政府资讯科技总监办公室

信息安全

信息安全事故处理

实务指南

[ISPG-SM02]

第 1.2 版

2021 年 6 月

版权公告

修改记录

修改次数	修改详情	经修改页数	版本编号	日期
1	G54 信息安全事故处理指南第 5.0 版已转换成信息安全事故处理实务指南。修改报告可于政府内部网络「信息技术情报网」查阅：(http://itginfo.ccgo.hksarg/content/itsecure/review2016/amendments.shtml)	整份文件	1.0	2016 年 12 月
2	增加关于信息技术安全管理的新章节及与其他实务指南保持参考上的一致。	整份文件	1.1	2017 年 11 月
3	详细解释政府信息系统的范围，以及举例说明对事故的评估和决定。报告机制的表格亦作出轻微修改。	第 6 页、26 页、附件 C	1.2	2021 年 6 月

目录

1. 简介

有效的信息安全管理包括识别、防范、侦测、应急和复原的互相配合。除部署强而有力的安全保护措施外，决策局／部门还应具备事故应急能力，以备在发生信息安全事故（以下简称为安全事故或事故）时启动适当程序。适当及预早的计划能确保人员知悉、协调及有系统地进行事故应急和复原活动。决策局／部门须建立、记录、测试及维护一套本身信息系统的安全事故应急／报告程序。

1.1 目的

本文件就信息安全事故处理计划的制订，以及信息安全事故的防范、侦测及应急，为管理、行政及其他技术和操作人员提供指导说明。由于不同信息系统的信息安全事故可能构成不同的影响和导致不同的后果，决策局／部门应根据其实际的操作需要，为本身的信息系统制订合适的信息安全事故处理程序。

本文件旨在提供政府内部信息安全事故处理的实际指南和参考，但并不包括对个别具体计算机硬件或操作系统平台的详细技术描述。决策局／部门应就有关技术细节咨询相关的系统管理员、技术支持人员和产品供货商。

1.2 参考标准

以下的参考文件为本文件在应用上的参考：

- 香港特别行政区政府《基准信息技术安全政策》[S17]
- 香港特别行政区政府《信息技术安全指南》[G3]
- Information technology - Security techniques - Information security management systems –Overview and vocabulary (fourth edition), ISO/IEC 27000:2016
- Information technology - Security techniques - Information security management systems - Requirements (second edition), ISO/IEC 27001:2013
- Information technology - Security techniques - Code of practice for information security controls (second edition), ISO/IEC 27002:2013
- Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management, ISO/IEC 27035‑1:2016
- Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response, ISO/IEC 27035-2:2016

1.3 定义及惯用词

本文件将会采用《基准信息技术安全政策》和《信息技术安全指南》内所使用的及以下的定义及惯用词。

缩写及术语	
信息安全事件	发生可能违反信息安全或控制失效的情况。
信息安全事故	会对政府信息系统及/或数据资产造成伤害，或会损害其运作的一个或多个相关的及已证实信息安全事件。

1.4 联络方法

1.4.1 一般联络

本文件由政府资讯科技总监办公室编制及备存。如有任何意见或建议，请寄往：

电邮： it_security@ogcio.gov.hk

Lotus Notes 电邮： IT Security Team/OGCIO/HKSARG@OGCIO

CMMP 电邮： IT Security Team/OGCIO

1.4.2 政府信息安全事故应急办事处常设办公室

政府信息安全事故应急办事处常设办公室的联络数据如下：

24 小时事故报告热线： 2827 8585

电邮： csirt@govcert.gov.hk

Lotus Notes 电邮： GIRO Standing Office/OGCIO/HKSARG@OGCIO

CMMP 电邮： GIRO Standing Office/OGCIO

有关更多政府事故处理联络数据，请参阅政府内部网络「信息技术情报网」的「信息技术安全专题」网页
(https：//itginfo.ccgo.hksarg/content/itsecure/sih/contacts.shtml)。

2. 信息安全管理

信息安全是关于安全控制和措施的规划、实施和持续提升，以保护信息资产的机密性、完整性和可用性，适用于信息的存储、处理或传输过程及其相关信息系统中。信息安全管理是一套有关规划、组织、指导、控制的原则和应用这些原则的法则，来迅速有效地管理实体、财务、人力资源和信息资源，以及确保信息资产和信息系统的安全。

信息安全管理涉及一系列需要持续监测和控制的活动。这些活动包括但不限于以下的范畴：

- 安全管理框架与组织；
- 管治、风险管理和遵行要求；
- 安全操作；
- 安全事件和事故管理；
- 安全意识培训和能力建立；和
- 态势感知和信息共享。

安全管理框架与组织

决策局 / 部门须根据业务需要和政府安全要求，制定和实施部门信息安全政策、标准、指南和程序。

决策局 / 部门亦须界定信息安全的组织架构，并为有关各方就安全责任提供清晰的定义和适当的分配。

管治、风险管理和遵行要求

决策局 / 部门须采用风险为本的方法，以一致及有效的方式识别信息系统的安全风险、订定应对风险的缓急次序和应对有关风险。

决策局 / 部门须定期和在必要时对信息系统和生产应用系统进行安全风险评估，以识别与安全漏洞相关的风险和后果，并为建立具成本效益的安全计划和实施适当的安全保护和保障措施提供依据。

决策局 / 部门亦须定期对信息系统进行安全审计，以确保当前的安全措施符合部门信息安全政策、标准和其他合约或法律上的要求。

安全操作

为保护信息资产和信息系统，决策局 / 部门应根据业务需要实施全面的安全措施，涵盖业务上不同的技术领域，并在日常操作中采取「预防、侦测、应急和复原」原则。

- 预防措施避免或阻止不良事件的发生；
- 侦测措施识别不良事件的发生；
- 应急措施是指在发生不良事件或事故时，采取相应行动来遏制损害；和
- 复原措施是将信息系统的机密性、完整性和可用性恢复到预期状态。

安全事件和事故管理

在现实环境中，由于存在不可预见并致服务中断的事件，故此安全事故仍可能会发生。若安全事件危及业务的连续性或引起数据安全风险，决策局 / 部门须启动其常规安全事故管理计划，以实时识别、管理、记录和分析安全威胁、攻击或事故。决策局 / 部门亦应准备与有关各方适当地沟通，透过分享对有关安全风险的应急以消除不信任或不必要的猜测。当制定安全事故管理计划时，决策局 / 部门应规划和准备适当的资源，并制定相关程序，以配合必要的跟进调查。

安全意识培训和能力建立

因为信息安全是每个人的责任，所以决策局 / 部门应不断提升机构内的信息安全意识，透过培训及教育，确保有关各方了解安全风险，遵守安全规定和要求，并采取信息安全的良好作业模式。

态势感知和信息共享

因应网络威胁形势不断变化，决策局 / 部门亦应不断关注由安全行业和政府计算机安全事故协调中心发布的现时安全漏洞讯息、威胁警报和重要通知。应将即将或已经发生具威胁的安全警报传达及分享给决策局 / 部门内的负责同事，以便采取及时的应对措施来缓解风险。

决策局 / 部门可以利用网络风险信息共享平台接收和分享安全事务、安全漏洞和网络威胁情报的讯息。

人员亦可以通过参与安全演习和参加研讨会、展示会或浏览载有安全情报信息（例如网络风险信息共享平台）和一般安全信息（例如网络安全信息站、信息安全网）的专页来提高安全意识。

3. 安全事故处理简介

在信息安全管理中，「安全操作」职能范畴包括适当地部署安全保护和安全措施以降低成功攻击的风险。但是，尽管采取了这些措施，安全事故仍会发生。故此，信息安全事故处理计划应预先准备，这是安全事件与事故管理下的一个主要范畴。一旦服务下降或暂停，这些计划能帮助决策局／部门对事故做好应对和恢复服务的准备。应当委派适当的人员和各按其职、预留资源和规划好处理程序，以应付安全事故。预先的准备将有助于响应安全事故，并能让信息系统以更有组织、有效率和有效地恢复。

3.1 信息安全事故

安全威胁是指可能会为信息资产、系统及网络带来负面影响（例如利用信息系统或网络的漏洞）的潜在事件或任何情况。信息安全事件是指可能违反信息安全或控制失效的事件。信息安全事件的发生并不一定代表攻击成功。不是所有信息安全事件都会被分类为信息安全事故。「信息安全事故」一词在本文件中指会对政府信息系统（包括由政府提供和负责维护的信息系统，不论该信息系统是在政府内部或以外推行）及数据资产造成伤害，或会损害其运作的一个或多个相关的已证实信息安全事件。例如，信息安全事故可以是指不合乎政府利益的数据泄漏，或信息系统及／或网络内的负面事件，而且对计算机或网络安全的机密性、完整性和可用性构成影响。本实务指南的重点是信息安全相关的事故，自然灾害、硬件／软件故障、数据线故障、停电等负面事件并不包括在本实务指南范围内。这些负面事件应通过相关系统维修和运作复原计划处理。

常见的安全事故包括：拒絕服务攻击、入侵信息系统或数据资产、保密数据在电子形态下泄漏、恶意破坏或窜改数据、滥用信息系统、大规模感染恶意软件、网站遭涂改，以及影响联网系统的恶意脚本程序。

下图解释威胁、安全事件及安全事故之间的关系：

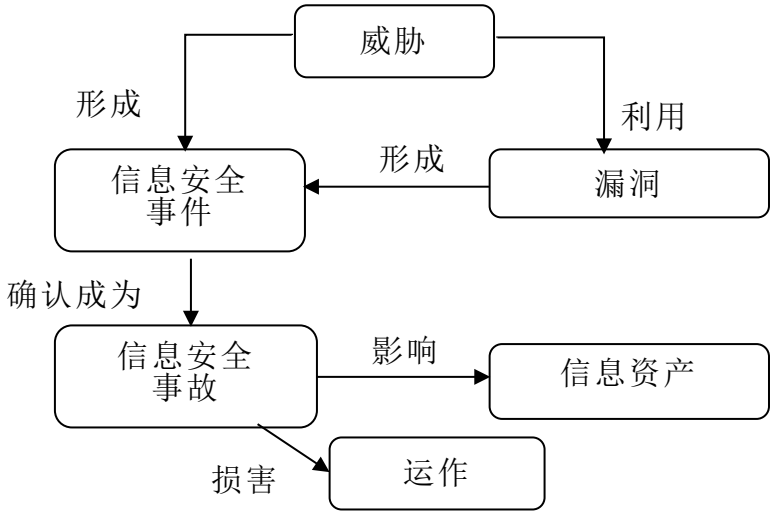


图 3.1 安全事件及安全事故的关系

3.1.1 安全事故处理

安全事故处理是一系列持续进行的程序，规管安全事故发生前、发生时和发生后所采取的措施。

安全事故处理始于规划和准备资源，以及制订适当程序（例如升级处理和安全事故应急程序），以备日后遵照执行。

一旦安全事故被识别，负责安全事故应急的各方须按照预定程序实施应急。安全事故应急是指为处理安全事故并恢复系统的正常操作状态，而进行的工作或采取的措施。

安全事故过后，应采取跟进行动对事故进行评估，并加强安全保护措施，以防止再度发生事故。应覆检规划和准备的工作，并作出相应的修订，以确保有足够的资源（包括人力资源、设备和技术知识）和有妥善制订的程序处理日后的同类事故。

3.2 安全事故处理的目的

明确清晰的安全事故处理计划对高效益及有效处理安全事故至为重要。它能于安全事故发生时减少影响和破坏，并有助迅速复原系统的运作。安全事故处理的主要目的如下：

- 确保具备处理事故所需的资源（包括人力资源、技术等）。
- 确保负责安全事故处理的各方明确了解，在发生安全事故时应按预定程序进行的工作。
- 确保事故应急有条不紊并具效益，而且能够迅速复原受袭系统。
- 确保事故应急工作已获确认和互相配合。
- 尽量减少泄漏数据、破坏数据和系统中断等事故可能造成的影响。
- 在适当情况下，分享事故应急经验。
- 防止受到进一步的攻击和破坏。
- 处理相关的法律问题及在认为有需要时转介警方作刑事调查。
- 若涉及个人资料，应向个人资料私隐专员公署报告。
- 在切实可行范围内尽量保存资料作调查之用。

鉴于信息技术在政府内部迅速发展，所有决策局 / 部门都必须制订一套安全事故处理计划，尤其是设有下列信息系统的决策局和部门：

- 与外部（例如互联网）连接的系统。
- 处理敏感数据和数据的系统。
- 关键任务系统。
- 任何可因安全事故的发生而受重大不良影响的系统。

3.3 披露事故信息

除向负责处理安全事故及系统安全工作，或获授权参与调查计算机罪行或滥用计算机事故的人士外，所有人员不得向任何人士披露有关计算机罪行及滥用计算机事故中的受害人、决策局 / 部门、受影响系统或造成该次事故的系统安全漏洞和入侵方法的数据。

披露任何事故信息，包括被攻击的方法、系统背景数据如实体位置或操作系统等，可能会鼓励黑客入侵具有相同漏洞的其他系统，亦可能会影响警方侦查时的鉴证及检控工作。但是，在事故事后分析之后，可能会得出防止类似安全事故的行动建议。如果建议内不包含个人、决策局 / 部门和系统发生事故的具体信息，便可以在政府内分享，让其他决策局 / 部门也可以防止类似的事故，并改善其安全处理程序。

4. 组织架构

下图所示为政府内部安全事故应急组织架构的通用参考模型。

根据基准信息技术安全政策，每个决策局 / 部门须成立一个信息安全事故应急小组以协调处理与决策局 / 部门有关的信息安全事故。政府信息安全事故应急办事处则集中统筹并支持各决策局 / 部门内部的信息安全事故应急小组。各决策局 / 部门的信息安全事故应急小组负责监督决策局 / 部门内部特定信息技术系统、计算机服务或职能范围的事故处理程序。

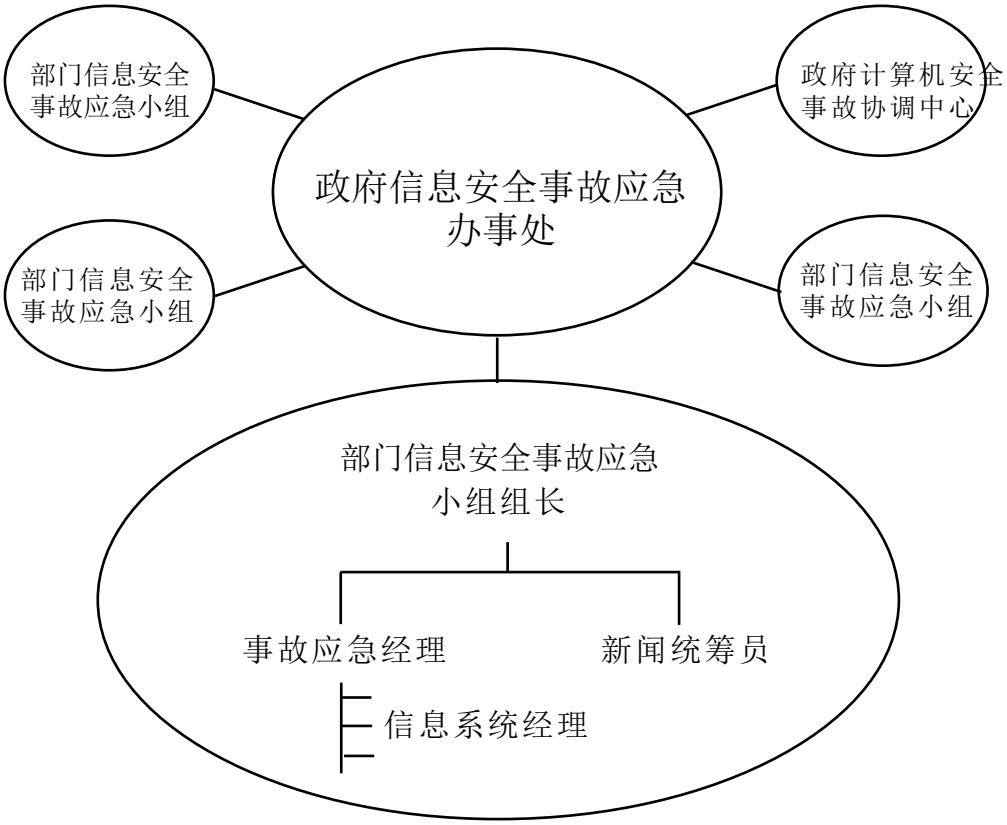


图 4.1 参与安全事故处理的各方

本章阐述信息安全事故处理的高层次组织架构和参与信息安全事故处理工作各方的职务和职责。信息安全事故应急小组及负责部门信息系统的人员，应根据决策局 / 部门或相关系统的特殊业务需要和操作要求，制订详细的信息安全事故处理程序。

4.1 政府信息安全事故应急办事处

政府信息安全事故应急办事处（GIRO）是为整个政府提供服务的组织，负责中央统筹及支持各个决策局 / 部门内的信息安全事故应急小组，以处理信息安全事故。

政府信息安全事故应急办事处常设办公室扮演政府信息安全事故应急办事处的执行机构。政府信息安全事故应急办事处常设办公室主要功能包括：

- 在信息安全事故报告中扮演信息安全事故应急小组组长的中心联络点，以及为可能涉及整个政府的信息安全事故作应急协调。
- 就事故跟进进度，以及提醒相关的部门信息安全事故应急小组提交事后报告及中期报告。
- 与政府计算机安全事故协调中心紧密合作，并在有需要时寻求对方建议。
- 若涉及刑事行为，与香港警务处网络安全及科技罪案调查科紧密合作。

4.1.1 政府信息安全事故应急办事处的职能

政府信息安全事故应急办事处主要有以下职能：

- 设立中央数据库，并监督政府内部对所有信息安全事故的处理。
- 定期编制政府信息安全事故统计报告。
- 充当中央协调办事处，以应付多点安全攻击（即不同的政府信息系统同时遭受攻击）。
- 促使决策局 / 部门的信息安全事故应急小组互相分享和交流信息安全事故处理的经验和数据。

4.1.2 政府信息安全事故应急办事处的结构

政府信息安全事故应急办事处的核心成员包括来自下列决策局 / 部门的代表：

- 政府资讯科技总监办公室
- 安全局
- 香港警务处

视乎不同安全事故的性质，必要时可能会邀请个别决策局 / 部门的信息安全事故应急小组成员和其他专家，为政府信息安全事故应急办事处的运作提供协助。

政府信息安全事故应急办事处常设办公室负责为政府信息安全事故应急办事处提供秘书处和职能方面的支持，并于应付可能影响整个政府的信息安全事故时，担任各部门信息安全事故应急小组组长间的中心联络点，以收集信息安全事故报告和统筹应急行动。

各决策局和部门须向政府信息安全事故应急办事处常设办公室提供信息安全事故应急小组组长的联络数据，如数据有任何更改，应向常设办公室提供最新的数据，以确保信息有效传递。部门信息技术安全联络数据更新表载于**附件 A**。

政府信息安全事故应急办事处在必要时可成立特殊专责小组（例如在发生多点攻击时），就影响遍及多个决策局 / 部门及 / 或政府整体运作和稳定的安全事故，协调应急工作。

4.2 政府计算机安全事故协调中心

政府计算机安全事故协调中心于 2015 年 4 月成立，与政府信息安全事故应急办事处常设办公室合作，负责协调政府内部的信息和网络安全事故。该中心还与其他计算机应急小组合作共享事故信息和威胁情报，并互相交流良好实践及做法，以加强该地区的信息和网络安全能力。政府计算机安全事故协调中心具有以下主要功能：

- 就即将发生和实际威胁，向决策局 / 部门发出安全警报。
- 作为计算机安全事故协调中心与其他计算机应急小组合作在处理网络安全事件时的桥梁。

4.3 部门信息安全事故应急小组

根据基准信息技术安全政策，各决策局 / 部门须成立信息安全事故应急小组。该小组是决策局 / 部门内部负责协调、传讯和采取安全事故处理行动的协调中心。信息安全事故应急小组的规模应按不同决策局 / 部门信息系统的规模和范围、系统的敏感程度以及安全事故对决策局 / 部门的潜在影响，作出相应调整。

虽然政府信息安全事故应急办事处负责集中统筹信息安全事故的报告，并为个别信息安全事故应急小组提供协调和咨询支持，但各决策局 / 部门的信息安全事故应急小组，仍须在处理决策局 / 部门内发生的安全事故时，负责整体指挥和控制。

4.3.1 信息安全事故应急小组的职能

信息安全事故应急小组的主要职能应包括：

- 整体监督和协调决策局 / 部门内部所有信息技术系统的安全事故处理。
- 在报告安全事故方面，与政府信息安全事故应急办事处合作，以便中央记录和采取必要的跟进行动，例如报告警方作进一步罪案调查。
- 转发政府信息安全事故应急办事处就即将发生及已经发生的事故所发放的警报，给决策局 / 部门内部负责有关工作的各方人士。
- 促进决策局 / 部门内部就安全事故处理，以及其他相关事务分享经验和交流信息。

4.3.2 信息安全事故应急小组的结构

信息安全事故应急小组是决策局 / 部门内协调所有信息技术安全事故的中央联络点。决策局 / 部门首长应从高层管理人员中挑选一名人员，担任信息安全事故应急小组组长。组长应有权任命信息安全事故应急小组的核心成员。

在筹组信息安全事故应急小组时，部门信息技术安全主任应给予建议和支持，以协助信息安全事故应急小组组长为部门信息系统制订个别系统的特定安全政策和事故处理计划，并制订相关的后勤安排。部门信息技术安全主任还须确保所在决策局 / 部门的所有信息系统，已遵守和履行部门整体信息技术安全政策的规定。

虽然信息安全事故应急小组可根据决策局 / 部门的不同计算机设备情况，决定小组成员的实际组合，但信息安全事故应急小组内也有一些必要的关键职务，包括信息安全事故应急小组组长、事故应急经理、新闻统筹员和信息系统经理等。这些职务可由多人或一人负责。

下文将详述信息安全事故应急小组内各项职务及职能。

4.3.3 信息安全事故应急小组成员的职责

4.3.3.1 组长

组长的职责包括：

- 全面监督及协调处理决策局 / 部门内所有信息系统的信息安全事故。
- 根据事故应急经理提供的事故报告及分析，就控制损毁、系统复原、外部机构委聘及其所参与工作的程度，以及复原后恢复正常服务的后勤工作等关键事项作出决策。
- 因应事故对决策局 / 部门业务运作的影响，在适当情况下启动部门的运作复原程序。
- 代表管理层批核为事故处理程序投放的资源。
- 代表管理层批核就事故的立场所作的公众发布。
- 在报告信息安全事故（特别是报告具有下列特点的信息安全事故）方面，与政府信息安全事故应急办事处常设办公室协调及合作，以便作中央记录及采取必要的跟进行动：
  - (i) 直接提供公共服务的系统，而且系统故障可能导致服务中断（例如向政府互联网网站的拒绝服务攻击）
  - (ii) 处理保密数据的系统
  - (iii) 支持关键任务操作的系统
  - (iv) 一旦发生安全事故，可能造成重大不良影响的系统，例如因网站遭涂改而使政府形象受损
- 促进决策局 / 部门内部互相交流和分享信息安全事故处理及相关事宜的经验和数据。
- 与调查机关协调及配合调查安全事故。

4.3.3.2 事故应急经理

事故应急经理负责监察决策局 / 部门内部的所有安全事故处理程序，并为处理事故程序寻求管理层提供资源和支持。事故应急经理的职责包括：

- 整体管理及监督决策局 / 部门内部与安全事故处理相关的所有事务。
- 在接获影响部门信息系统的安全事故报告后，通知信息安全事故应急小组组长。
- 与信息系统经理和有关方面跟进安全事故，汇编事故报告和进行分析。
- 向信息安全事故应急小组组长汇报安全事故处理程序的进展情况。

- 在处理信息事故时与警方、个人资料私隐专员公署、服务承包商、服务支持供货商及安全顾问等外部机构和人士协调。
- 为事故处理工作，向信息安全事故应急小组组长寻求提供所需的资源和支持。

4.3.3.3 新闻统筹员

新闻统筹员负责回复公众有关决策局／部门安全事故的查询。新闻统筹员还负责整体控制和监督向公众（包括传媒）发布信息的工作。

4.3.3.4 信息系统经理

应拨出特定的资源来应付个别信息系统、计算机服务或职能范围可能发生的安全事故。

当处理信息安全事故时，个别部门支持小组的规模和结构将视乎部门系统的范围和性质而有所区别。举例来说，就小型、非关键的内部系统而言，一人便已足以履行事故应急的职责。

对于个别部门的信息系统，相关的部门信息系统经理将监督整个系统安全事故处理流程或其职责范围。经理应代表个别部门信息系统下的支持小组，提供以下主要功能：

- 监督所负责职能范围的安全事故处理程序。
- 事先制订相关的事故处理程序和联络名单，以加快及推动处理程序。
- 提供直接接收可疑事故报告的途径。
- 直接并实时响应可疑活动。
- 协助将破坏减至最少，并回复系统正常操作。
- 向服务承包商、计算机产品供货商、警方或个人资料私隐专员公署等外部机构和人士寻求有关安全问题的意见。
- 与其他外部机构和人士协调相关信息系统的安全事故处理工作。
- 就所负责职能范围，对来自信息安全事故应急小组和政府计算机安全事故协调中心的安全警报，进行影响分析。

如果信息系统的部分操作或全部操作均已外包予外部服务供货商及／或已包括在其他政府部门提供的服务范围内，则外包服务供货商及／或提供服务的部门亦应委任信息系统经理及成立类似的支持小组以应对该特定的信息系统，并提供与其职责相应的服务。

除提供以上主要功能，信息系统经理应负责以下职务:

- 制订及推行个别系统的安全事故应急程序。
- 遵守并遵从安全事故应急程序，向决策局 / 部门的信息安全事故应急小组报告事故。
- 与服务供货商、承包商和产品支持供货商等相关各方安排及协调，针对事故采取修正和复原行动。
- 向信息安全事故应急小组报告安全事故，在信息安全事故应急小组的管理支持下，于调查和收集证据的过程中对外寻求协调，例如寻求警方、个人资料私隐专员公署或香港计算机安全事故协调中心的协助。
- 掌握最新的信息安全科技和技术，并了解与系统或所负责职能范围相关的最新安全警报和安全漏洞。
- 利用安全工具 / 软件及 / 或系统记录并检查审计追踪记录，找出可疑的攻击或未获授权的访问。
- 在诊断问题和复原系统过程中，提供有助于证据收集、系统备份和复原、系统配置和管理等技术支持。
- 为信息系统安排定期安全评估、影响分析和覆检。

5. 安全事故处理步骤概览

安全事故处理共有 5 个主要步骤，有关概述见下文。各步骤所涉及的过程在相应章节会有更详细描述。

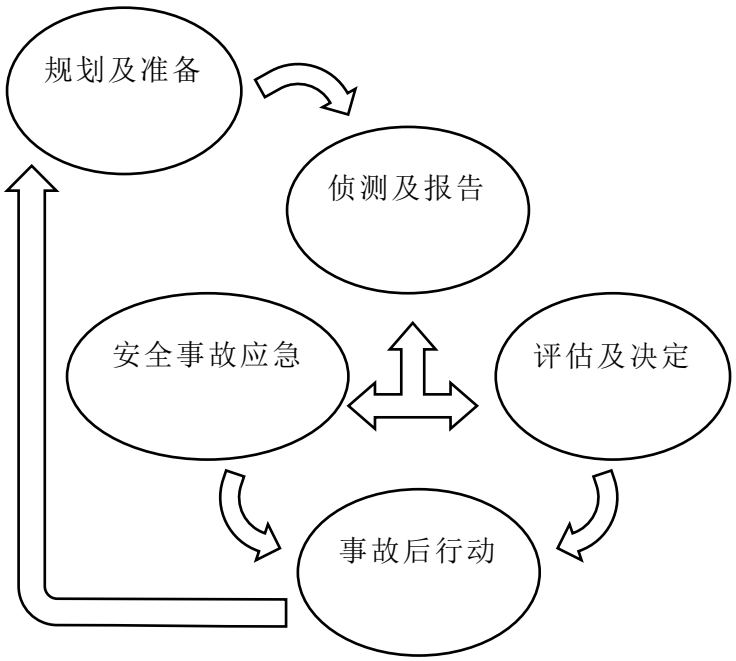


图 5.1 安全事故处理的循环过程

A. 规划和准备（第 6 章）

在这步骤中，决策局 / 部门应规划和准备资源，并制订适当程序，以备日后遵照执行。本步骤涉及的主要活动如下。

- 安全事故处理计划
- 报告程序
- 升级处理程序
- 安全事故应急程序
- 培训与教育
- 事故监察措施

B. 侦测及报告（第 7 章）

在这步骤中，决策局 / 部门应根据建立的检测和监控机制检测安全事件。决策局 / 部门也应遵循报告程序，使安全事件得到部门信息安全事故应急小组的关注。这一步有两个主要的活动：

- 侦测措施
- 报告

C. 评估及决定（第 8 章）

侦测到事件后，决策局 / 部门应确定是否真有事故发生。如果事件被识别为信息安全事故，决策局 / 部门应确定事故的类型，并评估其范围、损害和影响，以有效处理事故。决策局 / 部门还应遵循事先规划的升级处理程序通知相关方面，并将事件升级到适当的级别。这步骤涉及的主要活动有：

- 事故评估
- 升级处理

D. 安全事故应急（第 9 章）

当识别到安全事故时，决策局 / 部门应遵循安全事故应急程序，采取行动处理安全事故，恢复系统正常运作。应急程序大致分为三个阶段：

- 遏制
- 杜绝
- 复原

E. 事后跟进（第 10 章）

事故结束后，应采取后续行动对事故进行评估，加强安全防范，防止再次发生。主要后续行动如下：

- 事故事后分析
- 安全事故报告
- 安全评估
- 覆检现行的保护措施
- 调查及检控

6. 规划和准备

适当的事先规划可确保人员对应采取的事故应急及复原行动有所了解，使其能在互相配合及有条不紊的情况下执行。决策局 / 部门须备存最新信息系统列表，当中附有安全事故处理的紧急联络点。及早计划还有助决策局 / 部门在处理安全事故时作出适当和有效的决定，从而将安全事故可能造成的破坏减到最少。安全事故应急计划包括加强安全保护措施、采取适当的事故应急、系统复原和其他跟进工作。

规划和准备所涉及的主要工作如下：

- 安全事故处理计划
- 报告程序
- 升级处理程序
- 安全事故应急程序
- 培训与教育
- 事故监察措施

安全事故处理准备工作列表列于**附件 B**，以供参考。

6.1 安全事故处理计划

安全事故处理计划应符合基准信息技术安全政策及信息技术安全指南，一般应涵盖以下几个主要部分：

- 范围
- 目标和优先处理事项
- 职务和职责
- 限制

6.1.1 范围

这部分为界定安全事故应急小组的职能范围。有关范围既可包括整个决策局 / 部门（即信息安全事故应急小组），亦可局限于决策局 / 部门内部的特定信息系统或应用程序。

6.1.2 目标和优先处理事项

事先应明确制订安全事故处理计划的目标，并根据系统和管理需要为目标排列缓急次序。及后制订的安全事故应急程序应配合这些预定的目标。

视乎不同系统和管理需要，事故处理的目标宜包括：

- 评估事故的影响和破坏
- 尽快使系统恢复正常操作
- 尽量减轻事故对其他系统的影响
- 避免发生同类事故
- 找出事故的根本成因
- 收集证据为日后的个案调查提供证明
- 有必要时更新政策和程序

部分事故的性质过于复杂或规模过大，以致难以在同一时间解决所有问题。为处理的事项订定缓急次序便是一个关键步骤，让事故应急人员可以聚焦先处理最关键事项。建议优先处理以下的事项：

- 保障生命和人身安全
- 保护关键资源
- 保护遗失或损毁后会造成较大损失的敏感或重要数据
- 防止停顿后会造成较大损失及复原成本较高的系统受到损坏
- 对服务中断的影响减到最少
- 维护决策局 / 部门或政府整体的公众形象

6.1.3 职务和职责

参与安全事故处理工作各方的职务和职责应明确界定。上述第 4 章为界定安全事故应急小组主要成员的职务和职责提供了参考模型。

6.1.4 限制

资源、科技和时间等限制因素应予考虑。这些限制可能影响安全事故处理工作的结果。举例来说，决策局 / 部门如缺乏内部技术专才，便可能须委聘外部顾问或服务承包商。这些准备工作应事先办妥，确保在发生安全事故时能够顺利处理。

6.2 报告程序

应建立及记录一套报告程序，清楚订明任何可疑活动的报告步骤和程序，以便及时向有关各方作出报告。报告程序应列明详尽的联络数据，例如电话号码（包括办公时间及非办公时间内的联络电话号码和流动电话号码）、电邮地址和传真号码等，以确保负责人员之间能够有效沟通。一些建议的报告机制载于**附件 C** 第 1 节，以供参考。

事先应制订适当的报告程序，以便一旦发生安全事故，参与事故应急的全体人员知悉应向何人和以何种方式报告，以及应注意和报告的事项。

为有效执行报告程序，应注意以下几点：

- 报告程序应载列明确的联络点，并制订简单但明确的步骤以便遵从。
- 向所有相关人员发布报告程序，以供参阅和参考。
- 确保所有相关人员熟习报告程序，并能够立即报告安全事故。
- 编制安全事故报告表，以规范所收集的资料。
- 考虑是否需要在非办公时间启动报告程序，如确有需要，应制订一份独立的非办公时间报告程序，并指定相关人员担任非办公时间联络人。
- 有关事故的资料应根据「有需要知道」原则披露，除信息安全事故应急小组组长外，任何其他人士均无权阅览，也不得授权他人将有关安全事故的资料与他人分享。

为改善信息技术安全事故处理的效率和效益，当证实发生信息安全事故时，部门信息安全事故应急小组需要：

- 于 **60 分钟**内向政府信息安全事故应急办事处常设办公室作电话汇报，并于 **48 小时**内提交完整的信息安全事故初步报告表；
- 如安全事故牵涉关键电子政府服务、对安全有重大影响，或会引起传媒注意，尽快向政府信息安全事故应急办事处常设办公室分享以下数据：
  - (i) 事故类别及对事故范围、破坏及影响的评估；
  - (ii) 为遏止破坏及修正问题而正在或将会采取的行动；
  - (iii) 若引起传媒注意时的响应口径；以及
  - (iv) 传媒的查询及响应建议（如有）。
- 每日向政府信息安全事故应急办事处常设办公室更新受影响的关键电子政府服务的修复状况，直至服务恢复为止。
- 就任何已向香港警务处、个人资料私隐专员公署报告或向传媒机构发布的安全事故，通知政府信息安全事故应急办事处常设办公室。

应在解决事故后的1星期内，向政府信息安全事故应急办事处常设办公室提交事故事后报告。对于需要较长时间完成调查的个案，有关的部门信息安全事故应急小组需要就最新的修复情况及调查进度，每3个月向政府信息安全事故应急办事处常设办公室提交中期报告：

- 于证实事故后3个月内向政府信息安全事故应急办事处常设办公室提交第一份中期报告；以及
- 为令管理层获悉状况，每3个月向政府信息安全事故应急办事处常设办公室提交事故调查进度，直到结案为止。

6.3 升级处理程序

升级处理程序是指将事故上报管理层和有关方面，以确保立即作出重要决策的程序。

在发生事故时，往往需要处理大量紧急事项，所以很难找到适当人选处理林林总总的事项。为顺利执行安全事故处理的各阶段工作，应事先编备处理法律、技术和管理事项所需的重要联络名单。因此，制订升级处理程序是准备和规划阶段的主要工作之一。

升级处理程序按事故的类别和影响的严重程度，载列内部和外部各级别人员的联络点及各联络点的联络数据。

就不同类别的事故，升级处理程序的联络点和跟进行动也可能有所区别。不同类别的事故涉及不同的专业知识或管理决策，所以应编备特定的联络名单以处理这些事故。

有关升级处理程序的建议和升级处理程序示例载于**附件 D**，以供参考。报告及升级处理政府信息安全事故的工作流程示例载于**附件 E**，以供参考。

6.4 安全事故应急程序

安全事故应急程序界定了一旦发生事故应采取的步骤，其目的在于根据预定的目标和首要工作将破坏减至最少，杜绝事故的肇因，以及使系统恢复正常操作等。

须制订及记录安全事故应急程序，以便在事故处理程序中为安全事故应急小组提供指南。全体员工（包括管理层人员）均应知悉该程序，以作为参考和遵守的依据。这套程序应清晰明确而且容易理解，确保全体人员清楚了解应采取的行动。应急程序须定期进行测试和更新，以确保能迅速及有效地应对信息安全事故。此外，演习须至少每两年进行一次，最好每年进行一次，以评估程序的有效性。

有关事故应急演习流程及不同情景的行动卡详情，请参阅政府内部网络「信息技术情报网」的「信息技术安全专题」网页 (https://itginfo.ccgo.hksarg/content/itsecure/sih/actioncard/index.html) 。

第9章提供处理安全事故的参考模型，特别在遏制、杜绝和复原程序等方面。

6.5 培训与教育

决策局 / 部门须确保全体员工均遵守及遵从安全事故的处理 / 报告程序。各人员应熟习由事故报告、确认、采取适当行动到恢复系统正常操作的处理事故程序。决策局 / 部门应定期举行事故处理演习，使人员熟习有关程序。进行演习后，应对结果进行覆检，并提出建议，以在适当情况下改善事故处理程序。

此外，为了加强系统或职能范围的安全保护措施，并减低发生事故的机会，应向系统操作和支持人员提供足够的培训，使他们掌握有关安全预防的知识。由于终端用户往往最先察觉问题发生，因此应鼓励他们报告异常情况或涉嫌违反安全的情况。

6.6 事故监察措施

须采取足够的事故监察安全措施以便在正常操作时保护系统，同时监察潜在的安全事故。所采取措施的程度和范围则取决于系统、系统处理的数据及系统提供的功能的重要性和敏感程度。

下列是一些常见的安全事故监察措施：

- 安装防火墙构件并采取认证和访问控制措施，以保护重要系统和数据资源。
- 安装入侵检测工具，主动监察、侦测并就系统入侵或黑客活动作出应急。
- 安装抗恶意软件和恶意软件侦测及修复软件，以侦测及清除恶意软件，并防止恶意软件影响系统操作。

- 定期利用安全扫描工具进行安全检查，以找出目前存在的安全漏洞，并进行既定安全政策水平与实际安全工作环境之间的差距分析。
- 安装内容过滤工具，以侦测电子邮件或网络通讯的恶意内容或程序代码。
- 开启系统及网络审计记录功能，以便侦测和追踪未获授权活动。
- 开发程序和脚本程序协助侦测可疑活动、监察系统和数据的完整性，以及分析审计记录数据。
- 订阅安全新闻、警示、漏洞资料、报告和其他有关信息安全刊物，以提升对不断涌现的安全威胁和相关风险的警觉。
- 维护及记录漏洞管理机制，以识别、评估及减低安全风险。

7. 侦测及报告

7.1 侦测措施

决策局 / 部门应确保推行侦测及监察机制以侦测安全事件。决策局 / 部门应侦测信息安全事件的发生，并辅以以下资料，就事件作出报告：

- 网络监察装置（例如防火墙、网络使用分析工具或网页过滤工具）的警示。
- 安全监察装置（例如入侵检测系统、入侵防御系统、抗恶意软件方案、记录监察系统或安全信息管理系统）的警示。
- 来自装置、服务、主机及不同系统的记录数据分析。
- 来自用户或服务台的报告。
- 来自外来人士（例如其他信息安全事故应急小组、电讯服务供货商、互联网服务供货商、一般大众、媒体或外聘服务供货商）的外部通知。

信息安全事故应急小组应维护决策局 / 部门里所有信息安全事件的列表。

7.2 报告

人员应跟从报告程序，让信息安全事故应急小组注意有关安全事件。所有人员都须清楚知道及可以取得报告程序，以便报告不同种类的潜在信息安全事件。下列数据应是报告信息安全事件的依据：

- 侦测日期 / 时间
- 受影响系统
- 观察
- 报告该安全事件人士的联络资料

8. 评估及决定

在发现可疑活动后，信息系统的用户、操作员或管理员应遵照既定的报告程序，向有关信息系统经理报告事故。收集数据时可使用标准安全事故报告表，该报告表还可用作进一步调查和分析之用。另一方面，入侵检测工具和系统审计记录等监察工具亦可用来协助侦测未获授权或异常活动。

在侦测到异常情况后，信息系统经理应确认事故，此阶段的工作包括以下步骤：

- 判断是否发生事故，并进行初步评估
- 记录事故
- 如有需要，记录系统当前状况

要决定是否发生事故，决策局 / 部门应考虑包括但不限于以下情况：

- 有关系统是否在政府内部推行；
- 如有关系统并非在政府内部推行，

(i) 该系统是否由政府提供和维护；以及

(ii) 事故是否由系统的安全漏洞或不受政府控制的因素造成；例如推行该系统的一方犯错或违反政府的建议遗漏部分程序。

举例来说，决策局 / 部门发现由其提供和维护的系统存在安全漏洞，而该系统并非在政府内部推行。其后，决策局／部门为安全漏洞提供修补程序，并通知推行该系统的用户安装。如果用户没有安装，然后所推行的系统被黑客入侵，这通常不应视为政府安全事故。在类似情况下，如智能手机所安装的流动应用程序已获提供安全修补程序，但用户没有安装该修补程序，该手机所发生的违反安全事件也不算安全事故。

8.1 事故评估

首先，信息系统经理应判断是否确实发生事故。然而，判断所发现的异常情况是否就是发生事故的迹象往往十分困难。有些异常情况可能是由另外一些原因造成的（例如硬件故障或用户操作错误）。

为判断某种异常情况是系统问题还是真正事故所造成，信息安全事故应急小组应收集有关信息安全事件的信息，并要求报告安全事件的人士作任何澄清。**附件 F** 载列了一些值得特别注意的典型事故迹象、典型安全事故，以及决定事故范围及影响时需考虑的因素，以供参考。

8.2 升级处理

在某事件被识别为信息安全事故后，系统经理应判断事故的类别、评估事故的范围、破坏和影响，以便作出有效的应急。了解事故的类别有助确定处理事故的适当应急措施。此外，根据所造成的破坏和影响，还可立即采取一些预防或防卫措施。

相关的信息系统经理与负责整体协调的信息安全事故应急小组事故应急经理应通知适当人士，及跟从之前订立的升级程序，将事故提升至适当级别。

在升级处理过程中，建议在描述事故时提供下列数据：

- 简单描述事故：什么事故、事故在何时发生、系统如何受到攻击、所造成的破坏 / 影响。
- 说明攻击者（如有）是否仍在系统中活动。
- 系统数据，例如系统名称、功能，和主机名、互联网协议地址、操作系统及版本等其他技术数据。
- 补充数据（如有需要），例如撷取的屏幕画面、系统讯息等。

在升级处理过程中提供的资料应明确简洁、准确而真实。提供不准确、误导或不完整的数据可能会妨碍应急程序，甚至令情况恶化。决策局 / 部门还应考虑可否对外提供某些敏感数据。

如果决策局 / 部门确认有事故发生，有关信息安全事故应急小组组长应在确认事故后的 60 分钟内，向政府信息安全事故应急办事处常设办公室报告事故。

为便于记录和协调事故处理工作，信息安全事故应急小组组长还应提供一份信息安全事故初步报告（请参阅**附件 C** 第 2 节），向政府信息安全事故应急办事处常设办公室报告，包括但不限于下列各类信息安全事故（有关详情，请参阅**附件 F** 第 3 节）。

- 滥用信息系统
- 入侵信息系统或数据资产
- 拒绝服务攻击（包括中央或部门互联网网关闸、电邮系统、政府网站及／或向公众提供电子服务的系统）
- 泄漏电子保密数据
- 遗失存有保密数据的流动装置或抽取式媒体
- 伪冒
- 大规模恶意软件感染
- 勒索软件
- 网站遭涂改

与安全无关的事故（如下所列）无须向政府信息安全事故应急办事处常设办公室报告，而应该按照现行系统管理及操作的准则和程序处理。

- 系统受台风、水浸、火灾等自然灾害影响
- 硬件或软件问题
- 数据／通讯线故障
- 停电
- 例行系统关闭或维修时间
- 因管理／操作错误导致的系统故障
- 因系统或人为错误遗失或损毁保密数据
- 不影响政府系统和数据的欺诈电邮或网站

如发生对政府服务及／或形象构成重大影响的严重事故，政府信息安全事故应急办事处常设办公室与信息安全事故应急小组组长会密切监察事态发展。如果事故是针对整个香港特别行政区政府的多点攻击，常设办公室会立即通知政府信息安全事故应急办事处并采取必要的行动。

在处理数据外泄事故时，决策局／部门宜考虑采取补救措施如下：

- 立即收集有关外泄事故的重要资料。
- 采取适当措施，制止数据外泄。
- 评估造成伤害的风险。
- 考虑发出有关资料外泄的通报。

如果安全事故涉及个人资料，决策局／部门应尽快向个人资料私隐专员公署报告，通报表格模板可于个人资料私隐专员公署网站下载(http://www.pcpd.org.hk/chinese/publications/files/Notification_Form_c.pdf)。

决策局／部门应尽可能通知受影响人士。如基于合理原因而不作出通报，必须得到决策局局长／部门主管的批准方可。

如果决策局 / 部门怀疑发生计算机罪案，应联络香港警务处网络安全及科技罪案调查科。在向警方报告案件前，应事先征求信息安全事故应急小组高级管理层的意见和批准。此外，如果需要向警方或个人资料私隐专员公署报告安全事故，决策局 / 部门应通知政府信息安全事故应急办事处常设办公室，以便作中央记录和协调。

有关升级处理程序示例和有关安全事故升级处理程序的其他相关数据，请参阅**附件 D**。政府安全事故报告及升级处理工作流程阐述于**附件 E**，以供参考。

8.3 记录事故

应记录所有安全事故、已采取的行动和相关的行动结果。这些记录应以加密、上锁或访问控制方法妥善储存。这些记录有助确认和评估事故，为检控提供证据，并为及后的事故处理阶段提供有用的数据。整个安全事故应急过程都应保留记录。为事故设定编号有助在整个事故处理过程中作跟进和追踪。

事故记录最低限度必须包括以下数据：

- 系统事件和其他相关数据，例如审计记录
- 已采取的所有行动，包括日期、时间和参与行动人员
- 所有对外通讯，包括日期、时间、内容及有关各方

8.4 记录系统状况

在侦测到可疑活动后应以最快速度，并在技术和操作上可行的情况下记录受袭系统的状况。这些资料可防止攻击者销毁证据，并为日后的个案调查（例如收集法证证据）提供了证据。所记录的系统数据可包括下列项目：

- 服务器记录、网络记录、防火墙 / 路由器记录、访问记录等系统记录档案
- 仍在进行活动的系统登入或网络连接，以及有关程序状态的数据
- 受袭系统影像，以供调查，并作为日后采取跟进行动的证据

9. 安全事故应急

安全事故应急涉及制订程序评估事故并作出应急，尽快将受影响的系统组件和服务恢复正常。有关程序大致可分为 3 个阶段：即下图 9.1 所示的*遏制*、*杜绝和复原*。认识各阶段具体工作有利于制订有效的安全事故应急程序。

应急程序无须依足 3 个阶段的次序进行，决策局 / 部门可因应本身的实际需要自行制订应急程序各阶段的次序。

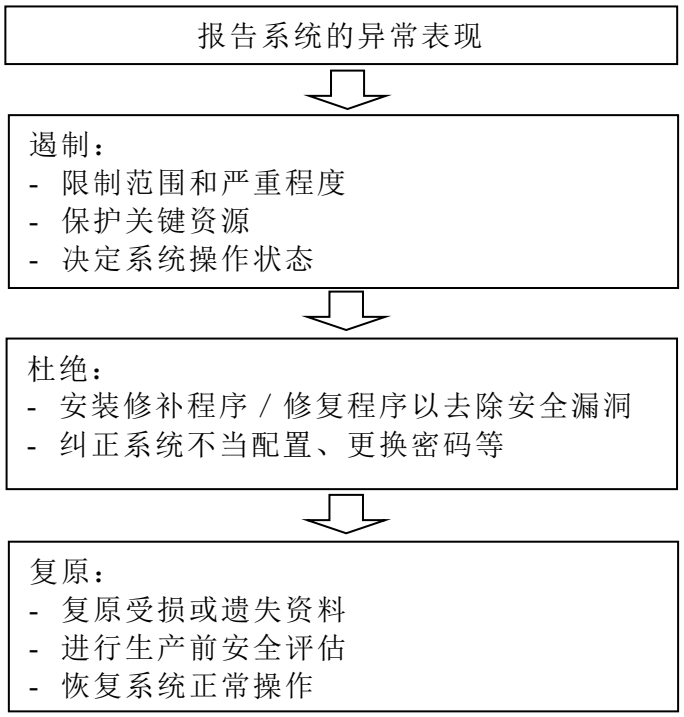


图 9.1 安全事故应急的主要阶段

9.1 遏制

事故应急的第一阶段是遏制。遏制的目的是限制事故的范围、严重程度和影响。有些事故，例如恶意软件感染可迅速传播，并造成大规模破坏。因此，在事故造成进一步破坏前，应限制事故的影响程度。

事先应清晰厘定并在安全事故应急程序中列明，针对不同的事故应采取哪种应急策略和程序，以及投入哪种资源。如果需要采取关键行动，便可能须要征求信息安全事故应急小组管理层的意见和批准（如有需要，信息安全事故应急小组也可能须要咨询政府信息安全事故应急办事处的意见）。

这一阶段的工作宜包括：

- 评估事故对数据和信息系统的影响，以确定有关的数据或数据是否已受事故破坏或感染。
- 保护敏感或关键数据和系统，例如将关键数据转移至与受袭系统或网络隔开的其他媒体（或其他系统）。
- 决定受袭系统的当前操作状态。
- 复制受袭系统的当前映像，以供调查，并作为日后采取跟进行动的证据；
- 记录这一阶段采取的所有行动。
- 检查共享网络服务，或任何因可信赖关系而与受袭系统连接的系统。

9.1.1 决定受袭系统的当前操作状态

有待作出的其中一项重要决定，是继续还是终止受袭系统的操作和服务。这项决定在很大程度上取决于事故的类别和严重程度、系统要求、对公共服务和决策局 / 部门以至整个政府形象的影响，以及事故处理计划内预定的目标和优先事项。

可采取的行动宜包括：

- 暂时关闭或隔离受袭的计算机或系统，以防止事故对互相连接的其他系统造成进一步破坏。这尤其是当事故会快速传播时，当储存敏感数据的计算机受到威胁时，又或是为了防止受袭系统被利用而向相连的系统发起攻击。
- 终止受袭信息系统的操作。
- 关闭系统的部分功能。
- 禁止用户访问或登入系统。
- 继续操作以收集有关事故的证据。该行动只适用于可承受某程度风险如服务中断或数据受损的非关键任务系统，而且在处理时须格外小心，并加以严密监控。

9.2 杜绝

遏制后的下一个阶段是杜绝。杜绝是指从系统清除导致事故的肇因，例如从受感染的系统和媒体清除恶意软件。

在移除任何档案或终止 / 删掉任何程序前，宜收集所有必需的数据，包括所有记录档案、仍在进行活动的网络连接及程序状态数据。这将有助于为日后的调查收集证据，因为这些数据可能会在清理系统时被删除或重新设定。

9.2.1 可杜绝事故的行动

在杜绝阶段，决策局 / 部门宜根据事故的类别和性质及系统要求，采取以下行动：

- 终止或删掉黑客在系统中产生或启动的所有程序，以停止破坏及逼使黑客离开。
- 删除黑客建立的所有伪冒档案。系统操作员在删除档案前应将伪冒档案作备分，以便日后调查。
- 清除黑客安装的所有后门程序和恶意软件。
- 采用修补和修复程序修补在所有操作系统、服务器和网络设备等发现的安全漏洞。在系统恢复正常操作前，应彻底测试所采用的修补或修复程序。
- 纠正系统和网络的不当设定，例如防火墙和路由器配置不当。
- 如发生恶意软件事故，应遵照抗恶意软件供货商的指南，在适当情况下，从所有受感染的系统和媒体清除恶意软件。
- 确保备份未受感染，以免系统在下一阶段利用备份复原系统时再度受到感染。
- 利用其他的安全工具，协助进行杜绝工作，例如利用安全扫描工具侦测入侵，并采用建议的解决方案。应确保使用具有最新检测模式的安全工具。
- 更换所有可能被黑客访问的登入帐户的密码。
- 在某些情况下，支持人员可能须要将所有受感染的媒体重新格式化，并利用备份重新安装系统和数据，尤其是在不确定事故对关键系统造成破坏的严重程度，或难以完全清理系统之时。
- 记录已采取的所有行动。

以上所列只是在处理安全事故时常见的措施示例。杜绝行动视乎事故的性质及事故对受袭系统的影响而定。在某些情况下，决策局 / 部门可能须寻求外部机构（例如警方、个人资料私隐专员公署及 / 或外部服务供货商）的意见，并参考其他决策局 / 部门处理类似事故的经验。此外，应寻求信息安全事故应急小组和政府信息安全事故应急办事处的意见和协调。

9.3 复原

事故应急的最后阶段是复原。本阶段的目的在于恢复系统的正常操作。复原工作包括：

- 评估事故的破坏。
- 必要时从可信赖的来源取得档案和数据，以重新安装被删除 / 遭破坏的档案或整个系统。
- 在受控制的情况下，按照需求的缓急次序逐阶段恢复功能 / 服务，例如可优先恢复最重要的服务或以大多数人为对象的服务。
- 检验复原操作是否成功，系统是否已恢复正常操作。
- 在恢复系统操作前，事先通知所有相关人士，如操作员、管理员、高级管理层和升级处理程序所涉及的其他人士等。
- 关闭不需要的服务。
- 记录已采取的所有行动。

在系统恢复正常操作前，其中的一项重要工作是进行生产前安全评估，以确保受袭系统及其相关组件已安全。这项工作可能会运用到安全扫描工具，以确定事故的问题根源已清除，同时找出系统内任何可能存在的其他安全漏洞。视乎事故的严重程度和系统的服务水平要求，评估可集中处理某个领域，也可以涵盖整个系统。

在进行一切复原工作前，须得到信息安全事故应急小组高级管理层批准。如有需要，可寻求政府信息安全事故应急办事处的支持和意见。

10. 事故后行动

系统恢复正常操作并不代表安全事故处理程序的结束。采取必要的跟进行动是十分重要的。跟进行动包括评估事故所造成的破坏、改良系统以防止再度发生事故、更新安全政策和程序及为日后的检控进行个案调查。

跟进行动可收以下效果：

- 改善事故应急程序。
- 改善安全措施，以保护系统日后免受攻击。
- 向违法者提出检控。
- 有助他人认识安全事故应急程序。
- 有助参与事故应急的各方人士汲取教训。

跟进行动包括：

- 事故事后分析。
- 事故事后报告。
- 安全评估。
- 覆检现行的保护措施。
- 调查及检控。

10.1 事故事后分析

事故事后分析是对事故及事故应急措施的分析，以作为日后的参考。这项分析有助更深入地了解系统受到的威胁及可能存在的安全漏洞，以便采取更有效的保障措施。

分析的范围包括：

- 防止再度受攻击的建议行动。
- 迅速取得所需的数据及获取有关数据的方法。
- 供侦测及杜绝程序所用或所需的额外工具。
- 准备和应急措施的足够程度。
- 沟通的足够程度。
- 实际困难。

- 事故的破坏，当中包括：
  (i) 处理事故所需的人力消耗
  (ii) 金钱成本
  (iii) 中断操作的损失
  (iv) 遗失或遭破坏数据、软件和硬件的价值，包括被泄露的敏感数据
  (v) 受托机密资料的法律责任
  (vi) 难堪或令信誉丧失
- 汲取的其他教训。

10.2 事故事后报告

根据事故分析所编制的事故事后报告，应概述事故、应急、复原行动、破坏和汲取的教训。相关信息系统的经理负责编制报告，并提交信息安全事故应急小组作参考，以便日后及时采取预防措施，避免其他系统和服务再度发生同类安全事故。

事故事后报告应包括下列项目：

- 事故的类别、范围和程度。
- 事故的详情：攻击的来源、时间和可能方法，以及发现攻击的方法等。
- 概述受攻击的系统，包括系统范围及功能、技术数据（例如系统硬件、软件和操作系统，以及版本、网络体系结构及程序编制语言等）。
- 事故应急及杜绝的方法。
- 复原程序。
- 汲取的其他教训。

事故事后报告应在解决安全事故后的1周内提交予政府信息安全事故应急办事处。事故事后报告样本载于**附件 C** 第 3.2 节，以供参考。

10.3 安全评估

可能受到安全风险威胁的系统宜定期进行安全风险评估和审计，尤其是曾经受安全事故影响的系统。安全覆检及系统审计应持续进行，以便及时发现可能存在的安全漏洞及／或因应安全保护措施及攻击／入侵科技的发展，而须作出的系统改善。

在发生安全事故时收集的资料亦有助于事后的安全评估，这对找出系统的安全漏洞和安全威胁尤其有用。

10.4 覆检现行保护措施

根据事故事后分析与定期安全评估所得出的结果，可确认系统的安全政策、程序和保护机制中可改善的范围。科技发展一日千里，所以必须定期更新安全相关政策、程序和保护机制，以确保整体安全保护措施对信息系统的效用。在进行事故事后分析时，如有需要应覆检和修订政策、标准、指南和程序，以配合预防措施。

10.5 调查及检控

在适当的情况下，还应对引起事故的个人采取个案调查、纪律处分或法律检控等行动。

如经评估后，事故已构成刑事罪行，则应向香港警务处网络安全及科技罪案调查科报告，以便展开个案调查和收集证据。在向警方报告案件前，应事先征求信息安全事故应急小组高级管理层的意见和批准。决策局／部门可能需要跟进法律程序及提供所需证据。

如果安全事故涉及个人资料，则决策局／部门应尽快向个人资料私隐专员公署报告。决策局／部门也应尽可能通知受影响的人。如基于合理原因而不作出通报，应得到决策局／部门主管的批准方可。

另外，对于向警方或个人资料私隐专员公署报告的任何安全事故，亦应通知政府信息安全事故应急办事处常设办公室以进行中央记录和协调支持。

完

附件 A：部门信息技术安全联络人数据更新表

<table>
<tr><th colspan="2">决策局 / 部门名称</th></tr>
<tr><td colspan="2"></td></tr>
<tr><th colspan="2">人员职务</th></tr>
<tr><td colspan="2">☐ 部门信息技术安全主任
☐ 部门信息技术安全副主任
☐ 部门信息安全事故应急小组组长
☐ 部门信息安全事故应急小组副组长</td></tr>
<tr><td colspan="2">更换人员:_____ (请为每位人员另备独立表格)</td></tr>
<tr><th colspan="2">联络数据</th></tr>
<tr><td>姓名：</td><td>职位：</td></tr>
<tr><td>办公室联络号码：</td><td>流动电话号码：
（作 7x24 紧急联络之用）</td></tr>
<tr><td colspan="2">电邮地址：</td></tr>
<tr><td colspan="2">收取信息技术安全相关数据的其他电邮地址：</td></tr>
<tr><th colspan="2">递交人</th></tr>
<tr><td>部门信息技术安全主任 / 信息安全事故应急小组组长* 姓名：</td><td>职位：</td></tr>
<tr><td>部门信息技术安全主任 / 信息安全事故应急小组组长* 签署：</td><td>有效日期：</td></tr>
<tr><th colspan="2">送交政府资讯科技总监办公室信息技术安全小组</th></tr>
<tr><td colspan="2">请通过以下途径向信息技术安全小组递交已填妥的表格：
电邮： it_security@ogcio.gov.hk
传真号码：2989 6073</td></tr>
</table>

**删除不适用部分*

附件 B: 安全事故处理准备工作清单

B.1 安全事故处理准备工作列表样本

	项目	详情	进展情况
1	安全事故处理计划	为安全事故处理制订计划	
2	报告程序	设计及准备报告机制	
		向全体人员颁布报告机制	
3	升级处理程序	收集需要联络 / 参与工作的全体人员（内部和外部）的联络资料	
		准备升级处理程序	
		向参与工作的全体人员颁布升级处理程序	
4	安全事故应急程序	准备安全事故应急程序	
		向参与工作的全体人员颁布安全事故应急程序	
5	培训与教育	向操作及支持人员提供有关安全事故处理的培训	
		确保各人员熟习事故应急程序	
6	事故监察措施	安装防火墙设备和访问控制措施，以保护重要的系统和数据资源	
		安装恶意软件侦测及修复软件，定期进行扫描并更新标识符	
		安装监察工具，例如入侵检测系统	
		开启系统及网络设备的审计记录功能	

附件 C: 报告机制

C.1 报告机制建议

电话热线

这是最便利和快捷的报告事故途径。部分系统可能已设有专门处理查询及/或安全事故报告的电话热线。

如果系统需要日夜不停运作，便可能需要提供 24 小时电话热线服务。

电子邮件

通过电邮报告事故也是个有效的途径。然而，如果发生属于网络攻击或针对电邮系统的事故，以电邮报告的途径便会受到影响。要解决这个问题，应采用其他的报告途径，例如电话或传真。

传真号码

通过传真报告是一个补充机制，特别是当要提交可能无法通过电话清楚及准确地报告的详细信息。但是，透过传真机报告事故应特别注意，最好由专人负责接收传真。 此外，还应特别注意处理传真报告，以防止向未经授权的人员披露事故。鉴于通过传真报告的须留意这些额外的安全措施，为了更有效率和更具成本效益，通常会使用电子邮件来提交报告。

亲身报告

这个办法被认为没有效率，而且还会构成不便。这只应用于，必须亲身由报告事故的人员提供详细资料或与报告事故的人员讨论事故的情况，又或者事故地点与事故报告联络人的所在地十分接近，否则应避免采取亲身报告的方式。

C.2 信息安全事故初步报告

限 阅

事故参考编号：_____
（只供政府信息安全事故应急办事处常设办公室填写）

信息安全事故初步报告

背景资料	
决策局 / 部门名称：	
概述受影响的系统（例如功能、网址等）：	
受影响系统的实体位置： ☐决策局 / 部门内部 ☐ 外聘服务供货商设施 ☐中央服务：_____ **系统管理员 / 操作员：** ☐ 内部人员 ☐ 终端用户 ☐ 外包服务供货商	
报告人资料	
姓名：	***职位：***
办公室联络号码：	***24 小时联络号码：***
电邮地址：	***报告日期：***
事故详情	
发生事故的日期 / 时间：	
发现事故的日期 / 时间：	**向政府信息安全事故应急办事处常设办公室报告的日期 / 时间：**
事故说明： ***发生事情*:** _____	

初步调查结果（如有）：

发生经过：

_____

发生原因：

_____

已识别漏洞：

_____

类别：

☐ 滥用信息系统
☐ 入侵信息系统或数据资产
☐ 拒绝服务攻击
☐ 泄漏电子保密数据
☐ 伪冒
☐ 遗失存有保密数据的流动装置或抽取式媒体
☐ 大规模恶意软件感染
☐ 勒索软件
☐ 网站遭涂改
☐ 其他：_____

受影响组件 / 资产：

☐ 电邮系统
☐ 硬件
☐ 数据 / 数据
☐ 网络
☐ 软件
☐ 网站
☐ 其他：_____

受影响组件 / 资产详情：

_____

影响：

☐ 机密性
☐ 完整性
☐ 可用性
☐ 政府形象
☐ 其他_____

请提供有关影响和中断服务时间（如有）的详情：

_____

事故有否涉及保密资料？

☐ 有，涉及 ☐限阅类别 ☐机密类别

☐ 没有

请提供所涉及保密数据的详情（例如数据是否加密、数据类型等）：

_____

事故有否涉及个人资料？

☐ 有，所涉及个人资料为：_____

☐ 没有

已通知人士 / 单位：

☐ 信息系统经理 ☐ 新闻统筹员

☐ 事故应急经理 ☐ 信息安全事故应急小组组长

☐ 政府信息安全事故应急办事处常设办公室 ☐ 其他：_____

已通知外部人士 / 单位（日期 / 时间）：

☐ 香港警务处网络安全及科技罪案调查科：_____
档案参考编号：_____

☐ 个人资料私隐专员公署：_____

☐ 其他：_____

为解决事故所采取的行动：

为解决事故所计划的行动：

未进行的行动：

目前系统的状况：

其他数据：

媒体 / 公众查询 （如适用）

媒体查询数目：	**公众查询数目：**

C.3.1 事故中期报告

限 阅

事故参考编号：_____

（只供政府信息安全事故应急办事处常设办公室填写）

事故中期报告

背景资料	
决策局 / 部门名称：	
概述受影响的系统（例如功能、网址等）：	
受影响系统的实体位置： ☐ 决策局 / 部门内部　☐ 外聘服务供货商设施 ☐ 中央服务：_____ **系统管理员 / 操作员：** ☐ 内部人员　☐ 终端用户　☐ 外包服务供货商	
报告人资料	
姓名：	***职位：***
办公室联络号码：	***24 小时联络号码：***
电邮地址：	***报告日期：***
事故详情	
发生事故的日期 / 时间：	
发现事故的日期 / 时间：	**向政府信息安全事故应急办事处常设办公室报告的日期 / 时间：**
事故说明： ***发生事情***： _____	

调查结果：

发生经过：

_____

发生原因：

_____

已识别漏洞：

_____

最新状况：

C.3.2 事故事后报告

限 阅

事故参考编号：_____

（只供政府信息安全事故应急办事处常设办公室填写）

事故事后报告

背景资料	
决策局 / 部门名称：	
概述受影响的系统（例如功能、网址等）：	
受影响系统的位置： ☐ 决策局 / 部门内部 ☐ 外聘服务供货商设施 ☐中央服务：_____ **系统管理员 / 操作员：** ☐ 内部人员 ☐ 终端用户 ☐ 外包服务供货商	
报告人资料	
姓名：	***职位：***
办公室联络号码：	***24 小时联络号码：***
电邮地址：	***报告日期：***
事故详情	
发生事故的日期 / 时间：	
发现事故的日期 / 时间：	**向政府信息安全事故应急办事处常设办公室报告的日期 / 时间：**
事故说明： ***发生事情***： _____	

调查结果：

发生经过：

_____

发生原因：

_____

已识别漏洞：

_____

类别：

☐ 滥用信息系统
☐ 入侵信息系统或数据资产
☐ 拒绝服务攻击
☐ 泄漏电子保密数据
☐ 伪冒
☐ 遗失存有保密数据的流动装置或抽取式媒体
☐ 大规模恶意软件感染
☐ 勒索软件
☐ 网站遭涂改
☐ 其他：_____

受影响组件 / 资产：

☐ 电邮系统
☐ 硬件
☐ 数据 / 数据
☐ 网络
☐ 软件
☐ 网站
☐ 其他：_____

受影响组件 / 资产详情：

_____

其他受影响场地 / 系统（如有）：

_____

影响：

☐ 机密性　　☐ 完整性

☐ 可用性　　☐ 政府形像

☐ 其他_____

请提供有关影响和中断服务时间（如有）的详情：

_____

已通知人士 / 单位：

☐ 信息系统经理　　☐ 新闻统筹员

☐ 事故应急经理　　☐ 信息安全事故应急小组组长

☐ 政府信息安全事故应急办事处常设办公室　　☐ 其他：_____

已通知外部人士 / 单位（日期 / 时间）：

☐ 香港警务处网络安全及科技罪案调查科：_____
档案参考编号：_____

☐ 个人资料私隐专员公署：_____

☐ 其他：_____

香港警务处调查结果（如有）：

-_____
_
-_____
_

事件发生的次序：

日期 / 时间	*事件*

已采取的行动及结果：

目前系统的状况：

参与人员：

姓名	*职位*	*电话号码*	*电邮地址*	*职务*

肇事者（如有）详情：

涉及的肇事者：

☐ 人　　☐ 组织

☐ 没有肇事者　　☐ 不明

☐ 其他：_____

事故的怀疑动机：

☐ 经济利益　　☐ 黑客攻击

☐ 政治　　☐ 报复

☐ 不明　　☐ 其他：_____

恶意软件（如有）详情：

如事故涉及保密资料，请提供详情（例如数据是否加密、数据类型等）：

保密资料：　☐限阅类别　☐机密类别

备注：

_____

_____

如事故涉及个人资料，请提供详情（例如：受影响人数、个人资料类别（如香港身份证号码）、是否已通知受影响人士等）：

受影响人数：_____

（*内部人员和市民人数分项数字*）

个人资料类别：

_____

是否已通知受影响人士：是／否。 如否，原因： _____ 备注： _____
成本因素（包括因事故招致的损失和复原成本 / 人力资源）：
防止再度发生事故的建议行动：
汲取的教训：

媒体 / 公众查询 （如适用）	
媒体查询数目：	**公众查询数目：**

附件 D: 升级处理程序

D.1 需要通知的各方

升级处理程序内需要包括哪些人员，取决于事故的性质和严重程度，及系统要求。举例来说，发生事故的初期可能只需要内部支持人员处理问题。其后可能需要通知高级管理层。如果问题仍无法解决，便可能需要视乎情况，寻求服务承包商、产品供货商、警方及个人资料私隐专员公署等外部支持服务机构的意见。

应为各系统设定个别的升级处理程序和联络人，以满足系统的特殊操作需要。

视乎系统受到的破坏或系统的敏感程度，在不同的阶段可通知不同的人员。联络人包括，但不限于：

内部：

- 操作及技术支持人员
- 相关信息系统的经理、信息安全事故应急小组及政府信息安全事故应急办事处常设办公室
- 其他受影响 / 有关联的系统或功能操作人员
- 香港警务处网络安全及科技罪案调查科
- 新闻统筹员，为准备对事故的立场和向传媒发布的新闻稿

外部：

- 支持服务供货商，包括系统的硬件或软件供货商、应用程序开发商和安全顾问等
- 服务供货商（例如电讯供货商、互联网服务供货商）
- 个人资料私隐专员公署
- 受影响人士

D.2 联络名单

参与工作人员的联络名单应包括下列资料：

- 专责人员的姓名
- 职衔
- 电邮地址
- 联络电话号码（按需要加入 24 小时联络号码）
- 传真号码

D.3 升级处理程序示例

以下所列是信息安全事故的升级处理程序示例。

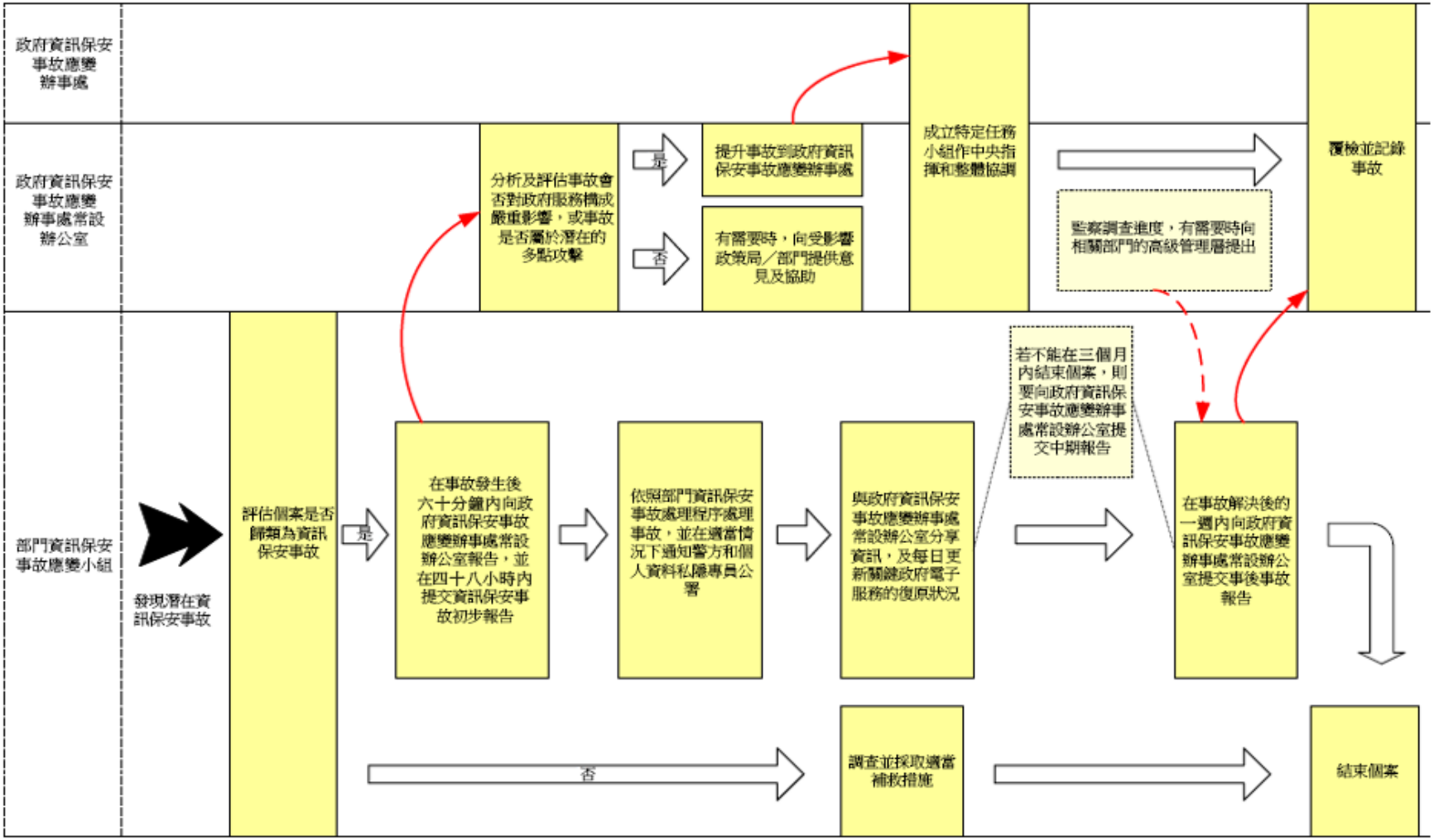
报告时限	**联络名单**	**联络方法**
事故发生后 15 分钟内	有关的信息系统经理、技术支持人员、提供支持的相关供货商和服务承包商	*流动电话及供货商 24 小时电话热线*
事故发生后 30 分钟内	上述各人员及信息安全事故应急小组的事故应急经理和新闻统筹员	*流动电话*
事故发生后 60 分钟内	通知信息安全事故应急小组组长	*流动电话*
事故发生后 60 分钟内	信息安全事故应急小组通知政府信息安全事故应急办事处 (及于事故发生后 48 小时内向政府信息安全事故应急办事处常设办公室提供信息安全事故初步报告)	*默认的电话热线或电子邮件*
其后每 30 分钟	向上述各人员汇报最新情况	*流动电话或电子邮件*
定期	信息安全事故应急小组向政府信息安全事故应急办事处汇报事故的最新情况	*电子邮件*
系统复原后（1 星期内）	信息安全事故应急小组向政府信息安全事故应急办事处递交一份事故事后报告作记录	*电子邮件*
如怀疑构成刑事犯罪，则由信息安全事故应急小组决定	向警方举报以调查案件	*默认的电话热线*
如涉及个人资料	向个人资料私隐专员报告 （并尽可能通知受影响人士）	*默认的电话热线或任何其他途径*

报告应包括下列资料：

- 概括描述问题：发生何事、何时发生、如何发生及持续时间
- 表明系统是否受到攻击
- 表明攻击者（如有）是否仍在系统进行活动
- 表明攻击是否来自本地
- 系统复原的最新进展情况

附件 E: 信息安全事故应急机制的流程

下图所示为政府安全事故报告及升级处理工作流程图：



附件 F: 确认事故

F.1 安全事故的典型迹象

为判断异常情况是由系统问题所造成，还是确实已发生事故，可留意安全事故一些特定迹象。安全事故的常见迹象包括下列任何或全部迹象：

与系统操作相关的迹象：

- 入侵检测、抗恶意软件或恶意软件侦测工具所发出的系统警报或类似讯息
- 可疑的系统或网络帐户（例如用户没有经过正常程序而取得根访问权限）
- 帐户资料错漏
- 部分或全部系统记录遗失或遭窜改
- 系统崩溃
- 系统性能突然大幅下降
- 未获授权下执行程序
- 可疑的试探，例如多次的登入失败
- 可疑的浏览活动，例如拥有根权限的帐户访问不同用户帐户的多个档案
- 系统时间出现预计以外的大幅偏差
- 网络通讯量出现异常偏差

与用户帐户相关的迹象：

- 预计以外的用户帐户之建立或删除
- 以往使用频率低的帐户突频繁使用
- 因账户遭窜改而无法登入
- 预计以外的用户密码更换
- 异常使用时间
- 对上一次登入或使用用户帐户的情况可疑
- 异常使用模式（例如没有参与程序编制的用户帐户在编制程序）
- 计算机系统显示奇怪的讯息
- 在无法解释的情况下，不能访问计算机系统
- 大量载有可疑内容的回弹电邮
- 用户报告收到恐吓电邮讯息

与档案及数据相关的迹象：

- 预计以外的档案或数据之建立、窜改或删除
- 陌生的文件名
- 预计以外的窜改档案大小或数据，尤其是系统的可执行文件案
- 预计以外的尝试写入系统档案，或修改系统档案
- 无法访问档案和数据
- 在公开地方（例如打印机出纸口）发现无人看管的敏感资料

然而，单凭一种迹象未必可确定是否有事故发生。拥有丰富安全和技术知识的技术人员应参与判断，以根据上述的一种或多种迹象确认事故。此外，在确认事故时，多人集思广益作出的判断往往优胜于一人作出的判断。

F.2 为确认事故收集的资料

在确认事故时还应查阅下列数据：

- 系统记录、防火墙 / 路由器记录、服务器记录和入侵检测系统记录等审计追踪或记录档案
- 仍在进行活动的网络连接及系统程序状态数据
- 有助调查人员更好地了解系统功能、网络基本设施及对外连接情况的任何其他文件

F.3 事故类别

所有信息安全事故都应予报告，下表列载一些安全事故的类别及其描述：

信息安全事故	描述
滥用信息系统	当有人利用信息系统作非获准用途，例如为信息资产带来负面影响，即已构成滥用。
入侵信息系统或数据资产	在未得到系统拥有人批准的情况下，实体或逻辑访问整个或部分信息系统及／或其数据。入侵可以经由不可信源头的手动或透过自动化技术造成。
拒绝服务攻击	蓄意或无意地妨碍使用信息资源，以影响信息资源的可用性。拒绝服务攻击的例子包括 SYN 泛滥、致命小包和 Ping 泛滥，这些攻击尝试使信息系统或网络连接超出负荷，而无法向其用户提供正常的服务。
泄漏电子保密数据	保密资料外泄，或被未获授权人士访问。
遗失存有保密数据的流动装置或抽取式媒体	流动装置／抽取式媒体因意外或失窃而遗失。
伪冒	使用他人身份，以取得超出本身原有的信息系统访问权限。
大规模恶意软件感染	恶意软件感染可以损毁档案、删改数据、加密档案、秘密偷取数据、关闭硬件或软件运作，或拒绝合法用户访问等。决策局／部门须识别及评估是否对业务运作有严重影响。
勒索软件	勒索软件是一种通过加密以阻止和限制用户访问其系统或档案并要求付款解密的恶意软件。
网站遭涂改	未获授权窜改互联网网页的内容。

F.4 影响事故范围和后果的因素

影响事故范围和后果的因素包括：

- 事故的影响程度：影响单一系统还是多个系统
- 对公共服务及 / 或政府形象可能造成的影响
- 新闻媒体的介入
- 涉及犯罪活动
- 事故的潜在影响
- 是否涉及保密资料
- 事故的进入点，例如网络、互联网、电话线、局部终端机等
- 攻击来自本地的可能性
- 预计事故后复原所需的时间
- 处理事故所需的资源，包括人员、时间和设备
- 造成进一步破坏的可能性