附件 1：信息技术安全事件分类与等级划分

《信息安全事件分类分级指南》（GB/Z 20986-2007）根据信息技术安全事件的起因、表现、结果等，将信息技术安全事件分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害事件和其他信息安全事件 6 个基本分类，每个基本分类分别包括若干个子类；根据信息系统重要程度、系统损失和社会影响，将信息技术安全事件划分为 4 个等级。

一、信息技术安全事件分类

1.有害程序事件

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等 7 个子类。

2.网络攻击事件

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等 7 个子类。

3.信息破坏事件

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等 6 个子类。

4.设备设施故障

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故、和其它设备设施故障等 4 个子类。

5.灾害性事件

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

6.其他事件

其他事件是指不能归为以上基本分类的信息技术安全事件。

二、信息技术安全事件等级划分

1.特别重大事件（Ⅰ级）

特别重大事件是指能够导致特别严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受特别严重的系统损失；

（2）产生特别重大的社会影响。

2. 重大事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受严重的系统损失、或使重要信息系统遭受特别严重的系统损失；

（2）产生的重大的社会影响。

3.较大事件（Ⅲ级）

较大事件是指能够导致较严重影响或破坏的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受较大的系统损失、或使重要信息系统遭受严重的系统损失、一般信息信息系统遭受特别严重的系统损失；

（2）产生较大的社会影响。

4.一般事件（Ⅳ级）

一般事件是指不满足以上条件的信息安全事件，包括以下情况：

（1）会使特别重要信息系统遭受较小的系统损失、或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失；

（2）产生一般的社会影响。