### **突发事件分类与响应层级表**

| 分类维度 | 类别名称 | 级别 | 描述/界定标准 | 典型示例 | 首要响应团队 | 目标响应时限 |
| --- | --- | --- | --- | --- | --- | --- |
| **按影响范围** | 特别重大突发事件 | I级 | 影响整个公司核心业务系统长时间中断（如超过4小时）；影响全部或绝大部分用户；对公司声誉或财务造成重大损失。 | 数据中心核心交换机宕机、大规模勒索病毒感染、主干网络中断。 | 应急领导小组、全体技术支持团队 | 立即响应，≤15分钟 |
|  | 重大突发事件 | II级 | 影响公司某个重要业务部门或关键应用系统中断；影响大量用户（如单个部门无法工作）。 | 财务系统崩溃、OA系统无法访问、大楼局域网中断。 | 运维部经理、技术部专家团队 | ≤30分钟 |
|  | 较大突发事件 | III级 | 影响局部范围，如单个团队或部分用户；核心业务系统性能严重下降但未完全中断。 | 部门打印机集体故障、某个非关键应用服务器宕机。 | 运维项目经理、服务工程师 | ≤1小时 |
|  | 一般突发事件 | IV级 | 影响单个或极少数用户，不影响其核心工作；或为常见的服务请求。 | 个人电脑蓝屏、软件安装请求、密码重置。 | 服务台（一线支持） | ≤4小时（或按SLA） |
| **按事件性质** | 网络安全事件 | - | 涉及系统漏洞、黑客攻击、数据泄露、恶意软件、网络入侵等。 | DDoS攻击、网站被篡改、敏感数据外泄。 | 应急管理办公室、运维部安全岗 | 立即响应 |
|  | 硬件故障事件 | - | 服务器、网络设备、存储设备等关键硬件设施故障。 | 硬盘损坏、内存故障、电源模块失效。 | 运维部硬件团队 | 根据备件情况 |
|  | 软件故障事件 | - | 操作系统、数据库、中间件或业务应用软件发生的错误、崩溃或性能问题。 | 数据库连接池满、应用服务无响应、软件报兼容性错误。 | 研发部、运维部 | ≤2小时 |
|  | 服务中断事件 | - | 任何导致IT服务不可用或性能严重下降的事件，可能由上述任何性质的原因引起。 | 邮箱服务无法收发、视频会议系统卡顿。 | 运维部 | 根据影响级别 |
| **按预警来源** | 监控自动告警 | - | 由Zabbix、Prometheus等监控系统自动触发的阈值告警。 | CPU使用率持续95%以上、磁盘空间不足。 | 运维部监控岗 | 实时 |
|  | 用户上报 | - | 通过服务台电话、邮件、工单系统等渠道由用户主动报告的事件。 | 用户拨打服务台电话申报故障。 | 服务台 | 按影响级别 |
|  | 外部通报 | - | 来自上级单位、监管机构或合作伙伴的漏洞预警、安全威胁通报。 | 上级单位下发网络安全风险预警。 | 应急管理办公室 | 立即响应 |