网络安全应急响应流程

㈠病毒爆发处理流程

单位各部门对外服务信息系统一旦发现感染病毒，应执行以下应急处理流程：

①立即切断感染病毒计算机与网络的联接；

②对该计算机的重要数据进行数据备份；

③启用防病毒软件对该计算机进行杀毒处理，同时通过防病毒软件对其他计算机进行病毒扫描和清除工作；

④如果满足下列情况之一的，应立即向本部门信息安全负责人通报情况：

⑴现行防病毒软件无法清除该病毒的；

⑵网站在 2 小时内无法处理完毕的；

⑶业务系统或办公系统在 4 小时内无法处理完毕的。

⑤在计算中心技术部的协助下，清除该病毒；

⑥恢复系统和相关数据，检查数据的完整性；

⑦病毒爆发事件处理完毕，将计算机重新接入网络；

⑧总结事件处理情况，并提出防范病毒再度爆发的解决方案；

⑨实施必要的安全加固。

㈡网页非法篡改处理流程

各部门和单位对外服务网站一旦发现网页被非法篡改，应执行以下应急处理流程：

①发现网站网页出现非法信息时，值班人员应立即向本部门信息安全负责人通报情况，并立即向计算中心网络安全技术部门报告。情况紧急的，应先采取断网等处理措施，再按程序报告；

②本部门信息安全负责人应在接到通知后立即赶到现场，做好必要记录，妥善保存有关记录及日志或审计记录；

③总结事件处理情况，向计算中心网络安全技术部备案，

并提出防范再度发生的解决方案；

④实施必要的安全加固。

㈢非法入侵处理流程

各部门对外服务信息系统一旦发现被远程控制等非法入侵行为，应执行以下应急处理流程：

①发现系统服务器被远程控制、植入后门程序，或发现有黑客正在进行攻击时，应立即向本部门信息安全负责人通报情况，并立即向计算中心网络安全技术部门报告；

②如服务器已被入侵，将被攻击的服务器等设备从网络中隔离出来，保护现场；

③本部门信息安全负责人应在接到通知后立即赶到现场，做好必要记录，妥善保存有关记录及日志或审计记录；

④由计算中心网络安全技术部对受攻击的网站、业务系统和办公系统进行现场分析，追查攻击源，修改防火墙等设备的安全配置阻断黑客继续入侵。相关部门做好配合工作；

⑤分析后台数据库操作日检查、校验数据的完整性和有效性；

⑥计算中心网络安全部门提取相关数据样本后，恢复与重建被攻击或破坏的系统。重新将恢复后的对外服务系统接入网络；

⑦总结事件处理情况，向计算中心网络安全技术部门备案，并提出防范再度发生的解决方案；

⑧实施必要的安全加固。

㈣拒绝服务攻击处理流程

单位各部门对外服务信息系统一旦发现遭受 DDoS 等拒绝服务攻击，无法正常访问时应执行以下应急处理流程：

①发现对外服务系统访问流量异常、无法正常访问，可能遭受拒绝服务攻击时，应立即向本部门信息安全负责人通报情况，并立即向计算中心网络安全技术部门报告；

②本部门信息安全负责人应在接到通知后立即赶到现场，做好必要记录，妥善保存有关记录及日志或审计记录；

③在计算中心网络安全技术部门提取相关数据样本后，对现场进行分析，追查攻击源，修改路由器、防火墙等设备的安全配置，缓解、消除拒绝服务攻击的影响。恢复对外系统正常运行。

④总结事件处理情况，向计算中心网络安全技术部门备案，并提出防范再度发生的解决方案；

⑤实施必要的安全加固。

备注：

本部门信息安全负责人可为本部门负责人，如：主任、处长、科长等。计算中心网络安全技术部电话：88236835

紧急网络安全事件举报电话：

马兰馨	13671128722
彦田	15801095733
安德海	13910695575
oncall 值班电话	17090170703