**信息安全事件管理制度**

文件类型：管理规范

文件编号：MR-T-IT-16

版本号：A/0

密级：商业秘密

生效日期：2024/01/05

|  |
| --- |
| 适用组织：☑凌创电子系统有限公司 |
| - | 审核部门 | 签核 | - | 审核部门 | 签核 |
| √ | 质量部 |  |  |  |  |
| √ | 销售部 |  |  |  |  |
| √ | 工程部 |  |  |  |  |
| √ | 安全部 |  |  |  |  |
| √ | 制造部 |  |  |  |  |
| √ | 人事部 |  |  |  |  |
| √ | 行政部 |  |  |  |  |
| √ | 采购部 |  |  |  |  |
| √ | 财务部 |  |  |  |  |
| √ | IT部 |  |  |  |  |
|  |  |  |  |  |  |
| 文件批准 |  |

**文档修订履历**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 变更章节 | 变更事项 | 编制部门 | 变更人 | 修订日期 |
|  | 新版发行 | IT部 | 李忠富 | 2024/01/04 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

**1目的** 4

**2范围** 4

**3定义** 4

**4职责** 4

**5程序** 4

**6引用文件** 8

**7记录** 8

**1目的**

为对公司信息安全的事件/漏洞管理活动实施控制，特制定本制度。

**2范围**

适用于对信息安全的事件/漏洞管理。

**3定义**

3.1信息安全事件：信息安全事件可以被定义为对计算机系统、网络、软件或数据等信息资源进 行的未经授权的访问、使用、披露、修改、破坏或中断的行为。这些事件可能导致信息的泄 露、损坏、丢失或服务的中断，对个人、组织和社会造成负面影响。

3.2信息安全漏洞/脆弱性（vulnerability）：信息安全脆弱性是指在计算机系统、网络、软件或硬件中存在的潜在弱点或缺陷，可能被恶意攻击者利用来获取未经授权的访问、披露、修改、破坏或中断信息资源的机会。常见如：软件漏洞、弱密码、操作系统漏洞、非安全的数据存储等。本制度下文以“漏洞”表示“漏洞或脆弱性（vulnerability）”。

**4职责**

4.1IT部

负责信息安全的事件的收集、响应、处置和调查处理。

4.2其他部门

负责信息安全事件的及时报告，及时落实相关的处理措施。

**5程序**

**5.1信息安全事件的报告与评估**

5.1.1员工发现信息安全事件/漏洞以后，应通过即时通信工具/电话/邮件/口头等方式向信息安全联系人报告。报告的内容，应符合《信息安全事件报告单》中的要求。信息安全事件的类型划分为，与人员有关/与物理环境有关/与网络有关/与供应商有关等

5.1.2事件的报告，应扩大报告的渠道，包括但是不限于本部门领导/IT部门相关人员/ 信息安全负责人/信息安全专员等。在员工无法或者不清楚联系何人的情况下，应通过培训等宣导方式，告知员工在任何情况下的唯一联系人。

5.1.3潜在威胁的感知：公司应建立并维护潜在威胁的上报渠道，如聊天群，公共邮箱等，确保员工发现的任何可疑事件，及时反馈给信息安全团队。

5.1.4外部信息安全事件报告渠道：建立并维护外部信息安全事件报告渠道，包括但是不限于官网、邮件、微信好友等方式，确保任何来自于外部的信息安全事件得到及时的报告和处理。来自于供应商的事件沟通主要由采购部负责，来自与客户的事件沟通主要由销售部负责，其他来自外部的事件沟通，由IT部负责。

5.1.5事件报告机制及如何报告事件的信息能够被所有报告者访问，如将信息安全事件报告的路径公示。建立并维护充分的报告反馈机制，确保报告人及时了解事件处置进度，事件处理结果等。

**5.2信息安全报告注意事项：**

5.2.1根据公司的现状，对信息安全事件/漏洞的反应由IT部门负责，IT部门应及时对收到的报告进行分析和处置。

5.2.2公司正式的报告渠道为：云之家IT需求申请流程、邮件、电话、当面告知、~~某某报告单~~等

5.2.3处理主体：一般信息安全事件为IT部门，重大信息安全事件为信息安全委员会，事件处理人员缺勤的情况下，部门内部应指定备用处理人员

5.2.4公司正式的反馈程序为：云之家IT需求申请流程、邮件、电话、当面告知、~~某某报告单~~等

5.2.5纪律处分：如处置后发现某事件或漏洞为主观人为，则启动公司相关纪律制度进行处理

5.2.6重大/紧急信息安全事件特殊渠道：对已经确认为重大信息安全事件的信息安全事件，应立即启动相关处置流程，相关人员立即成立事件处理小组，组建事件沟通群，并不需要依照事件处理流程按部就班处理，以解决事件为第一要务。

**5.3事件追溯**

5.3.1 一般信息安全事件未造成重大损失的，不进行事件调查和追溯

5.3.2 重大信息安全事件启动事件调查和追溯机制。当发生重大信息安全事件以后，由IT部门负责调取事件发生前后的系统操作日志，确定造成事件发生的账号和操作过程，由IT部门/行政部门调取设备有关的监控录像，确认事件发生之时的具体操作人，由人事部门调取事件发生之时的值班表，确认当时值班操作人员和主管。各部门证据收集以后，以此填写《重大信息安全事件调查追溯表》，该表格以及所有事件相关电子和纸质证据，交IT部门备份存储，以备将来事件回溯之用。

**5.4信息安全事件/漏洞的评估办法**

5.4.1，信息安全事件的评估

|  |  |
| --- | --- |
| 级别 | 说明 |
| 重大信息安全事件 | 1. 造成业务系统运行中断，严重影响业务活动进行的;
2. 数据被破坏，无法恢复或者恢复时间过长，超过90分钟，严重影响业务活动进行的;
3. 绝密、机密信息泄露，给公司造成较大损害的,或产生重大影响的;
4. 其它涉密信息泄露，给公司造成极大损害的，产生特别重大的社会影响的;
5. 将恶意代码或其他有害程序传播至公司，产生特别重大的社会影响的;
6. 客户真实数据泄漏或者对客户数据造成破坏的，产生特别重大的社会影响的;
7. 内部人员（包括员工/外协人员/实习生/客户/服务人员等）任何故意破坏信息系统/泄漏涉密信息的行为,产生特别重大的社会影响的;
8. 网络设备受到攻击，影响网络畅通的安全事件，攻击流量超过正常流量的50％，或者持续时间大于90分钟的安全事件;
9. 相同业务一周重复出现的安全事件。
10. 利用相关信息平台，传播违法等不良信息，产生特别重大的社会影响的;
11. 重大软件/操作系统/硬件漏洞引起重大经济损失的事件
 |
| 一般安全事件 | 1. 对业务活动进行没有造成太大影响，只影响到单台应用服务器，且为业务分布式服务器的安全事件，30分钟内已查明原因，可以在60分钟内解决的安全事件。
2. 数据被破坏，可以较快恢复，对业务活动进行没有造成太大影响的;
3. 涉密信息泄露，没有给公司造成明显损害的;
4. 不遵守规章或者操作流程，没有给公司造成明显损害的;
5. 任何外来的非法攻击/病毒入侵，尚没有对业务活动进行造成明显影响的;
6. 已发布相关安全公告的安全事件。
7. 不安全的软件/操作系统/硬件因为缺乏补丁或配置不正确引起的轻微事件（漏洞）
 |
| 评估标准 | 1. 严重影响：生产/研发/等关键流程中断超过30分钟，不进行索赔以及法律追溯
2. 重大影响：直接经济损失5万元以上或者间接经济损失10万元以上，内部针对特定人员启动索赔，视情况启动法律追责
3. 特别重大影响：直接经济损失10万元以上，或者导致公共媒体负面报道的，内部针对特定人员启动索赔，并启动针对特定人员的纪律处分，存在主观恶意的情况下，必须上报公安部门调查，并持续进行法律追责
4. 重大经济损失：直接经济损失10万元以上，内部针对特定人员启动索赔，并启动针对特定人员的纪律处分，存在主观恶意的情况下，必须上报公安部门调查，并持续进行法律追责
5. 没有造成太大影响：直接经济损失1000元以内或者解决时间小于等于30分钟的一般信息安全事件，针对特定人员进行批评教育，存在主观恶意的，启动公司内部纪律处分
6. 轻微：当场解决且未造成任何经济损失的事件，不进行责任追究。
 |

5.4.1漏洞的评估办法：参考《漏洞和补丁管理制度》

**5.5信息安全事件\漏洞的反应**

5.5.1无论任何类型的信息安全事件、漏洞，相关责任部门都应该采取充分的反应，在条件允许的情况下，应立即采取行动。

5.5.2反应策略：

5.5.2.1事件升级

一般信息安全事件未得到有效解决，或发生了影响扩大造成了损失的，信息安全联系人或处置人应向信息安全委员会汇报，由信息安全委员会决定是否将事件升级处理

5.5.2.2事件补救措施

事件发生以后，根据事件发生的原因采取相应的补救措施。如更新设备，采购安全软件，更新补丁，加强员工教育等

5.5.2.3与内外部相关方沟通

根据事件的等级，影响和发生原因，由信息安全委员会决策与内外部相关方沟通的方式和策略，内部相关方如集团高层，外部相关方如设备厂家，IT专家，以及向执法机构报警，启动刑事立案等

5.5.2.4内部追责与处分。事件造成的损失，由行政部跟踪并解决关于损失追讨的问题，同时启动责任追究程序。与供应商有关的信息安全事件，造成经济损失或者保密信息泄露的，由采购部、行政部、公司相关领导，联合成立调查组，并出具调查结论，根据调查结论处置相关责任人

**5.6向外部相关方报告和公告**

5.6.1向相关方报告：信息安全事件发生以后，公司根据信息安全事件的等级和影响，及时与外部相关方取得联系，联系方式和联系策略，见《外部相关报告联系人清单》

5.6.2、对外公告：信息安全事件处置完成以后，对外公告由公司行政部负责执行，公告的方式包括但是不限于公司官网，邮件，新闻媒体，视频账号等，公告的内容。公告之前，应对公告内容进行讨论和批准，批准以后由专人发布。

**5.7关于信息安全事件的培训、演练和持续改进**

5.7.1公司对所有新员工进行信息安全事件有关的培训，确保新员工了解信息安全事件的定义以及上报流程、上报唯一接口人等

5.7.2发生重大信息安全事件并处置完成以后，对公司所有员工开展针对该事件的专项培训，确保此类事件不再发生

5.7.3公司定期开展关于信息安全事件的报告、处置演练，确保公司信息安全事件报告和处置流程的有效性，对演练结果形成《信息安全事件演习报告》，演练应包括一般信息安全事件、重大信息安全事件、极少发生的信息安全事件，针对演练过程中出现的问题进行分析和总结，持续改进

**5.8供应商信息安全事件处理程序**

5.8.1供应商反馈的信息安全事件，应通过事件管理平台或者系统及时向供应商反馈，并确保供应商能够实时查看事件进度

5.8.2公司内部发生的与供应商有关的信息安全事件，公司根据对公司造成的影响（参考信息安全事件/漏洞评估准则），决策是否向供应商通报或者采取进一步的行动。

**6引用文件**

《信息安全方针》

《人力资源控制程序》（违规处理部分）

《漏洞和补丁管理制度》

《应急准备与响应管理控制程序/业务连续性管理制度》

**7记录**

《信息安全事件演习报告》

《外部相关报告联系人清单》

《重大信息安全事件调查追溯表》