ZWLINK 展旺				文件编号：ZW-RBA-OP-074
				制定日期：2025-03-05
文件类型	程 序 文 件	制定部门	管理部	版　　次：　　A0
文件名称	业务连续性管理程序			页　　次：　第 1 页/共 6 页

文件履历表

版本	修订内容描述	修订日期	制定人	审核人	批准人
A0	首次发行	2025-03-05	李勤	张楠	刘仁

制定人/日期	审　核/日期	批　准/日期
李勤/2025-03-05		刘仁

文件发行章
展旺公司 2025.03.05 文件受控

1. 目的

确保本公司各项业务能够持续稳定的进行，最低限度的降低信息安全事件对业务的影响，特制定本程序。

2. 适用范围

本程序适用于本公司业务活动提供 IT 支持，包括业务活动中断时的信息系统安装和配置，还包括提供备份或容灾恢复的技术手段，以及关键业务过程所需要的 IT 基础设施、人员支持、数据等。

3. 定义

无

4. 职责

4.1 信息安全小组组长:

4.1.1 审批业务连续性计划，分配相关资源，确保业务持续性。

4.1.2 负责公司的灾难性恢复计划的制定和实施。

4.1.3 确保活动顺利进行;在发生重大信息安全事件或灾难时担任本单位业务中断的恢复的总指挥与总协调。

4.2 技术部：

4.2.1 负责组织进行业务影响分析，相关业务连续性计划编写、审核、组织演练、监督修改完善。

4.2.2 在发生重大信息安全事件或灾难时，负责协调进行信息和资产保护，及时恢复中断的业务。

4.3 各部门配技术部执行业务连续性计划的编写与演练，在发生重大信息安全事件或灾难时，负责保护本部门的信息和资产，及时恢复中断的业务。

5. 工作程序

5.1 业务影响分析

业务影响分析是通过对所支持的客户业务过程进行分析和评估，以得出关键业务过程，以及对业务过程中断或发生灾难所能接受的水平，包括损失程度、恢复时间、优先级别等，并最终映射到 IT 服务和 IT 基础设施上，从而得到对业务连续性管理的需求。并进行相应的风险评估，以及根据风险评估的结果建议相应的控制方式。

5.1.1 识别组织关键业务

在开发业务应急预案之前，应从以下方面对组织进行分析:

——识别组织的目标、利益相关方的义务、法定责任和组织运行的环境;

——识别活动、资产和资源，包括组织以外支持组织产品和服务交付的活动、资产和资源;

——活动、资产和资源的失效随时间推移的影响和后果;

——在分析的基础上确定组织的关键业务，以及关键业务得到恢复的时间要求(RTO)以及数据恢复要求(RPO)。

5.1.2 识别关键信息系统

那些信息系统的崩溃将在最短的时间内带来重大影响，并需要快速恢复的系统，可被视为“关键信息系统”。组织应识别为关键业务提供支持的关键信息系统和(或)支持服务。

5.1.3 风险评估

应对关键信息系统所面临的风险进行分析和评估，确定风险级别，特别是有关组织关键活动及导致关键活动中断的风险。

5.1.4 风险处置建议

作为业务影响分析和风险评估的结果，组织应该识别措施，以降低服务中断或崩溃的可能性、缩短中断期限、降低灾难对业务的影响。

5.2 连续性架构规划

组织应该对信息系统的连续性的架构进行规划和设计,在进行规划和设计时需要考虑的方面包括:

——人员;

——基础设施;

——技术设施;

——信息和数据;

——其他供给;

——利益相关方。

5.2.1 确定团队与人员

组织应确定识别管理参与服务连续性管理和恢复所需的核心技能和知识的合适方式,以及相关参与的人员。

能力和知识是指各种技术资源，包括技术人员、文档等，使得参与的团队和人员能够透彻地了解组织的业务情况和信息系统情况，深刻地把握单位灾难恢复系统的状态，并具有各种相关的技术能力，经历了多次灾难恢复演练，能在灾难发生时，迅速灾难备份中心在软件、硬件和网络等方面的技术支持要求，包括技术支持的组织架构、灾难备份中心在软件、硬件和网络等方面的技术支持要求，包括技术支持的组织架构、各类技术支持人员的数量和素质等要求。

5.2.2 确定利益相关方

组织应确定参与服务连续性管理和恢复的相关利益方、业务或服务合作伙伴及承包方的关系，以及联络方式和所分担的职责。

5.2.3 确定数据和信息的获取方式

组织应确定数据备份到安全地点的方式，以及在灾难发生时所需的数据获得方式和地点。这将影响前期的数据备份方式和存储方式。

为了能达到信息系统灾难恢复的需求，还需要根据用户具体信息系统情况、备份的数据量、备份网络情况、数据的变化量等因素，制定备份策略和日程安排，以确保能在灾难恢复时间指标内实现恢复;另外，若备份系统是依靠电子传输的数据备份系统，还包括数据备份线路和相应的通信设备。

5.2.4 确定 IT 技术设施

备用技术设施是指当灾难发生时，确保业务持续运行所需的技术设施(包括网络、应用系统等)。对于恢复所需的软、硬件设备以及与外部的通讯方式和线路等，应提前确定获取的方式和存放的位置，以及事前应该保证的状态等。

5.2.5 确定其他供给需求

确定恢复时所需的其他供给需求，如办公设备和支持性设备等。

5.2.6 形成设计方案

将上述关键活动的策略选项以及每一活动恢复所需的资源以及资源需求的获取方式，形成设计方案，设计方案由业务系统相关使用部门组织人员编写，技术部提供必要的信息设施支持，由信息安全管理者代表进行评审和发布。

5.3 制定演练方案

技术部依据信息系统应急预案，结合自身情况，负责公司的灾难性恢复计划的制定和实施，每年 12 月制定演练计划和演练方案，演练方案包括：

5.3.1 确定团队职责与分工

描述灾难恢复的组织结构，各个岗位的职责和人员名单，灾难恢复组织包括应急响应组，灾难恢复组等。并列出灾难恢复相关人员和组织的联络表，包括灾难恢复团队，运营商、厂商、经理部门、媒体、员工、家属等，联络方式包括固定电话、移动电话、对讲机、电子邮件和住址等。

5.3.2 确定突发事件通告机制

任何人员在发现信息系统相关突发灾难发生或即将发生时，应按预定的过程报告相关人员，并由相关人员进行初步判断，通知和处理。

5.3.3 确定人员疏散方式

提供指定的集合地点和替代的集合地点，还包括通知人员撤离的办法，撤离的组织和步骤等。

5.3.4 确定损害评估机制

在突发事件发生后，应由应急响应组的损害评估人员，确定事态的严重程度，由灾难恢复责任人召集相应的专业人员对突发事件进行慎重评估，确认突发事件对信息系统造成的影响，确定下一步将要采取的行动，一旦系统的影响被确定，应将最新信息按照预定的通告过程通知给相应的团队。

5.3.5 确定灾难启动机制

应预先明确灾难恢复预案启动的条件，当损害评估的结果达到一项或多项启动条件时，组织将正式发出灾难启动，宣布启动灾难恢复预案，并根据宣告过程通知各有关部门。

5.3.6 确定系统恢复过程

5.3.6.1 恢复

按照业务影响分析中确定的优先顺序，在灾难备份中心恢复支持关键业务功能的数据，同时还包括特定情况发生时各团队之间进行协调的指令，以及异常处理过程。同时还包括特定情况发生时各团队之间进行协调的指令，以及异常处理过程。

5.3.6.2 重启运行

灾难备份中心的系统替代主系统，支持关键业务功能的提供，这一阶段包括主系统运行管理所涉及的主要工作，包含重续运行的所有操作过程和规章制度。

5.3.6.3 灾后重建和回退

最后阶段是主要信息安全区域的重建工作，中止灾难备份系统的运行，回退到组织的主系统。

5.3.7 形成文档

将上述计划中的内容形成服务应急预案，并提交信息安全小组组长及相关各方人员进行评审。

6.4 演练与维护

6.4.1 设计演练方案

演练应该是实际的、经过周密的计划，并获得利益相关方的认可，以使演练过程中业务中断的风险最小。演练应经过计划，以使得因演练直接导致事故的风险最小。每次演练都应清晰定义目的和目标。演练的方式可能包括:桌面演练、模拟演练和真实演练。

6.4.2 演练

除非经过演练并实施维持，否则组织的业务连续性和事故管理安排不能认为是可靠的。演练核心是开发团队合作、能力、信心和知识，这在发生事故时是非常重要的。演练的计划应在项目计划时进行确定。

6.4.3 评审和改进

演练后的简报和分析应考虑目的和目标的达成。在演练结束以后以及在系统本身或外界环境发生重大变化时，应对服务连续性方案进行评审和维护，并保留必要的评审和改进记录。

6.5 冗余

根据公司业务运行及风险评估的结果，创建冗余信息处理设施，具体的要求按照《系统运行维护管理程序》的要求执行，并进行必要的冗余信息处理设施的故障切换测试，确保信息处理设施发生意外时，将业务中断对本公司的影响降低到最低程度。

6. 相关文件

6.1《信息系统应急预案》

6.2《系统运行维护管理程序》

7. 相关记录

7.1《业务连续性计划》

7.2《业务影响分析报告》

7.3《业务连续性计划实施方案测试报告》