障、损坏事件或意外破坏性变更需要恢复，ProcessMind 可以从最新的适用备份恢复，或恢复至选定的时间点，验证恢复后的环境，并将应用程序流量返回至恢复后的数据库路径。

****4.5 对象和构件恢复。****客户文件上传内容和运营构件存储在 Amazon S3 中。上传存储桶和资源存储桶已启用版本控制，以支持从意外删除或覆盖情形中恢复。网站和前端部署存储桶被视为可复现构件，可以从源代码重建，而非作为备份恢复。

****4.6 异步工作负载恢复。****异步处理路径使用死信队列保留失败事件以供调查。恢复可能包括重试失败消息、重新运行处理逻辑，或在底层工作流支持安全重新处理的情况下重放工作。

****4.7 应用程序和基础设施重建。****基础设施通过受源代码控制的基础设施即代码定义进行管理。如果需要重新创建应用程序基础设施或静态资产，ProcessMind 可以根据版本控制的定义和构建构件重建并重新部署受影响的组件。

****4.8 恢复服务前的验证。****在关闭事件之前，ProcessMind 使用可用的监控、日志、合成检查和有针对性的功能验证来验证服务运行状况，并使用经过验证的部署、恢复和基础设施程序恢复受影响的功能。当事件涉及数据恢复或数据完整性风险时，可能会进行额外审查。

5. 业务连续性措施

****5.1 运营连续性。****ProcessMind 维护成文的运营程序，以便在发生中断事件期间继续进行事件处理、客户支持请求受理、工程响应和决策。

****5.2 沟通。****对于重大生产事件，ProcessMind 将采取商业上合理的努力，通过客户支持渠道，并在适当情况下通过公共状态页面processmind.com/status提供更新。

****5.3 受控变更管理。****采用纵深防御式软件开发生命周期，其中包括多个相互独立的自动验证层、受控部署、集中式监控和事件后审查，以减少可避免的中断，并随着时

间推移改善连续性。

****5.4 恢复期间的安全。** **恢复行动须遵循适用于正常运营的相同一般安全原则，包括最小权限访问、在可用情况下记录运营活动，以及对生产系统和数据实施受控访问。

6. 备份和数据保护摘要

****6.1 数据库备份。** **Aurora 自动备份经过加密并保留七（7）天，在该保留期限内可进行时间点恢复。

6.2 S3 保护。 Amazon S3 为存储的对象提供高持久性。可变客户数据存储桶依赖主要区域内的持久性和版本控制。ProcessMind 目前未为这些存储桶启用跨区域 S3 复制。

6.3 日志和诊断。 集中式日志、警报和遥测支持故障调查和恢复验证。这些机制支持连续性运营，但其本身并不作为单独的备份产品提供。

7. 事件识别与分级

7.1 初步评估。 对报告的事件进行分级，以确定其是否符合 Security Incident 的定义、哪些系统或数据可能受到影响、可能的范围和严重程度，以及是否需要立即遏制。证据保存以适合事件性质及所涉系统的方式进行。

7.2 值班与升级。 ProcessMind 为生产环境事件提供值班覆盖，包括为 Critical 事件（定义见 Service Level Agreement）提供全天候（24x7）覆盖，以便随时确认并分级处理事件。

7.3 文档记录。 ProcessMind 记录重大调查结果、响应措施和恢复决策，以便在事件发生后审查事件时间线及由此产生的纠正措施。

8. 通信与通知

8.1 内部通信。 ProcessMind 协调响应人员、决策人员和支持渠道，以确保技术响应与客户沟通在整个事件生命周期内保持一致。

8.2 客户通知。 如发生根据 DPA 或适用法律需要通知的 Security Incident，ProcessMind 将在不无故延迟的情况下通知受影响的客户；在可行的情况下，于知悉事件后七十二（72）小时内通知。通知通常包括事件的性质和范围（如已知）受影响的数据类别、为遏制和补救事件所采取的措施，以及在相关情况下建议客户采取的行动。

8.3 持续更新。 如事件仍在进行中或重大事实发生变化，ProcessMind 将在获得更多经核实的信息后提供后续更新。对于范围更广的生产服务中断，ProcessMind 也可能使用客户支持渠道，并在适当情况下使用公开状态页面 processmind.com/status。

9. 测试、审查与维护

ProcessMind 至少每年审查这些程序，并在发生重大事件或架构发生重大变化后进行审查；定期演练响应和恢复方法的相关要素（例如备份恢复、部署重建、监控、警报和事件通信）；并将经验教训纳入其安全性、可靠性和连续性程序。

10. 限制与合同边界

本文件是高层次摘要，并未以运营细节描述每一份内部运行手册、升级路径、调查方法或证据处理步骤。本文件不使 ProcessMind 承诺采用单独的跨区域故障转移设计、为所有可变存储桶提供不可变存储保留，或提供适用协议或订单中明确规定以外的独立 RTO/RPO 保证。

如本文件与适用的 Customer Agreement、Data Processing Addendum、Service Level Agreement 或强制性法律之间存在任何冲突，以该等来源为准。