11--中国人民银行关于印发《银行计算机安全事件报告管理制度》的通知  
（银发〔2002〕280号）

人民银行各分行、营业管理部、省会（首府）城市中心支行，政策性银行，国有独资商业银行，股份制商业银行：

现将《银行计算机安全事件报告制度》印发给你们，请遵照执行。

本通知由人民银行各分支行转发辖区内城市商业银行、外资商业银行和城乡信用合作社，请遵照执行。

附：

银行计算机安全事件报告制度

第一条　为加强银行计算机安全管理，防范信息系统的技术风险，保障银行信息系统安全运行，根据《中华人民共和国计算机信息系统安全保护条例》，制定本制度。

第二条　本制度适用于人民银行、政策性银行、中资商业银行、在中华人民共和国境内的外资商业银行、城乡信用社。

第三条　银行计算机安全事件的报告必须做到快速及时、客观真实，并实行归口管理、分别报告的原则。

第四条　人民银行总行计算机安全主管部门，负责全国银行系统计算机安全事件的接报、汇总、通报和处置工作。

第五条　人民银行当地分支机构计算机安全主管部门，负责辖区内银行系统计算机安全事件的报告、接报和处理工作。

第六条　政策性银行、中资商业银行、外资商业银行、城乡信用社的计算机安全主管部门，负责本系统内计算机安全事件的报告、接报和处理工作。

第七条　发生计算机犯罪案件的银行应当按照有关规定向人民银行当地监管行保卫部门报告，并同时抄报计算机安全主管部门。

第八条　银行计算机安全事件具体包括：

（一）信息系统软硬件故障；

（二）网络通信系统故障；

（三）供电系统故障；

（四）系统感染计算机病毒；

（五）数据处理中心遭水灾、火灾、雷击；

（六）银行网络遭遇入侵或攻击；

（七）信息系统敏感数据泄露；

（八）信息系统数据失窃；

（九）银行数据处理设备失窃。

第九条　符合以下条件之一的计算机安全事件必须报告：

（一）计算机信息系统中断或运行不正常超过4小时；

（二）造成直接经济损失超过100万元；

（三）严重威胁银行资金安全；

（四）因计算机安全事件造成银行不能正常运营，且影响范围超过一个县级行政区域。

第十条　计算机安全事件报告包括以下内容：

（一）计算机安全事件发生的时间、地点、单位、单位负责人和联系方式；

（二）计算机安全事件的类别、涉及软硬件系统的情况和事件发生的过程；

（三）计算机安全事件造成的后果和影响范围；

（四）计算机安全事件发生的原因；

（五）责任人或涉案人员；

（六）计算机安全事件发生后采取的应急措施。

第十一条　银行发生计算机安全事件后，按照逐级上报程序，由事件发生单位在事件发生12小时内向本系统上级单位报告，并同时向人民银行当地分支行计算机安全主管部门报告。事件发生单位没有上级单位的，直接向人民银行当地分支行计算机安全主管部门报告。

第十二条　中国人民银行分支行接到银行系统的计算机安全事件报告后，应当在12小时内报告至人民银行分行、营业管理部、省会（首府）城市中心支行计算机安全主管部门。接到报告的中国人民银行各分行、营业管理部、省会（首府）城市中心支行，应当在事件发生24小时内报告人民银行总行计算机安全主管部门。

第十三条　任何单位或者个人均有权向人民银行当地分支行报告银行存在的计算机安全隐患。接到报告的人民银行有关部门应当立即对报告进行初步评估，如有必要应立即组织对计算机安全隐患进行检查和处置。

第十四条　计算机安全事件必须及时上报，报告内容应当要素齐全，客观准确。银行计算机安全事件报告制度执行情况列为银行计算机安全检查内容。

第十五条　本制度由中国人民银行负责解释。

第十六条　本制度自印发之日起实施。

2002年9月7日