数字政策办公室

信息安全

信息安全事故处理

实务指南

[ISPG-SM02]

第 1.8 版

2025 年 2 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
4	如发现有迹象显示可能发生信息安全事故，政府部门可咨询政府信息安全事故应急办事处常设办公室的建议。	第 20 页、26 页、附件 F	1.3	2022 年 9 月
5	更新个人资料私隐专员公署的《资料外泄事故通报表格》的超连结，以及修改报告机制的表格。	第 28 页、附件 C	1.4	2023 年 6 月
6	基于最新的《资讯科技保安指引》(G3) v10.0 而作出的修改	整份文件	1.5	2024 年 4 月
7	将「政府资讯科技总监办公室」修改为「数字政策办公室」 将「香港电脑保安事故协调中心」修改为「香港网络安全事故协调中心」		1.6	2024 年 7 月
8	增加信息安全事故报告的新要求。修改报告机制表格。	第 22 页、附件 C、 D 和 E	1.7	2024 年 8 月
9	修改部门信息技术安全联络人信息更新表和报告机制表格。	附件 A 和 C	1.8	2025 年 2 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应变计划。

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 (fifth edition), ISO/IEC 27000:2018
- Information technology - Security techniques - Information security management systems - Requirements (third edition), ISO/IEC 27001:2022
- Information technology - Security techniques - Code of practice for information security controls (third edition), ISO/IEC 27002:2022
- Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management (second edition), ISO/IEC 27035‑1:2023
- Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response (second edition), ISO/IEC 27035-2:2023

- NIST SP 800-61 – Computer Security Incident Handling Guide

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	
中央处理单元	中央处理单元是计算机的主要组件，充当计算机的「控制中心」。中央处理单元也称为「中央」或「主」处理器，是一组复杂的电子电路，用于运行机器的操作系统和应用程序。
主机入侵检测系统	入侵检测系统是一种监察网络流量是否存在可疑活动并在发现此类活动时发出警报的系统。
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。
入侵指标	入侵指标充当主机系统或网络潜在入侵的鉴证证据。
随机存取存储器	随机存取存储器是一种计算机存储器，可以按任何顺序搜索并根据需要进行更改。
复原点目标	复原点目标定义为从灾难、故障或类似事件中恢复后，在数据丢失超出组织可接受范围之前可能丢失的最大数据量（按时间衡量）。
复原时间目标	复原时间目标是应用系统、计算机、网络或系统在发生意外灾难、故障或类似事件后可以停机的最长可接受时间。
SYN 泛滥	SYN 泛滥（半开放攻击）是一种分布式拒绝服务攻击，其目的是通过消耗所有可用的服务器资源来使服务器无法用于合法流量。

1.4 联络方法

1.4.1 一般联络

本文件由数字政策办公室编制及备存。如有任何意见或建议，请寄往：

电邮：	it_security@digitalpolicy.gov.hk
Lotus Notes 电邮：	IT Security Team/DPO/HKSARG@DPO
CMMP 电邮：	IT Security Team/DPO

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 / 部门亦须制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 / 部门可以利用威胁情报网络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和一般安全信息（例如网络安全信息站、信息安全网）的专题网页来提高安全意识。

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，信息安全事故应变计划应预先准备，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：

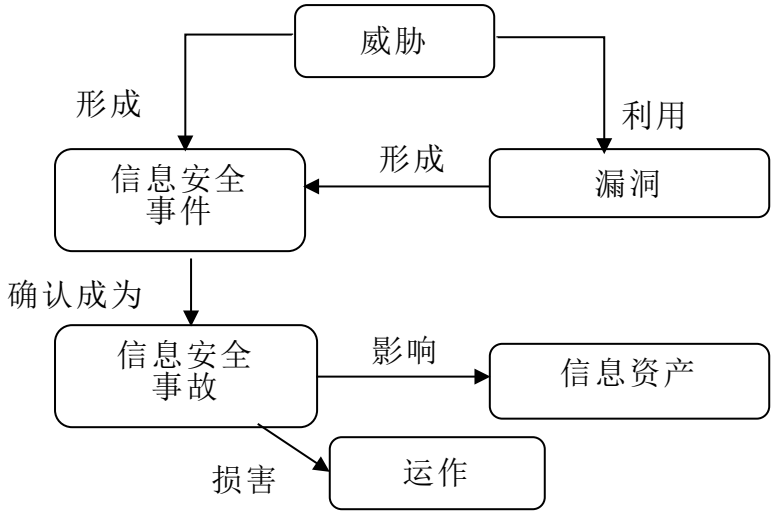


图 3.1 安全事件及安全事故的关系

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

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应变计划，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。

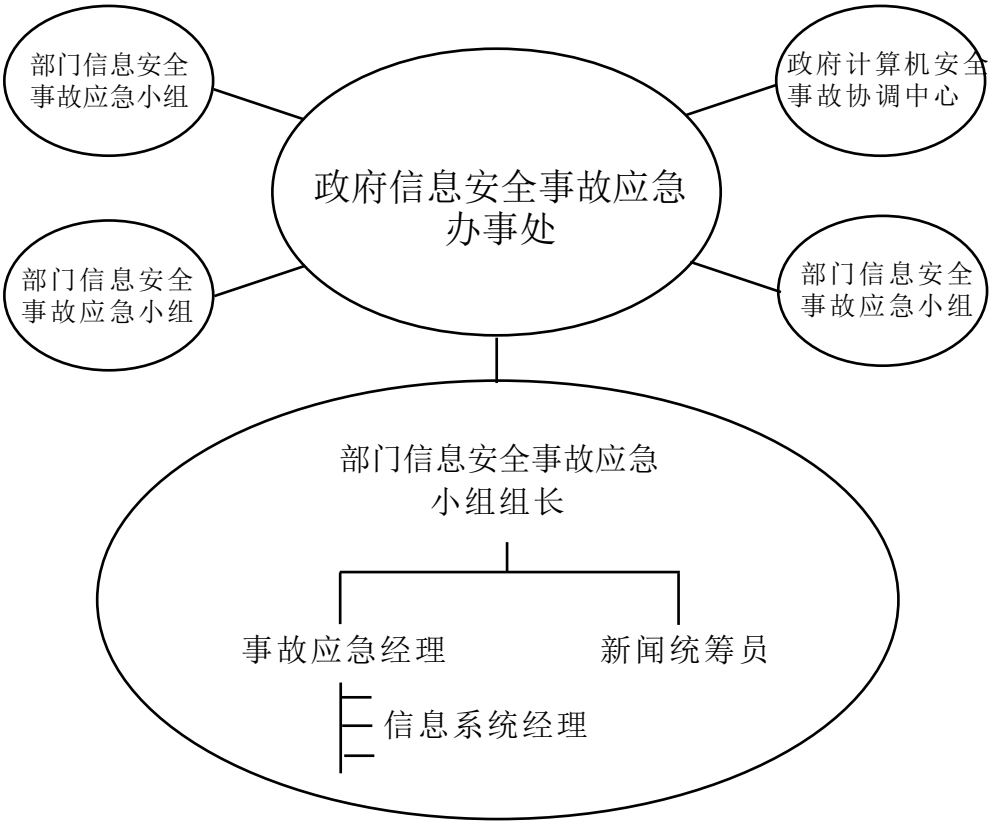


图 4.1 参与安全事故处理的各方

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：

- 数字政策办公室
- 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应变计划，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。决策局 / 部门应定期评估团队的工作量并相应地分配资源，以避免出现瓶颈和延误。

下文将详述信息安全事故应急小组内各角色的职责。

4.3.3 信息安全事故应急小组成员的职责

(a) 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。

(b) 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。

(c) 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。

(d) 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网络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。

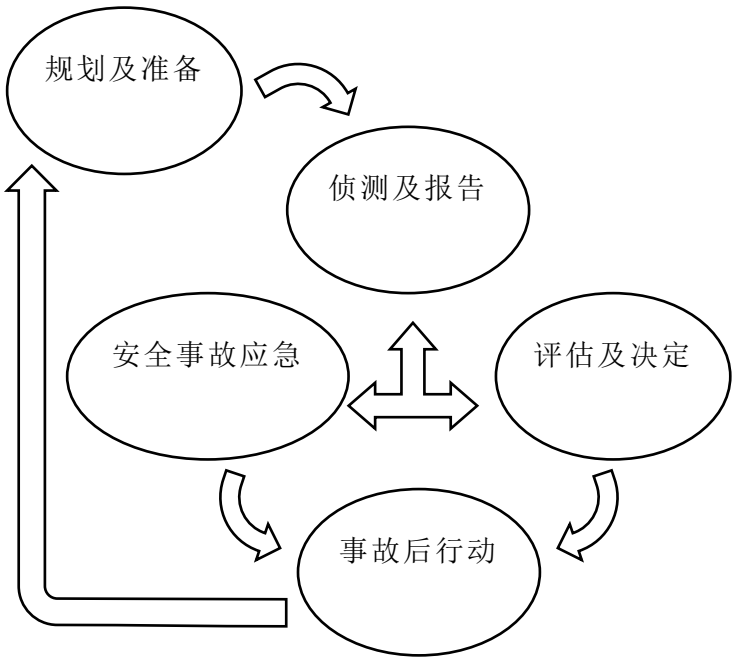


图 5.1 安全事故处理的循环过程

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。本步骤中规划和准备所涉及的主要活动如下。

- 规划事故监察和侦测
- 规划安全事故应变
- 规划培训与教育

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：

- 规划事故监察和侦测
- 规划安全事故应变
- 规划培训与教育

安全事故应变准备工作清单列于**附件 B**，以供参考。

6.1 规划事故监察和侦测

须推行足够程度的事故监察安全措施，以便在系统正常操作期间保护系统，同时监察潜在的安全事故。所采取措施的程度和范围取决于系统、系统数据及系统功能的重要性和敏感度。

下列是一些常用的安全事故监察措施：

- 安装防火墙设备，并采取认证和访问控制措施，以保护重要系统和数据资源。
- 安装入侵侦测工具，主动监察、侦测并就系统入侵或黑客活动作出应变。
- 安装抗恶意软件工具和恶意软件侦测及修复工具，以侦测及清除恶意软件，并防止恶意软件影响系统操作。
- 利用安全扫描工具定期进行安全检查，以找出现有的安全漏洞，并进行既定安全政策与实际安全安排之间的差距分析。
- 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的活动。
- 开发程序和指令码协助侦测可疑活动、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、警报、漏洞信息、报告和其他信息安全出版物，对新兴的安全威胁和相关风险保持警觉。

- 备存并记录漏洞管理机制，以识别、评估和减低安全风险。
- 将威胁情报源和数据应用到监察流程中。威胁情报集成与应用请参考《信息技术安全威胁管理实务指南》。

6.2 规划安全事故应变

决策局 / 部门须委任两名指定人士作为事故处理的 7x24 联络点，以确保持续可用及可即时响应安全事故。这些人员必须全天候（包括周末和节假日）随时可联系，并准备好参与事故处理活动。

对这些接触点的期望包括：

- 指定的联络点必须随时待命，以接听和响应有关信息技术安全问题的紧急电话，即使是在非工作时间。这对于促进即时沟通和快速事故处理、有效减少安全事故造成的潜在损害和损失至关重要。
- 指定联系人应迅速确认收到的任何通信并立即采取行动，确保事故应变过程不会出现延误。
- 指定联系人必须能够直接处理安全事故，或者有权限和能力将紧急安全信息及时转发给负责人员。
- 决策局 / 部门应定期核实指定人士的联系方式，以确保他们的联系方式是最新的，并且在有需要时可以无障碍地立即联系他们。

须制订及记录安全事故应变计划。安全事故应变计划须至少包括以下内容：

- 事故应变小组的结构以及相应的角色和职责；
- 报告程序；
- 缓解事故影响、保留证据、调查事件原因和影响的程序；
- 复原计划；
- 与利益相关者和公众的沟通计划；和
  事故后的覆检程序。

安全事故应变计划须至少每两年定期检讨一次，或当决策局 / 部门的运作环境有任何重大改变时进行。决策局 / 部门须确保所有相关人员熟悉该计划，并且全体人员（包括管理层人员）均应知悉该计划，以作为参考和遵行有关要求。这套计划应清晰直接而且容易理解，让全体人员清楚了解他们需采取的行动。决策局 / 部门应在事故应变计划中纳入不同的场景及相应的应变程序。事故应变计划须定期进行测试和更新，以确保可迅速及有效地就信息安全事故作出应变。此外，决策局 / 部门须至少每两年进行一次演习，最好每年进行一次，以评估计划的有效性。事件应变小组成员须参加演练，以熟习自己在事故应变计划中的角色，确保快速和有效地应变安全事件。

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)。

6.2.1 事故应变小组的结构以及相应的角色和职责

事故应变小组的结构和参与安全事故处理工作各方的角色和职责应明确制定。上述第 4 章为制定安全事故应急小组主要成员的职务和职责提供了参考的模型。

6.2.2 报告程序

(a) 报告

须建立及记录一套报告程序，清楚制定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，当政府部门发现有迹象显示可能发生信息安全事故，可咨询政府信息安全事故应急办事处常设办公室的建

议。**附件 F** 第 1 节载列了此类事故的常见迹象。

通过向政府信息安全事故应急办事处寻求意见，决策局 / 部门可以主动识别和解决系统异常情况，确保及早发现整个政府的信息技术安全威胁和事件。这种协作方法可以维护整体安全并创造一个具复原能力和安全的环境，从而使政府受益。

当知悉发生信息安全事故时，部门信息安全事故应急小组须：

- 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（见**附件 C** 第 2 节）；
- 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。

根据总务通告第 6/2024 号「加强资讯科技系统的管治和保安」，若决策局 / 部门的政府信息技术系统发生信息技术安全事故，而有关局长认为事故已令政府尴尬或损害其监督角色的形象，有关的项目负责人员(就「指定资讯科技系统」)或部门信息技术安全主任(就决策局 / 部门的所有其他信息技术系统)须在事故发生后两个历日内向其局长提交信息技术安全事故初步报告，然后在七个历日内提交信息技术安全事故全面报告。载有建议跟进工作并经相关局长批核的事故全面报告须提交予数字办，以作记录、监察和视乎情况给予技术意见。决策局 / 部门应参阅总务通告第 6/2024 号及其专题网站(https://sgsits.host.ccgo.hksarg)以了解更多有关提交和汇报政府信息技术安全事故报告的详情。

决策局 / 部门被视为「知悉」事故的成立基准是，当合理程度上确定信息安全事件已对政府信息系统或数据资产的机密性、完整性或可用性造成了损害，或已对决策局 / 部门的运作造成损害。这种意识通常在对情况进行初步评估之后建立，这可能需要一些时间才能彻底进行。

对事故的知悉可能在多种情况下产生。例如：

- 如果检测到不寻常的系统行为，例如非预期的的数据导出或不寻常的登录模式，并且经调查发现这些行为与未获授权的访问或数据泄露有关，决策局 / 部门将被视为对事故「知悉」。
- 如果决策局 / 部门从外部实体收到可靠信息，表明未获授权的披露，则该确认将构成对事故的「知悉」。
- 如果发生勒索软件攻击，决策局 / 部门发现攻击者的加密文件和勒索字条，一旦该攻击得到内部验证，决策局 / 部门将被视为对事故「知悉」。

对事故的知悉不一定是最初发现异常时，而是在初步调查确认安全事故确实发生后。事故的具体细节将影响确认事件的时间线。

决策局 / 部门在发现或收到潜在事故通知后立即作出应变，启动初步调查以确定事故是否确实发生，这一点至关重要。这个初始阶段是关键的，不应被误认为是对事故的「知悉」阶段。只有当调查以合理的确定性证实该事故时，决策局/部门才正式「知悉」。

然而，重点仍应是迅速采取行动调查安全事件，如果得到证实，则采取修正措施并进行相应报告。及早报告可疑安全事故可以为保护整体安全和营造一个完善和安全的环境作出贡献，从而使政府受益匪浅。值得注意的是，在初步报告后，如后续调查显示怀疑的安全事故并未发生，决策局 / 部门须向数字政策办公室通报情况。

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须根据以下规定，就最新的修复情况及调查进度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：

- 于首次报告事故后 14 日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。

附件 C 第 3.1 节载有报告样本报告以供参考。

(b) 升级处理

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。

6.2.3 应变程序

视乎不同系统和管理需要，事故处理程序宜包括：

- 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
- 避免进一步发生事故
- 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

6.2.4 复原计划

有效的复原计划对于安全事故后将系统恢复正常操作至关重要。复原计划应该全面、有据可查，并包括确保恢复后系统安全性和完整性的步骤。

复原计划应包括：

- 评估损害和识别受影响服务的程序。
- 复原系统和恢复服务的缓急次序。
- 安全地重新安装损坏或受入侵组件的步骤。
- 确保系统恢复到正常状态的验证过程。
- 用于通知相关方复原状态的通信规约。

复原过程应包括以下步骤：

- 进行彻底的损害评估，以确定事故的范围和影响。
- 确定功能和服务的恢复顺序，优先考虑必需服务和影响大多数用户的服务。
- 从可信赖来源重新安装损坏或删除的文件，确保软件的完整性和安全性。
- 从最关键的服务开始，以受控方式恢复功能/服务。
- 确认系统已恢复至正常操作且没有留下安全事故的痕迹。
- 通报所有相关方系统恢复操作的情况，确保操作员、管理员和高级管理人员了解当前状态。
- 关闭所有不必要的服务，以最大程度地减少系统的攻击面。
- 记录复原过程中采取的所有操作。

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。

6.2.5 沟通计划

应建立与利益相关者和公众的沟通程序。沟通对于控制围绕事故的信息至关重要，包括传递信息的地点、时间、内容和方式。有效应变和恢复需要内部沟通，维护政府形象也离不开外部沟通。有关事故的不受控制的沟通可能会产生严重后果。只有经过适当授权和准备的人员才可以在最佳时机以适当的形式代表决策局/部门进行沟通，告知必要的信息。

有效的沟通计划应先确定事件期间需要通知的关键受众。这些通常包括内部利益相关者（例如使用者、管理层和事故应变团队）和外部利益相关者（例如民众、合作伙伴、监管机构和媒体）。对于每个受众，计划应指定具体的信息、沟通渠道以及提供更新的频率。

该计划应详细说明通信基础设施，包括主要和备用通信方法，以确保信息流不间断。这可能涉及电子邮件、内部公告、新闻稿、社交媒体和新闻发布会。基础设施必须足够完善以能够应对危机期间增加的通信量。

沟通计划中必须明确定义角色和职责。这包括任命接受过危机沟通训练的一名发言人或一队发言人团队，向公众和媒体传递信息。还应该有信息的批准和传播的规约，以确保一致性和准确性。

该计划还应包括针对各种场景而预先起草的模板，以加快沟通速度。这些模板可以快速调整以适应事故的具体细节，确保快速应变。

沟通计划必须灵活并就适应事件不断变化的事故性质而调整。它应该包括一个回馈循环来评估沟通的有效性并作出必要的调整。事故解决后，覆检沟通流程对于确定哪些内容有效以及哪些内容可以为针对未来事故进行改进至关重要。此覆检过程确保沟通计划是一个根据过去的经验不断发展的动态文件。

6.2.6 事故后的覆检程序

事故后覆检是安全事故应变计划的重要组成部分。它彻底分析了事故、其应变和复原步骤。事故后覆检程序应有条理并记录在案，纳入吸取的经验教训，以改善未来的应变和预防措施。覆检应评估安全事故的处理，识别成功和失败之处，并详细说明提高未来事故应变能力的行动。覆检应包括：

- 事故的初步发现和报告。
- 应变和遏制策略的有效性。
- 执行沟通计划执行的准确性和效率。
- 复原计划的充分性及其执行情况。
- 恢复正常操作和服务。
- 证据保存过程及其在分析中的作用。

覆检程序的结构应如下：

- 覆检应在恢复阶段后和恢复正常操作后启动。
- 应收集和覆检与事故相关的所有文件和日志，以重建时间表和采取的行动。
- 根据既定指标评估应变绩效，并识别与应变计划的任何偏差。
- 与事故应变团队、管理层和其他相关利益相关者召开会议，讨论事故并收集反馈。
- 准备一份综合报告，其中包括：
    - 事故及其影响的摘要。
    - 应对措施的优点和缺点。

- 未来改进的建议。
- 解决已发现的弱点的可行步骤。

- 应召开会议讨论报告结果，确保所有利益相关者了解结果和必要的改进。

事故应变小组须负责以下事项：

- 追踪覆检期间确定的改进的实施情况。
- 根据需要更新政策、程序和应变计划。
- 开展培训和提高意识课程，以弥补已发现的差距。
- 重新评估指标并进行调整，以更好地衡量未来的事故应变。

应保留所有事故后覆检的记录，以便为未来的事故应变和合规要求提供信息。这些记录应该是安全并且只有获授权人员才能访问。事故后覆检过程应该是迭代的，每个事故都为安全事故应变计划的持续改进提供见解。

6.3 规划培训与教育

决策局 / 部门须确保全体员工均遵守及遵从相应的信息系统安全事故应变计划。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。决策局 / 部门亦须参加数字政策办公室指定的安全演习。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。

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（例如威胁情报平台、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：

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

要决定是否已发生事故，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。当政府部门发现有迹象显示可能发生信息安全事故，如有需要，可咨询政府信息安全事故应急办事处常设办公室的建议。**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，以便作出有效的应变。此初步分析流程对于了解事故和制定适当的相应措施起着至关重要的作用。通过实施结构化的初步分析流程，我们可以确保对事故进行彻底评估，并及时采取必要的预防措施和防御措施。应利用标准化的检查表作为收集事故详细信息和评估关键因素的指南，以辅助此流程。

在通知适当的有关各方并将事件升级到适当的级别时，检查表应与升级处理流程无缝整合。在描述升级处理过程中的事故时，建议包含以下信息：

A. ***事故详细信息：***记录事故的日期和时间，以及简短的摘要描述。此信息将提供事故时间线和性质的快照。

1. ***日期和时间：***记录事故发生或首次检测到的确切日期和时间。该时间戳将作为追踪事故进展和响应时间线的参考点。
2. ***事故摘要：***提供事故的简明描述。包括相关详细信息，例如事故的性质（例如安全漏洞、系统中断、数据丢失）、受影响的系统以及任何初步观察结果或症状。该摘要将帮助利益相关者快速掌握事故的背景并采取适当的应对行动。
3. ***事故分类：***根据预先定义的类别或严重级别对事故进行分类。常见的分类可能包括安全事故、技术故障、人为错误或自然灾害。对事故进行分类有助于确定响应工作的优先级并有效地分配资源。
4. ***事故来源：***确定事故的来源或起因（如果已知）。这可能是触发事故的特定事件、操作或外部因素。了解事故来源可以提供对潜在原因的宝贵见解，并有助于确定预防措施。
5. ***报告方：***注明报告该事故的个人或团队。如有必要，请附上他们的联

系信息，以便进一步沟通或澄清。此信息有助于与报告方建立直接沟通渠道，以获取更多事故详细信息或更新。

6. ***通知和升级：***记录有关事故的任何初始通知或升级。包括通知的个人或团队、使用的沟通渠道以及通知时间。此信息可以帮助确保正确启动事故应变流程并将其传达给相关利益相关者。

(i) 知情方：记录向哪些相关方通报了该事故，包括香港警务处、个人资料私隐专员公署和媒体（如果相关）。

(ii) 采取的行动：记录事故发生后立即采取的行动。这可能包括隔离受影响的系统、启动鉴证或启动危机管理团队。

B. ***系统信息：***包括有关受影响系统及其各自拥有者的详细信息。如果多个部门共同拥有一个系统，请注明所涉及的相关部门。了解拥有权对于有效的沟通和协作至关重要。

1. ***系统拥有者联系信息：***提供一个子字段来记录系统拥有者或受影响系统负责人的详细联系信息（姓名、电子邮件、电话）。这些信息将有助于事故应变期间的沟通和协调。

2. ***系统关键性：***系统关键性有助于确定与事件相关的影响程度和紧急程度。评估系统关键性时请考虑以下因素：

2.1. ***系统等级：***分配给每个受影响系统的指定系统等级。

2.2. ***业务影响：***评估受影响系统的丢失或降级对关键业务运营的影响。考虑创收、用户服务、规管遵行性和声誉等因素。

2.3. ***可用性要求：***根据业务和操作需求确定系统可用性的预期级别。考虑服务级别协议、正常运行时间要求以及系统在支持时间敏感流程中的角色等因素。

2.4. ***数据敏感性：***评估受影响系统处理、存储或传输的数据的敏感性和机密性。

2.5. ***复原时间目标：***复原时间目标表示事故发生后将系统恢复到全部功能的最大可容忍持续时间。它有助于优先考虑应变工作并有效分配资源。

2.6. ***复原点目标：***复原点目标表示恢复过程中可容忍丢失的最大数据量。它有助于建立备份和数据恢复策略，以最大限度地减少潜在的数据丢失。

3. ***系统描述：***提供受事故影响的系统的概述。包括系统 / 应用系统的用途、其主要功能以及其在支持业务流程中所扮演的角色等详细信息。此描述将有助利益相关者了解该应用系统的重要性及其与决策局 / 部门运作的相关性。

3.1. ***工作流程概述：***描述系统内的典型工作流程或流程。确定使用应用系统实现特定结果所涉及的关键步骤、操作或交互。此概述将提供对应用系统的使用方式及其关键路径的宏观理解。

3.2. ***受影响的功能：***确定受事故影响的系统的特定功能或特性。描述这些功能受到影响的程度以及它们不可用或降级的潜在后果。了解受影响的功能将有助于评估事故的严重性并确定应变行动的缓急次序。

3.3. ***系统依赖性：***识别并记录受影响的系统对其他系统 / 应用系统或服务的任何依赖性。这可以包括数据库、应用系统接口、网络连接或第三方集成。了解这些依赖性对于评估事故对互连系统的潜在影响至关重要。

3.4. ***与用户的交互：***描述用户如何与系统交互。这可以包括用户界面、输入机制或通信渠道。了解用户交互将有助于评估事故对用户体验、生产力和用户满意度的影响。

4. ***系统文档：***包含一个子字段来记录系统文档的可用性，例如用户手册或架构图。这些信息将协助事故应变团队全面了解系统的结构和功能。

4.1. ***用户手册：***记录与受影响系统相关的用户手册或指南的可用性。这些手册提供了有关系统设置、配置和操作的详细说明。请注意手册是否易于访问，以及它们是否涵盖了受事故影响的系统的相关方面。用户手册在手有助于事故应变团队了解系统的预期用途、其功能以及任何特定的配置要求。

4.2. ***架构图：***记录架构图的可用性以描述受影响系统的整体设计以及与其他系统或组件的集成。架构图提供了对系统模块、接口和依赖关系的深入了解。指出架构图是否可访问以及它们是否准确地表示了系统的当前状态。了解系统的架构有助于识别潜在的弱点，评估事故对系统功能的影响，并规划有效的应变。

4.3. ***备份和复原过程：***附加受影响系统的备份和复原过程。包括备份频率、存储位置以及最近备份的可用性等详细信息。此信息对于评估复原选项和规划恢复过程非常有价值。

4.4. ***其他相关文档：***考虑可能与受影响的系统相关的任何其他文档。这可能包括系统规格、配置指南、安全政策或任何其他提供系统结构、配置或安全控制见解的文档。请注意此类文档的可用性和可访问性。额外的文档可以增强事故应变团队对系统的理解，并有助于在整个调查和缓解过程中做出明智的决策。

5. ***系统配置：***包含一个子字段来记录受影响系统的配置详细信息，例如硬件规格、软件版本和已安装的修补程序。此信息将有助于了解系统的漏洞和潜在的受入侵领域。

5.1. ***硬件规格：***记录受影响系统的硬件规格。这包括处理器类型和速度、随机存取存储器数量、存储容量以及任何其他相关硬件组件等详细信息。了解硬件规格有助于评估系统的功能、性能以及对事故应变活动的潜在影响。

5.2. ***软件版本：***识别并记录受影响系统上安装的软件版本。这包括操作系统、应用系统、框架、库和任何其他软件组件。指定确切的版本号以提供准确的信息。了解软件版本有助于识别已知漏洞、安全补丁和潜在的危害区域。

5.3. ***已安装的修补程序：***记录受影响系统上已安装的修补程序和更新。这包括操作系统修补程序、应用系统更新、固件更新以及任何其他相关已应用的修补程序。指定修补程序名称、版本号和安装日期。了解修补程序状态有助于评估系统对已知漏洞的恢复能力，并确定是否有任何缺失的修补程序可能导致该事故。

5.4. ***配置更改：***记录最近对受影响系统所做的任何配置更改。这包括对防火墙规则、用户权限、网络设置的更改或任何其他相关配置修改。指定变更的性质、变更时间以及责任人。追踪配置更改有助于识别可能导致事故的潜在错误配置、未获授权的修改或政策违规。

6. ***网络图：***记录与事故相关的内部互联网规约地址，并提供与事故相关的网络拓扑。这将有助于识别潜在的攻击媒介并了解事故的范围。

6.1. ***网络拓扑概述：***提供与事故相关的网络拓扑的概述。这包括网络基础设施的布局和结构，包括路由器、交换机、防火墙和其他网络设备。描述不同组件如何互连以及网络的整体架构。

6.2. ***内部互联网规约地址***：记录与事故关联的内部互联网规约地址。这包括受影响的系统、服务器和网络设备的互联网规约地址。通过记下这些互联网规约地址，您可以识别事故中涉及的特定组件并追踪它们在网络内的连接。

6.3. ***子网信息：***识别与事故相关的子网或网段。这包括与每个子网关联的互联网规约地址范围以及任何相关的子网掩码。了解子网结构将有助于分析网络流量模式和潜在的漏洞区域。

6.4. ***网络设备配置：***记录事故涉及的网络设备的配置详细信息，例如路由器、交换机、防火墙和入侵检测系统。包括相关信息，例如设备型号、固件版本以及可能影响事故的任何特定配置或规则。

6.5. ***攻击媒介：***分析网络图以识别攻击者可能利用的潜在攻击媒介或路径。这包括检查系统之间的连接、访问控制机制以及网络基础设施中潜在的安全弱点。通过识别可能的攻击媒介，您可以评估事故的范围以及对网络的潜在影响。

6.6. ***事故范围：***根据网络图，评估事故影响的网段、系统和服务的范围。确定事故在网络内传播的程度，并识别可能面临风险的

任何关键资产或敏感区域。该评估将有助于确定应变行动和遏制工作的缓急次序。

C. ***入侵指标：***列出与事故相关的所有受影响的互联网规约地址、主机名称和用户名称。识别可疑文件或流程以及未获授权的访问或活动的任何证据。

1. ***受影响的互联网规约地址：***识别并列出已受影响或与事故相关的互联网规约地址。这包括与调查相关的内部和外部互联网规约地址。记录受影响的互联网规约地址有助于追踪网络流量的来源和目的地、识别潜在的攻击媒介以及了解事故的范围。
2. ***受影响的主机名称：***记录受事故影响的任何主机名称或域名。这可能包括受入侵的网站、未获授权的子域或异常的域名系统解析模式。列出受影响的主机名称可以深入了解潜在的威胁区域，并表明哪些系统或服务可能成为攻击目标。
3. ***受影响的用户名称：***识别在事故期间受到影响或泄露的任何用户名称或帐户。这包括与受影响的系统、应用系统或服务关联的用户帐户。记录受影响的用户名称有助于追踪未获授权的访问、识别潜在的内部威胁以及评估损害的程度。
4. ***可疑文件或流程：***记录调查期间发现的任何可疑文件或流程。这包括恶意软件、恶意脚本、未获授权的可执行文件或任何其他引起怀疑的文件或流程。提供详细信息，例如文件名称、文件位置和关联的流程名称（如适用）。识别可疑文件或流程有助于了解事故的性质、检测潜在的恶意软件感染并启动适当的应变操作。
5. ***未获授权的访问或活动的证据：***记录表明未获授权的访问或恶意活动的任何证据或指标。这可能包括日志条目、时间戳、异常网络流量模式或调查期间观察到的任何其他异常情况。撷取未获授权的访问或活动的证据有助于了解攻击者的技术、识别潜在的数据泄露并减轻进一步的风险。

D. ***备注：***在本节中，提供每个入侵指标的详细支持信息。解释为何将这些指标被认为是入侵并表明信赖度。此外，请注明与事故相关的任何其他观察结果或信息。

1. ***入侵指标详细信息：***对于每个已识别的入侵指标（互联网规约地址、主机名称、用户名称、可疑文件或进程、未获授权的访问或活动的证据），提供支持详细信息，解释为何它们被视为入侵。包括导致其被纳入指标的具体观察、行为或特性。这可以包括日志条目、网络使用分析、系统日志或调查期间收集的任何其他证据。
2. ***入侵理据：***解释将每个指标视为入侵的例句。描述与该指标相关的潜在影响或风险，以及它如何与已知的攻击模式、漏洞或恶意活动保持

一致。该理据将为将每个指标列为入侵指标提供背景和理由。

3. ***信赖度：***指示与每个入侵指标相关的信赖度。该范围可以从低到高，反映评估的确定性水平。考虑证据的质量、来源的可靠性以及调查人员的专业知识等因素。指定信赖度有助于确定应变行动的优先级并适当地分配资源。
4. ***其他观察结果：***记下任何其他与事故相关但可能不适合特定入侵指标的观察结果或信息。这可能包括异常的系统行为、漏洞评估的结果或任何其他可能有助于了解事故或其潜在影响的见解。这些额外的观察结果提供了宝贵的背景信息，有助于全面了解该事故。

在升级处理过程中提供的资料应明确简洁、准确而真实。决策局 / 部门必须保持系统信息/文件的持续可用性，以支持沟通的准确性和完整性。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。

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的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。

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。报告事故并不标志着信息安全事故应急小组职责的结束。信息安全事故应急小组预期将随时待命并积极参与。报告事故后立即遗下工作可能会导致事故应变流程出现延误或间隙，从而损害信息安全事故应急小组保护决策局/部门的能力。

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完成初步分析并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**）。

- 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，《资料外泄事故通报表格》可于个人资料私隐专员公署网站下载(https://www.pcpd.org.hk/tc_chi/resources_centre/publications/forms/files/DBN_c.pdf)。通报表格亦可以透过网上方式递交(https://www.pcpd.org.hk/sc_chi/enforcement/data_breach_notification/dbn_form.html) 。

此外，决策局／部门可参考个人资料私隐专员公署发出的《资料外泄事故的处理及通报指引》。

(https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidance_note_dbn_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，应在完成初步分析的同时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

须记录所有安全事故、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。

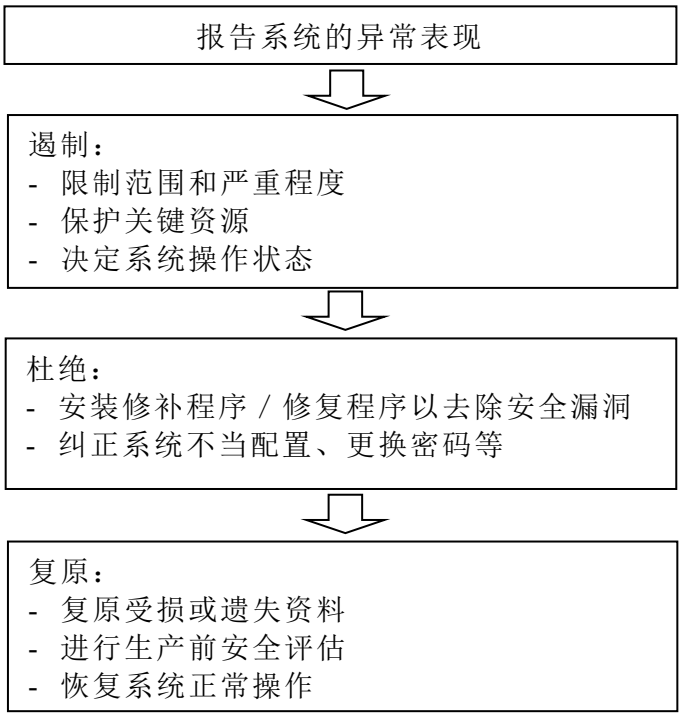


图 9.1 安全事故应急的主要阶段

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，以及事故应变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第 1 级信息系统，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第 2 级或以上的信息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。

分析结果应纳入信息技术安全风险管理及持续改进程序，以加强决策局 / 部门的安全保护，减少事故发生的机会。

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信息更新表

决策局 / 部门名称	
提交更新表的单位资料	
姓名：	职位：
联络号码：	电邮地址：
提交至 IT Security Team/DPO	
请将填妥的表格透过电子邮件提交至 IT Security Team， 并副本抄送更新表内的所有相关联系人： 电邮地址：*it_security@digitalpolicy.gov.hk*	

新增 / 更换 / 删除的更新请求*	
人员职务	
☐ 部门信息技术安全主任 ☐ 部门信息技术安全副主任 ☐ 参与支援部门信息技术安全主任 / 副主任工作的人员 ☐ 部门信息安全事故应急小组组长 ☐ 部门事故应急经理 ☐ 部门信息安全事故应急小组组员	
拟更换的现任人员（如有）：_____	
更新请求联络信息	
姓名：	职位：
办公室联络号码：	流动电话号码： *（作 7x24 紧急联络之用）*
电邮地址：	有效日期：

*(*删除不适用部分)*

附件 B：安全事故应变准备工作清单

B.1 安全事故应变准备工作清单样本

	项目	详情	进展情况
1	事故监察和侦测	安装防火墙设备，并采取访问控制措施，以保护重要系统和数据资源	
		安装抗恶意软件和修复工具，定期执行扫描和更新标识符	
		安装监察工具，例如入侵侦测系统	
		开启系统和网络设备的审计记录功能	
2	安全事故应变	准备安全事故应变计划	
		设计及准备报告机制	
		向全体人员颁布报告机制	
		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	
		向参与工作的全体人员颁布安全事故应变计划	
3	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	

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）：	
系统等级： ☐第 1 级　☐第 2 级　☐第 3 级	
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：	***信息安全事故初步报告提交日期：***
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：_____

☐ 保安局：_____

☐ 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）：	
系统等级： ☐第 1 级　☐第 2 级　☐第 3 级	
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：	***事故中期报告提交日期：***
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）：	
系统等级： ☐第 1 级　☐第 2 级　☐第 3 级	
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：	***事故事后报告提交日期：***
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
☐ 拒绝服务攻击
☐ 伪冒
☐ 大规模恶意软件感染
☐ 网站遭涂改
☐ 入侵信息系统或数据资产
☐ 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
☐ 勒索软件
☐ 其他：_____

受影响组件 / 资产：

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

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：_____

☐ 保安局：_____

☐ 其他：_____

香港警务处调查结果（如有）：

_____

事故发生的次序：

日期 / 时间	*事故*

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（如香港身分證號碼）：

_____

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：**

C.4.1 信息技术安全事故初步报告

限 阅

信息技术安全事故初步报告参考编号：_____

信息技术安全事故初步报告

（应在事故发生后两日内向局长提交报告）

背景资料	
决策局 / 部门名称：	
概述受影响的系统： *（例如系统名称、面向公众的信息技术服务、网址等）*	
系统等级： ☐第 1 级　☐第 2 级　☐第 3 级	
事故详情	
发生事故的日期 / 时间： 按一下或點選以輸入日期。	**发现事故的日期 / 时间：** 按一下或點選以輸入日期。
事故说明： ***事情发生和影响：*** _____	
调查结果（如有）： ***发生经过：*** _____ ***发生原因：*** _____	
涉及数据： **事故有否涉及保密资料？** ● ☐ 有，涉及 ☐限阅类别 / ☐机密类别数据 - 已通知保安局　☐ 有及于：_____ - ☐ 没有，将完成于：_____ - 请提供所涉及保密资料的详情： （例如数据是否加密、数据类型等） _____ ● ☐ 没有	

事故有否涉及个人资料？

- ☐ 有，所涉及个人资料为：_____
  - 已通知保安局 ☐ 有及于：_____
  - ☐ 没有，将完成于：_____

- ☐ 没有

事故有否涉及涉嫌犯罪行为？

- ☐ 有
  - 已报告香港警务处网络安全及科技罪案调查科
    ☐ 有及于：_____
    ☐ 没有，将完成于：_____

- ☐ 没有

为短期遏制或完全解决事故所采取的行动：

为解决事故所计划的行动：

目前系统的状况（完全恢复 / 有限服务）：

媒体 / 公众查询 （如适用）	
媒体查询数目：	**公众查询数目：**
项目负责人员 / 部门信息技术安全主任资料	
姓名：	***职位：***
办公室联络号码：	***24 小时联络号码：***
电邮地址：	***向局长提交报告的日期：*** 按一下或點選以輸入日期。
备注*（如有）**：***	

决策局局长资料	
姓名：	***职位：***
办公室联络号码：	***24 小时联络号码：***
电邮地址：	
备注*（如有）**：*** 批核☐　　不批核 ☐	

C.4.2 信息技术安全事故全面报告

限 阅

信息技术安全事故全面报告参考编号： _____

信息技术安全事故全面报告

（应在事故发生后七日内向部门首长提交报告）

背景资料	
决策局 / 部门名称：	
概述受影响的系统： *（例如系统名称、面向公众的信息技术服务、网址等）*	
系统等级： ☐第 1 级　☐第 2 级　☐第 3 级	
事故详情	
附上信息技术安全事故初步报告副本 *(与信息技术安全事故初步报告参考编号）*	
发生事故的日期 / 时间： 按一下或點選以輸入日期。	**发现事故的日期 / 时间：** 按一下或點選以輸入日期。
事故说明： ***事情发生和影响：*** _____	
有佐证的调查结果： ***事件发生的顺序：*** _____	

日期 / 时间	*事件*
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	
按一下或點選以輸入日期。	

有佐证的事故发生原因：

_____

涉及数据：

事故有否涉及保密资料？

- ☐ 有，涉及 ☐ 限阅类别 / ☐机密类别数据
  - 已通知保安局于：_____
  - 请提供所涉及保密资料的详情：
    （例如数据是否加密、数据类型等）

_____

- ☐ 没有

事故有否涉及个人资料？

- ☐ 有，所涉及个人资料为：_____
  - 受影响人数：_____
    （内部人员和市民人数分项数字）
  - 个人资料类别（如香港身份证号码）：

    _____
  - 是否已通知受影响人士：是／否。如否，原因：

    _____
  - 已通知个人资料私隐专员公署于：_____
    （附有向个人资料私隐专员公署提交的资料外泄事故通报表格）
- ☐ 没有

事故有否涉及涉嫌犯罪行为？

- ☐ 有
  - 已报告香港警务处网络安全及科技罪案调查科于

    _____
- ☐ 没有

已采取的行动及结果：

目前系统的状况（完全恢复 / 有限服务）：

如果恢复了有限服务，请提供完全恢复服务的时间表：

于责任方的问责和建议采取的后续行动<u>并提供佐证</u>：

（根据相关事故报告的调查结果、既定机制或适用规则和条例，以及相关管治框架，责任方可能包括承建商、人员和 / 或相关公共机构）

媒体 / 公众查询 （如适用）	
媒体查询数目：	**公众查询数目：**
项目负责人员 / 部门信息技术安全主任资料	
姓名：	***职位：***
办公室联络号码：	***24 小时联络号码：***
电邮地址：	***向局长提交报告的日期：*** 按一下或點選以輸入日期。
备注 *（如有）：*	
决策局局长资料	
姓名：	***职位：***
办公室联络号码：	***24 小时联络号码：***
电邮地址：	
备注 *（如有）：* 批核☐ 不批核☐	

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 / 部门信息技术安全主任 / 项目负责人员及政府信息安全事故应急办事处常设办公室
- 决策局局长
- 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*
2 日内（就事故已令政府尴尬或损害其监督角色的形象）	项目负责人员或部门信息技术安全主任向决策局局长递交信息技术安全事故初步报告	*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*
7 日内（就事故已令政府尴尬或损害其监督角色的形象）	项目负责人员或部门信息技术安全主任向决策局局长递交信息技术安全事故全面报告，并将已批核的信息技术安全事故全面报告副本递交予数字办	*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*

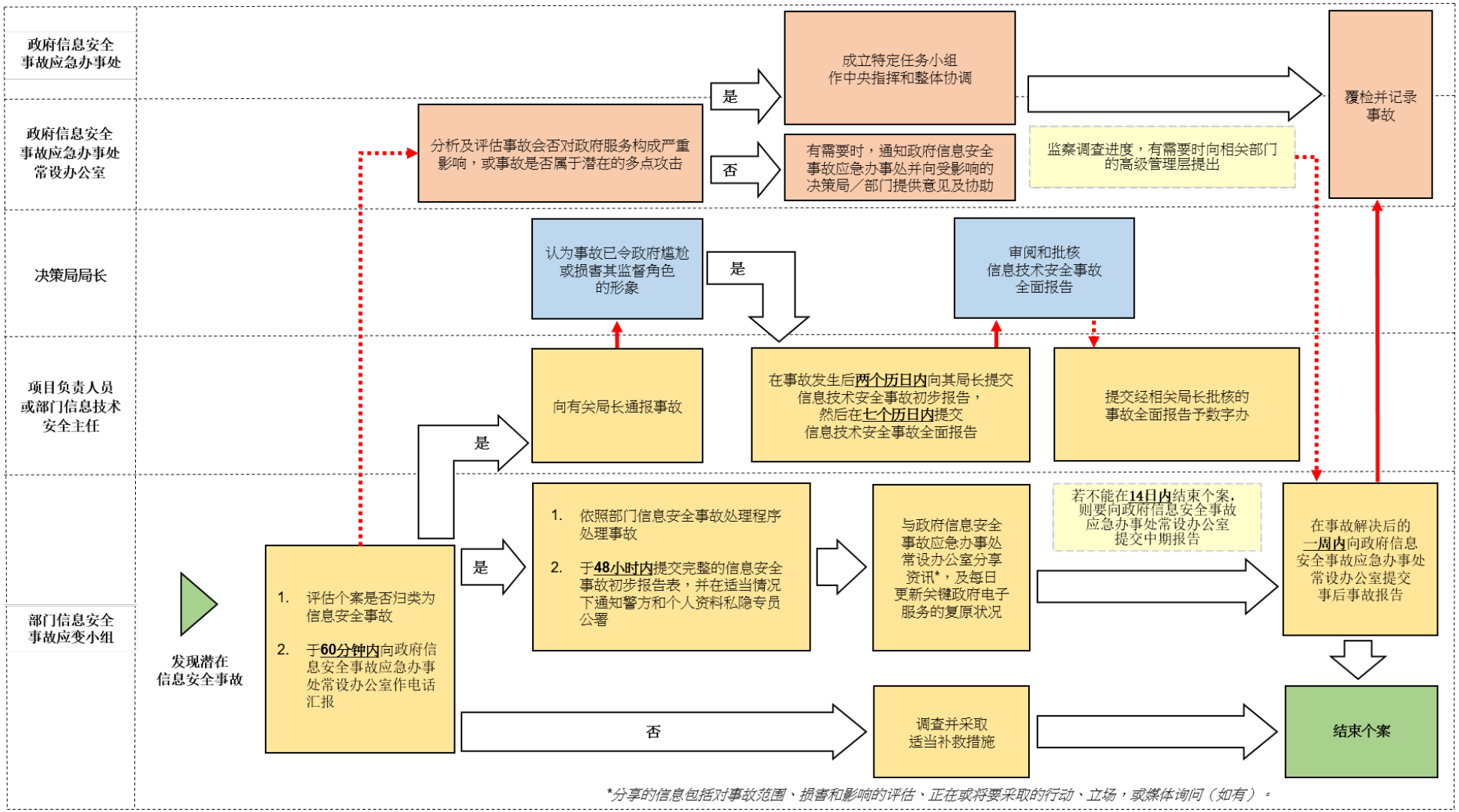
如怀疑构成刑事犯罪，则由信息安全事故应急小组决定	向警方举报以调查案件	*默认的电话热线*
如涉及个人资料	向个人资料私隐专员报告 （并尽可能通知受影响人士）	*默认的电话热线或任何其他途径*

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

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 安全事故的典型类型和迹象

为判断异常情况是由系统问题还是确实事故所造成，可留意安全事故一些特定迹象。安全事故的常见类型和迹象包括以下任意一种。此列表仅供参考，并非详尽无遗。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
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。	• 信息系统上的异常或未获授权的活动。 • 故意滥用或未获授权访问的证据。 • 对信息资产造成不利影响的行为。	1. 收集有关举报活动或滥用事故的信息。 2. 确定所涉及的个人或帐户。 3. 分析系统日志和审计追踪以确定滥用的程度。 4. 采访相关人员或用户以收集更多信息。 5. 评估滥用行为对信息资产的影响，并确定需要立即采取的行动，例如撤销访问或阻止未获授权的活动。 6. 如有必要，记录事故并将其报告给适当的利益相关者或当局。	• 系统访问和用户活动日志。 • 未获授权的系统操作或违反政策的记录。 • 与滥用事件相关的通信日志（电子邮件、聊天记录等）。 • 任何撷取的证据，例如屏幕截图或录音。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
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交互或透过自动化技术造成。	• 异常帐户活动，例如未获授权的访问尝试或权限升级。 • 异常系统或网络日志条目。 • 未获授权更改系统配置或数据。 • 存在未知或未获授权的用户帐户。 • 非预期的系统行为或性能下降。 • 未获授权访问或泄露数据的证据。 • 安全工具检测到的恶意软件或入侵迹象。 • 未获授权的远程访问或控制系统。 • 异常的网络流量模式或连接。	1. 识别并隔离受影响的系统或帐户，以防止进一步受到入侵。 2. 收集并保存相关日志和系统工件以供分析。 3. 分析系统日志、网络流量和其他可用数据，以确定攻击的切入点和程度。 4. 进行彻底调查以确定危害的性质，包括识别任何恶意软件、后门或未获授权的修改。 5. 评估入侵的影响，例如数据泄露或未获授权的访问，并采取适当的补救措施以减轻进一步的损害。 6. 将事件通知利益相关者，例如系统拥有者、用户和管理层。	• 显示未获授权的访问或可疑活动的日志。 • 显示入侵迹象的系统或应用系统日志。 • 恶意软件样本（如有）。 • 显示与怀有恶意的人士通信的网络流量日志。 • 用于入侵的用户帐户凭证或帐户。 • 任何撷取的证据，例如系统快照或鉴证图像。
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、死亡之 Ping	• 网络流量异常增加或网络拥塞。 • 系统性能下降或中断。 • 无法访问或使用特定资源或服务。	1. 确定遇到拒绝服务情况的受影响系统或服务。 2. 确定攻击的类型和性质，例如基于网络或基于应用系统。	• 流量日志，包括源互联网规约地址和攻击模式。 • 攻击的持续时间和强度。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
	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。	• 传入异常模式的请求或连接。 • 网络流量或日志中存在已知的拒绝服务攻击标识符。 • 非预期的系统或应用系统崩溃。	3. 分析网络流量日志、系统日志或入侵检测系统警报，以识别攻击的模式或标识符。 4. 通过实施流量过滤、速率限制或其他应对措施来减轻攻击的影响。 5. 与局部区域网络/系统管理员或服务供应商合作，确定攻击的来源或起源。 6. 记录事故，包括观察到的攻击模式以及对系统或服务的影响，以供进一步分析和报告。	• 任何撷取的攻击证据，例如流量撷取或日志。 • 表明与攻击相关的任何赎金要求或威胁的通信日志。 • 来自防火墙、路由器或其他安全设备的日志。
泄漏电子保密数据	保密资料外泄，或被未获授权人士访问。	• 对保密数据进行异常或未获授权的访问。 • 异常的数据传输或复制活动。 • 存在未获授权的用户访问保密数据的情况。 • 不寻常的访问模式，例如在正常工作时间之外或从未获授权的位置访问保密数据。	1. 确定保密数据泄露或暴露的来源和性质。 2. 确定泄露数据的范围和敏感性，包括保密级别和潜在影响。 3. 收集并分析系统日志、访问记录和其他相关证据，以识别未获授权的访问或活动。 4. 保留任何可用的鉴证证据以供进一步分析或采取法律行动。	• 显示未获授权的访问或数据泄露的日志。 • 显示数据泄露迹象的系统或应用系统日志。 • 与事件相关的通信日志（电子邮件、聊天记录等）。 • 有关泄露数据的信息，包括其性质和敏感性。 • 任何撷取的证据，例如屏幕截图或录音。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
		• 数据泄露或未获授权共享保密信息的证据。 • 未获授权披露或发布保密数据。	5. 将事件通知适当的利益相关者，例如资料拥有人、信息技术安全管理部门或管理层。 6. 评估数据泄露的影响并立即采取行动以控制进一步的泄露或未获授权的访问。 7. 进行彻底调查以确定事件的根本原因，包括安全控制措施中的潜在漏洞或弱点。	
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。	• 流动装置或抽取式媒体错放或丢失。 • 对丢失或被盗的装置进行未获授权的访问尝试。 • 异常的用户行为或模式，例如在未获授权的设备上访问保密数据。 • 未获授权访问与丢失或被盗设备相关的数据或帐户的证据。	1. 收集有关丢失或被盗的移动设备或可移动媒体的信息，包括设备标识符、内容和存储数据的分类。 2. 确定丢失或被盗的日期、时间和地点。 3. 采访相关人员或证人以收集更多详细信息。 4. 分析系统日志、访问记录或安全监控录像（如有），以识别与丢失或被盗设备相关的任何未获授权的访问尝试或可疑活动。	• 有关丢失设备或媒体的信息，包括其品牌、型号和序列号。 • 丢失的设备或媒体上存储的数据的详细信息。 • 应用于设备或媒体的任何加密或安全措施。 • 表明丢失时间和地点的报告或日志。 • 任何撷取的证据，例如照片或证人陈述。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
			5. 评估丢失或被盗的潜在影响，例如数据的敏感性和未获授权访问的可能性。 6. 将事件通知适当的利益相关者，例如数据拥有者、安保人员或管理层。 7. 采取措施降低数据泄露风险，例如远程删除、密码重置或帐户暂停。	
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。	• 使用其他用户的凭据进行异常或未获授权的登录尝试。 • 用户帐户使用的异常模式，例如无正当理由访问敏感数据或系统。 • 未获授权访问或滥用用户帐户的证据。 • 用户对未获授权的访问或可疑行为的投诉或报告。 • 试图绕过身份验证机制或冒充合法用户的证据。 • 用户帐户设置或权限的异常更改。	1. 识别已观察到伪冒尝试的受影响用户帐户或系统。 2. 收集相关日志、审计记录或系统工件，以分析与伪冒事件相关的活动。 3. 分析登录尝试、帐户使用模式或系统访问记录，以识别未获授权的访问或可疑行为。 4. 核实所报告的与伪冒相关的投诉或事件的真实性。 5. 评估伪冒事件的影响和潜在风险，例如未获授权访问敏感数据或系统。 6. 立即采取措施防止进一步未获授权的访问，例如禁用受损帐户或增强身份验证机制。	• 指示未获授权的访问或伪冒尝试的日志。 • 显示伪装活动迹象的系统或应用程序日志。 • 用于伪冒的用户帐户凭证或帐户。 • 与事件相关的通信日志（电子邮件、聊天记录等）。 • 任何撷取的证据，例如屏幕截图或录音。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
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。	• 异常的系统行为，例如频繁崩溃或冻结。 • 非预期的弹出窗口或错误消息。 • 系统性能缓慢或无响应。 • 异常的网络流量模式，例如频繁连接到可疑或恶意域。 • 通过安全软件检测已知的恶意软件标识符或指示符。 • 磁盘活动异常或中央处理单元使用率高。 • 未获授权访问或更改文件或系统配置。 • 用户关于可疑文件或活动的报告或投诉。 • 非预期的加密或与加密相关的活动。	1. 识别出现恶意软件感染迹象的受影响系统或网段。 2. 将受感染的系统与网络隔离，以防止进一步传播和破坏。 3. 收集恶意软件样本以进行进一步分析和识别。 4. 分析系统日志、网络流量和安全软件报告，以识别恶意软件活动的模式或指标。 5. 确定恶意软件的类型和行为，例如其传播方法、持续机制和负载。 6. 评估恶意软件感染对决策局／部门的系统、数据和运作的影响。 7. 进行初步调查，了解感染载体和潜在的切入点。 8. 部署适当的工具和技术来消除或减轻恶意软件感染。 9. 识别并关闭任何允许恶意软件渗透系统的安全漏洞或弱点。	• 恶意软件样本（如有）。 • 入侵指标或已知的恶意软件标识符。 • 显示可疑活动或连接的系统日志。 • 显示与恶意域或互联网规约地址的通信的网络流量日志。 • 受恶意软件影响的文件或目录。 • 有关恶意软件行为或负载的信息。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
		• 数据泄露或与指令和控制服务器通信的证据。	10.从未被感染的备份中恢复受影响的系统或在必要时重建它们。	
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。	• 无法访问或打开档案并显示勒索消息或警告的文件。 • 异常的文件扩展名称或文件名称更改。 • 无用户干涉而被加密或修改的文件。 • 异常网络流量模式，例如与已知勒索软件指令和控制服务器的通信。 • 系统上存在与勒索软件相关的文件或可执行文件。 • 勒索软件感染后出现异常系统行为，例如性能缓慢或崩溃。 • 攻击者要求支付赎金或进行通信。	1. 识别受影响的系统或网段。 2. 将受感染的系统与网络隔离，防止进一步传播。 3. 收集勒索软件样本以供进一步分析（如有）。 4. 分析系统日志、网络流量和安全软件报告，以识别勒索软件活动的指标。 5. 确定勒索软件的类型和变种。 6. 评估勒索软件感染对系统和数据的影响。 7. 识别切入点或感染载体。 8. 解密来自攻击者的任何可用的赎金票据或通信。 9. 确定赎金金额和加密货币钱包地址（如提供）。 10.收集有关受影响文件及其加密状态的信息。 11.研究任何潜在的备份系统或数据恢复选项。	• 勒索软件样本（如有）。 • 来自攻击者的勒索字条或通信。 • 入侵指标或已知勒索软件标识符。 • 显示可疑活动或连接的系统日志。 • 显示与恶意域或互联网规约地址的通信的网络流量日志。 • 勒索软件附加的加密文件或文件扩展名称。 • 有关赎金金额和加密货币钱包地址的信息。 • 备份系统和数据恢复信息。 • 任何相关的系统或网络配置。

信息安全事故	描述	迹象	初步分析／处理	识别／分析所需的信息
网站遭涂改	未获授权窜改互联网网页的内容。	• 网页外观或内容发生显着变化。 • 未获授权添加、删除或修改内容。 • 含有未获授权的消息或内容的网页被污损或破坏。 • 非预期的重新定向到未知或恶意网站。 • 异常的网络服务器日志，例如多次失败的登录尝试或对敏感目录的访问。 • 用户对可疑或更改的网络内容的报告或投诉。 • 未获授权访问或修改网站配置或文件的证据。 • 搜索引擎排名或网站可见度发生非预期的变化。	1. 识别被破坏的网站。 2. 撷取被篡改内容的屏幕截图或记录。 3. 分析网络服务器日志以确定损坏的程度和持续时间。 4. 识别日志中任何未获授权的访问或修改。 5. 评估污损对网站功能和声誉的影响。 6. 确定用于破坏的方法（例如，利用漏洞、未获授权的访问）。 7. 调查任何潜在的安全配置错误或弱点。 8. 从未被感染的备份中将网站恢复到原始状态（如有）。	• 被破坏网站的划一资源定地址或网址。 • 被篡改内容的屏幕截图或记录。 • 显示未获授权的访问或修改的网络服务器日志。 • 有关对网站功能和声誉的影响的信息。 • 任何安全配置错误或漏洞的详细信息。 • 原始网站内容的备份副本（如有）。 • 任何相关的系统或网络配置。

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。

尽早侦测和识别潜在的安全事故至关重要。因此，决策局 / 部门必须保持警惕，留意其装置 / 环境内任何异常或可疑的活动。以上仅列出了常见的迹象，该列表并非详尽无遗。决策局 / 部门应主动监察其系统，并及时调查任何异常行为或与安全相关的异常的迹象。以上提供的初步分析步骤和识别 / 分析所需的信息仅供参考。由于各决策局 / 部门的情况和事故应变程序可能有所不同，决策局 / 部门应相应调整其应变措施。决策局 / 部门应优先考虑持续监察，并对任何异常或可疑活动保持警惕，以提高及时侦测和识别潜在安全事故的能力，以便及时作出应变和缓解措施。

F.2 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