个人信息事故判定标准及处理级别

根据《个人信息事故报告制度》，特制定个人信息事故判定标准及处理级别。

一、 事故判定标准

1、事故等级判定标准主要根据个人信息事故发生的性质、原因及对社会、信息主体造成的影响和损失来判定，判定标准按照严重程序由高至低分为四级（3、2、1、0）。

2、标准值修定因素

（1） 不报或瞒报的增加一级；

（2） 反复发生同类事故的增加一级；

（3） 及时采取措施，减轻损失的降低一级。

事故级别判定表

事故级别	性质	影响	原因	损失
3	非法搜集、非法使用、违反法规	对社会影响很大	故意或有组织的	信息量大，损失大
2	违反规范	对社会影响较大或对信息主体影响大	管理制度严重漏洞	信息量大，损失较大
1	违反本单位个人信息保护管理制度的	对社会影响较小或对信息主体影响较大	管理制度不完善或个人原因	信息量较大，损失较小
0	没有违反规定	对信息主体影响较小	不是人为因素	信息量小，没有造成损失

事故判定级别，按表中有关性质、原因、影响、损失分级，按其中一项符合的最高级别判定。

3、个人信息事故判定参考事例

下表为个人信息事故等级判定参考事例，对不在表中的事例，可根据事故恶劣程度及所造成的危害和损失与表中事例对应，选择合适的级别，并给予相应的处理。

事故级别	参考事例
3	• 单位有组织的违反个人信息保护规范的行为。 • 单位非法搜集大量个人信息用于不正当目的的行为。 • 单位非法买卖个人信息。

	• 因个人信息保护管理措施的不完善造成大量的个人信息流失,从而导致社会不稳定。
2	• 大量个人信息丢失和泄漏的案件多次发生; • 职工个人长期非法搜集个人信息,致使个人信息泄漏给信息主体造成严重经济损失的。 • 员工出卖单位保管的个人信息。 • 未经信息主体许可,将个人信息与其它单位间进行交流,造成个人信息非法使用并给信息主体千万重大损失的。
1	• 员工把禁止带出的个人信息带出公司,并造成个人信息丢失。 • 保存有个人信息的笔记本电脑或电子媒体被偷或丢失。 • 由于系统设置错误,而导致网站上的客户信息泄露。 • 由于盗窃致使在办公室保管的个人信息丢失。 • 超过使用目的外过量搜集大量个人信息,并进行非法使用的。
0	• 员工将携带出公司的个人信息丢失,但信息有密码设置,有保护措施; • 由于管理原因或系统原因造成个人信息丢失,并及时找回,没有给客户和信息主体造成损失; • 由于系统原因造成少量个人信息泄漏,但及时发现并弥补了损失

二、 事故处理

按照事故判定级别,对不同类型单位分别处理,并备案。具体处理见下表:

事故处理	处理办法		
	已认定单位	正在审查过程中	申请过程中
3	取消认定	停止审查	半年内不可申请
2	严重警告(停止使用标志三个月)	3 个月内停止审查	3 个月内不可申请
1	警告	1 个月内停止审查	1 个月内不可申请
0	批评	不影响审查	不影响申请