信息安全事件管理制度

固德威技术股份有限公司（以下简称“固德威”或“公司”）将信息安全与业务连续性视为经营底线，制度明确信息安全委员会及工作小组、管理部门（IT）与各业务部门、现场处置人员的职责分工，规范分级响应、证据留存、对外联络与客户沟通、以及处置结论与预防措施落实的要求，确保全过程可追溯、可审计、能改进。

一、 目的

为加强和改进信息安全事件管理；在发生信息安全事件时能及时报告，快速响应，将损失控制在最小范围；在发生信息安全事件后，能够分析事故原因及产生影响、反馈处理结果、吸取事故教训；在发现信息安全异常现象时，及时沟通，采取有效措施，防止信息安全事故的发生；特制订本管理制度。

二、 范围

本制度适用于固德威影响信息安全的所有事故以及安全异常现象以及全体人员（包括外协人员、实习生、长期客户员工、来访客户等）。

三、 定义

1. ISO/IEC 27001：2022 信息安全、网络安全和隐私保护-信息安全管理体系-要求
2. ISO/IEC 27002-：2022 信息技术-安全技术-信息安全控制实用规则
3. GB/T 22080-2008/ISO/IEC 27001:2013 信息技术-安全技术-信息安全管理体系要求
4. GB/T 22081-2016/ISO/IEC 27002:2013 信息技术-安全技术-信息安全管理实施细则

四、 职责

1. **信息安全委员会主任委员（信息安全管理领导小组）**

负责对内部信息安全事件的处理和奖惩意见进行审批；负责对纠正预防措施进行审批

2. **信息安全委员会执行委员（信息安全工作小组）**

制定事件处理制度与流程；受理上报并组织调查取证；提出处理措施、奖惩意见以及纠正预防措施，统筹事件相关文件的归档与管控。

3. **信息安全工作人员**

负责对信息安全事件的实际处理，负责执行信息安全委员会执行委员提出的处理措施。

4. 各部门

积极预防信息安全事件的发生；及时准确的汇报信息安全事件，配合信息安全事件的调查取证工作；配合执行处理措施，奖惩决定以及纠正预防措施。

5. 异常现象和事件发现人

异常现象和事件发现人有义务及时准确地报告异常现象和事件的真实情况，并采取适当的临时措施制止事故的进一步扩大。

五、 工作内容

1. 信息安全异常现象

(1) 信息安全异常现象定义

信息安全异常现象是指被识别的一种系统、服务或网络状态的发生，表明一次可能的信息安全策略违规或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况。

(2) 信息安全异常现象处理流程

- 异常现象发现者应及时上报信息安全工作小组该部门信息安全委员会执行委员，由信息安全委员会指派相应人员信息安全工作人员进行处理。
- 信息安全工作人员相应人员判断异常现象是否为信息安全事件，如果是的话，进入信息安全事件处理流程；如果不是，由信息安全工作人员相应人员对异常现象进行处理。

2. 信息安全事件处理

(1) 信息安全事件定义

信息安全事件：是指办公设备/计算机/网络设备系统/信息管理系统的硬件、软件、数据因故障/非法攻击/病毒入侵/恶意破坏/非授权外传/遗失/灾难等安全原因而遭到破坏、更改、泄露而造成业务活动不能正常进行或者涉密信息泄露或者在其他方面造成损失的事件。

(2) 信息安全事件分类

- 有害程序事件（MI）：因蓄意制造、传播有害程序，或受其影响引发的事件。有害程序会危害系统数据、程序或系统运行。包含计算机病毒、蠕虫、特洛伊木马、僵尸网络、混合攻击程序、网页内嵌恶意代码及其他有害程序事件 7 类。
- 网络攻击事件（NAI）：通过网络等技术手段，利用系统缺陷或暴力攻击，使系统异常或存在潜在危害的事件。涵盖拒绝服务攻击、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼、干扰及其他网络攻击事件 7 类。
- 信息破坏事件（IDI）：通过网络等技术手段，导致系统中信息被篡改、假冒、泄

漏、窃取等的事件。包含信息篡改、信息假冒、信息泄漏、信息窃取、信息丢失及其他信息破坏事件 6 类。

- 信息内容安全事件（ICSI）：利用信息网络发布、传播危害国家安全、社会稳定和公共利益内容的事件。包括违反法规、形成敏感舆论热点、组织串连煽动集会游行及其他信息内容安全事件 4 类。
- 设备设施故障（FF）：因信息系统自身、外围保障设施故障，或人为非技术手段破坏引发的事件。包含软硬件自身故障、外围保障设施故障、人为破坏事故及其他设备设施故障 4 类。
- 灾害性事件（DI）：因不可抗力（如水灾、地震、恐怖袭击等）对信息系统造成物理破坏的事件。
- 其他事件（OI）：无法归为上述 6 类的信息安全事件。

3. 信息安全事件处理流程

(1) 安全事件的发现

相关部门应建立监控措施和日志查看制度，采用必要的技术手段，确保及时发现安全事件；相关部门根据风险评估、安全事件和安全告警的内容，及时发现潜在安全事件；应向所有员工和第三方服务商提供培训，使之认识到发现并报告安全事件是其应尽的义务。

(2) 安全事件的处理

- 一般安全事件处理流程

相关人员发现异常并判断为安全事件后，需通过邮件或电话向信息安全工作人员上报时间、地点、系统名称等核心信息并确认接收。信息安全工作人员判断级别，无法判断或为严重事件则上报信息安全组长（信息安全委员会执行委员）并转严重事件流程；一般 / 较大事件协助信息安全副组长(信息安全委员会执行委员)处理，一般事件 1 小时内查因、42 小时内解决，较大事件 2 小时内查因、8 小时内解决，超时未解决立即上报信息安全组长启动对应响应流程。

- 严重安全事件处理流程

信息安全工作人员上报部门总监及信息安全组长（信息安全委员会执行委员），部门总监跟踪进度；信息安全组长分析处理并上报信息安全管理领导小组（信息安全委员会主任委员），领导小组指示信息安全工作小组（信息安全委员会主任执行委员）协调处理，必要时联系厂商协助，工作小组统筹服务商与部门人员配合。处理成功则恢复系统并总结，失败则转入事故流程。

- 信息安全事故处理流程

事故发生后，相关人员立即报董事会，信息安全组长（信息安全委员会主任委员）填《信息安全异常报告表》上报信息安全管理领导小组(信息安全委员会主任委员 / 董事长 / 上级组织）求助，同时信息安全组长（信息安全委员会主任执行委员）组织专

业人员处置。信息安全主任委员或上级组织协调工作小组、相关部门及服务商指导技术人员处理，系统恢复后由信息安全组长（信息安全委员会主任执行委员）撰写总结报告。

4. 信息安全事故事件的紧急处置和业务回复

部门负责人、管理部门（IT 部）、信息安全工作小组信息安全委员会主任执行委员组长在接到信息安全事故事件的报告后，应该立刻相互协调进行处置。

(1) 原因分析：责任部门会同管理部门立即定位原因。

(2) 应急控制：同步采取隔离、封堵、限权等措施，防止事态扩大。

(3) 业务恢复：尽快恢复核心业务；必要时按《业务连续性管理制度》启动预案。

(4) 影响评估与补救：联合评估影响范围与损失，调整业务并实施补救。

(5) 外部沟通

- 由部门负责人向客户通报并协调后续业务；
- 涉嫌违法的，由主任委员或其指定人员按规定向主管机关报告；
- 涉及外协/服务商的，及时通知其单位配合处置。

(6) 重大/直接影响客户的事件：责任部门负责人、管代与管理部门立即成立应急小组，拟定对策报总经理批准后执行，并及时向客户反馈处置过程与结果。

5. 信息安全事件证据的收集

为了清楚地分析原因，过程和影响范围，确定级别和责任人，以利于改进，包括为可能涉及到的诉讼（民事的或刑事的）行为提供证据支持，在信息安全事件发生时，信息安全工作小组信息安全委员会执行委员要进行证据的收集工作。

进行证据收集时要注意：

(1) 及时性

第一时间启动取证，在证据收集超越公司管辖权边界的情况下，及时联络相关机构或委托合规第三方取证。

(2) 证据的份量：即证据的质量和完备性。

- 纸质证据：保全原件并记录“四要素”（发现人、地点、时间、见证人）；调查不得改动原件。
- 电子证据：对介质/硬盘/内存制作镜像或拷贝，全过程留存操作日志；原始介质与日志（或至少一份镜像/拷贝）安全保管、不得改写。
- 取证原则：法律取证仅在拷贝上完成；拷贝须在可信人员监督下进行，完整记录时间、地点、执行人、工具与流程，确保可追溯。

(3) 证据的可容许性：即证据是否可在法庭上使用

确保信息系统与取证过程符合适用标准或规则以获得被容许的证据。

6. 信息安全事件和信息安全异常现象的报告和反馈

(1) 信息安全事件

- 报告

事故责任部门填写《信息安全事件报告表》，内容包括：原因、处置过程与结果、再发防止措施与改进计划、证据附件；提交信息安全工作小组（执行委员）。

- 反馈与升级

执行委员将处置过程与结果反馈给部门负责人及发现人；重大/达“事故”等级事件同步报总经理并抄送相关负责人；必要时由部门负责人向客户反馈。

(2) 信息安全异常现象

- 处理

执行委员接报后组织核查，确认异常后明确处置责任部门并督办处理。

- 报告

处置责任部门在《信息安全事件报告表》中填报异常处理，含原因与预防/改进计划，提交执行委员。

- 反馈与升级

执行委员将处置结果反馈给发现人及涉及部门/项目组；重大异常报总经理。

7. 改进和预防工作

(1) 信息安全事件或异常现象所涉及的部门应在信息安全工作小组信息安全委员会执行委员的协调指导下根据事件或异常现象报告中的再发防止措施考虑进行安全体系的改进工作。

(2) 信息安全工作小组信息安全委员会执行委员应监控并确认相关改进活动的执行，并向信息安全主任委员报告。

(3) 在需要启动内审和管理评审的情况下，根据规定启动相应的审核活动。

(4) 信息安全事件管理活动记录由信息安全工作小组信息安全委员会执行委员保存，作为内审和管理评审的输入。

8. 实施策略

(1) 发现一级信息安全事故时，责任部门经理会同发现人填写《信息安全事件报告表》，报信息安全工作小组（执行委员）。

(2) 执行委员研判并调查取证，按分级采取控制措施，完善《信息安全事件报告表》处置内容。

(3) 处置后由执行委员在报告中总结教训、提出预防措施，相关部门落实，防止复发。

固德威技术股份有限公司

2025 年 9 月

版本：2025V1