国际民航组织内部人员威胁工具包

概述

国际民航组织与航空安保专家组培训工作组协作开发的这个工具包旨在帮助在航空环境中运行的组织更好地对不断演化的内部人员威胁做出反应。正如国际民航组织《航空安保全球风险背景综述》（Doc 10108号文件，限制发行）所指出的，恐怖分子一直在寻求利用安保管制中的易受攻击点，并针对航空实施非法干扰行为（AUI），这些都可以通过利用内部人员来实现。

哪些人员属于内部人员？

内部人员是指在航空部门工作或为航空部门工作的全职或兼职雇员（包括承包商、临时人员和自己单干的人员），其角色为他们提供了接近已采取了安保措施的地点、物品或敏感安保信息的特权和/或知识。

内部人员威胁是什么？

内部人员威胁是指航空雇员通过使用被授权的访问权限以及这种访问权限带来的有利条件，进行非法干扰行为或为非法干扰行为提供便利所产生的风险。

内部人员的动因是什么？

内部人员可能会因缺乏意识、怀有满不在乎的情绪或恶意而进行或促成非法干扰行为。缺乏对政策和程序的认识以及怀有满不在乎的情绪（对政策和程序采取马虎态度）可能会导致内部人员因疏忽、不作为或未能遵守安保政策和程序而无意中为非法干扰行为提供便利。

另一方面，怀有恶意的内部人员 — 那些有意识地决定进行非法干扰行为的人 — 可能受到个人弱点、生活中的事件和情境因素（如经济收益、意识形态、报复、渴望被认可或胁迫）的共同驱使。

怀有恶意的内部人员可能故意寻求加入某个组织进行非法干扰行为，或在其受雇期间产生这样做的意图（例如，被第三方征聘以利用其受信任的职位）。

内部人员可以如何行动？

内部人员可以进行任何非法干扰行为（如破坏处于使用状态的航空器，将用于犯罪目的的武器或危险装置或材料带入航空器或机场）。内部人员可以共享机密信息、为进入限制区提供便利、未充分履行职责从而允许将违禁品带入限制区，帮助外部各方获得访问计算机系统或其他数字基础设施[1]等的机会。

风险减轻措施

一系列由安保人员实施的安保措施和政策可以帮助各组织减轻内部人员构成的威胁。总体而言，这些措施旨在降低因征聘其行为可能构成安保关切的工作人员所带来的风险；将现有雇员变成安保关切的可能性降至最低；减少内部人员活动的风险；以及保护组织的资产。

[1] 数字基础设施是指主要与移动和互联网通信相关的资产。

可按以下方面对内部人员威胁减轻措施和工具进行分组：

背景调查和审查

政策和程序：强有力的背景调查政策和程序，包括雇员的身份、之前的工作经历、犯罪记录和教育背景，是旨在减轻内部人员构成的威胁的任何框架的基石。这些政策和程序必须明晰、简明，并应定期接受审查。

初始背景调查：所有需要在无人陪同的情况下进入空侧和安保限制区的雇员以及接触敏感安保信息的人员都必须接受主管当局规定的背景调查[2]。

初始背景调查应包括：

- 身份（如提供护照、身份证、出生登记记录等）；
- 犯罪记录（在当地规章和法律允许的范围内）；
- 举荐调查（证明未来员工的职业道德和总体适合性）；和
- 之前的就业情况（如之前的雇主、受教育情况等）。

重复性背景调查：作为周期性人员安保检查的一部分，应定期进行背景调查并定期对背景调查的相关信息进行更新。每次需要更换机场身份识别通行证时，进行一次新的背景调查是一种好的做法。

那些通过内部人员进入安保限制区或利用内部人员提供的情报实施非法行为或非法干扰行为的人通常在获得工作岗位后有了这样做的意图。此外，许多内部人员可能已经引起了管理层的注意（例如，因为违反纪律和表现不佳），这种情况在重复性背景检查过程中应予以考虑。

持续性审查：应鼓励与有关主管当局（以及其他国家的有关当局）合作进行持续性审查过程。这是为了评估雇员是否仍满足适用的就业要求。

[2] 附件 17 —《安保》（第十二版，第 18 次修订）中的标准 3.5.2。

经强化的背景调查：涉及情报（以及关于一个人是否适合履行某一职责的任何其他相关信息）的背景调查可能是有用的。实际上，各国可与有关国家主管当局合作，将一些经强化的数据纳入分层背景调查和审查过程。

同样，如果工作人员发现某人有可疑或异常行为，应联系相关安保部门和当地主管当局，因为可能需要进行经强化的情报背景调查。

培训和意识

意识培训：应鼓励对所有工作人员进行安保意识和安保文化培训。这将有助于确保所有人员了解安保政策、标准、指导原则和程序，并理解他们维护高级别安保的目的。这项培训还将使新雇员能够培养识别可疑行为并向主管当局或执法人员/机构安全报告这些可疑行为的能力，包括通过匿名方式。

培训一体化：可将安保意识纳入初训和现有的复训，或通过使用宣传材料、讲习班、临时培训班等方式，推广强有力的和有效的航空安保文化。

针对特定角色的培训：对于一些工作人员，包括但不限于主管、管理人员以及负责人员安保的人，更深入的、针对特定角色的培训将有利于取得有针对性的培训结果。

意识宣传：应开发涵盖关键安保方面的视觉信息，在各组织内和机场环境中展示，作为对工作人员的视觉提醒。

通行管制措施

检查：应制定通行管制措施，以确保旅客以外的人员以及他们携带的物品在进入机场安保限制区之前接受检查[3]。这类检查应包括一些随机的和不可预测的检查方法，以减少内部人员获得信息的机会，并减少违禁物品被运送至空侧的机会，包括它们由雇员带入空侧的情况。

政策和程序：政策和程序应明确，并包括：

- 停用已离开机构（辞职、退休等）的雇员的身份识别标牌；
- 根据严格的运行需要，限制通行证持有人进入限制区域的权限；
- 充分保护周界和通行管制点，确保无法绕过工作人员安检；和
- 在适当情况下，实施监督协议，并在运行活动中更广泛地使用闭路电视（CCTV）。

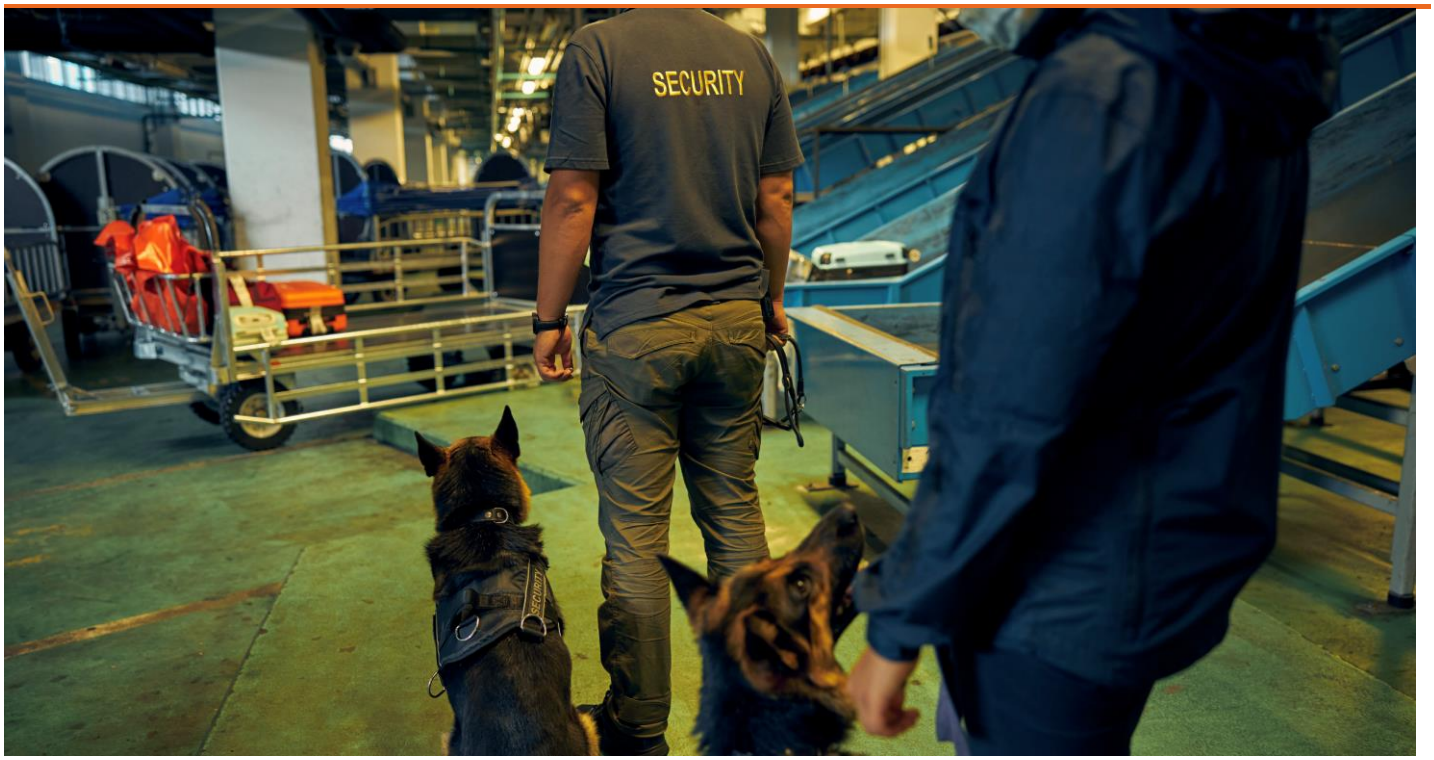
[3] 附件 17 — 《安保》（第十二版，第 18 次修订）中的标准 4.2.5。

审查通行人员名单：建议审查机场签发身份识别通行证的程序，以确保要求进入某一区域的雇员是出于运行需要而进入这一区域。

巡逻

随机性和不可预测性：巡逻应以随机的和不可预测的方式进行巡逻（如抽查），这样就不会因恶意侦察或内部人员的信息而避开或绕过巡逻。此外，巡逻不仅应关注对机场人员的监视，还应包括旅客、其他机场利害攸关方、机场基础设施和货物，以发现异常活动安保状况不佳的迹象。

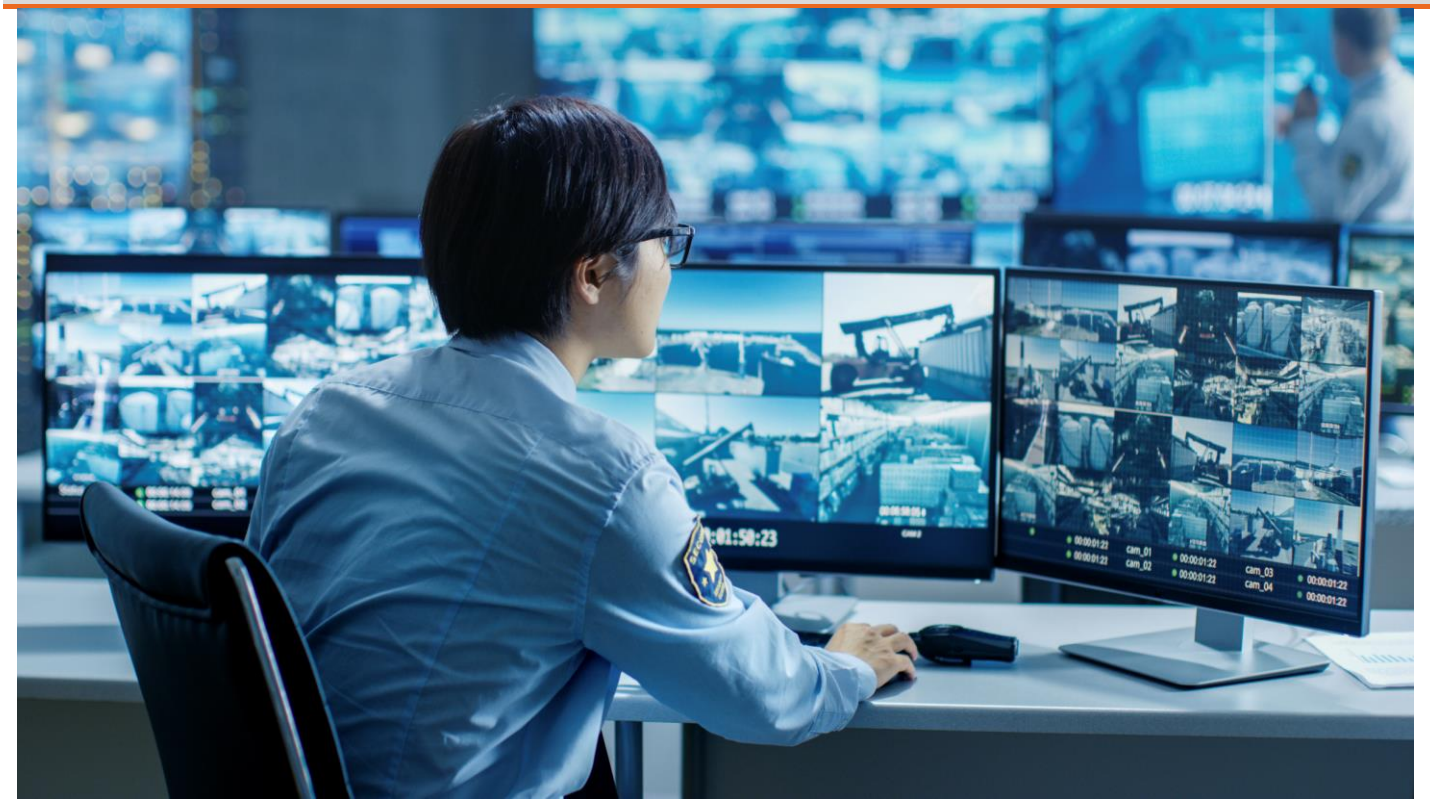
如果巡逻人员穿着制服并使用有标记的车辆，巡逻可以有效地起到视觉威慑作用。或者，如果以秘密的方式进行，巡逻可以增加监视力度。



监视和监控

方法：对针对内部人员威胁的程序和雇员进行质量控制和监控可以在避免或快速解决安保征候事件和非法干扰行为方面发挥重要作用。监视方法包括 CCTV、审查系统日志（如进入请求）和对地面工作人员进行监视。

主管还在识别和监控受其监视的雇员的异常活动和行为方面发挥关键作用。



数据：在一些组织中，可以在记录雇员行动的各种软件应用程序日志中找到雇员数据。这些数字化数据可以凸显工作模式，并作为工具用于确定机场工作人员中是否存在任何恶意意图（如在没有运行需求的情况下进入区域）。

应用程序可包括：

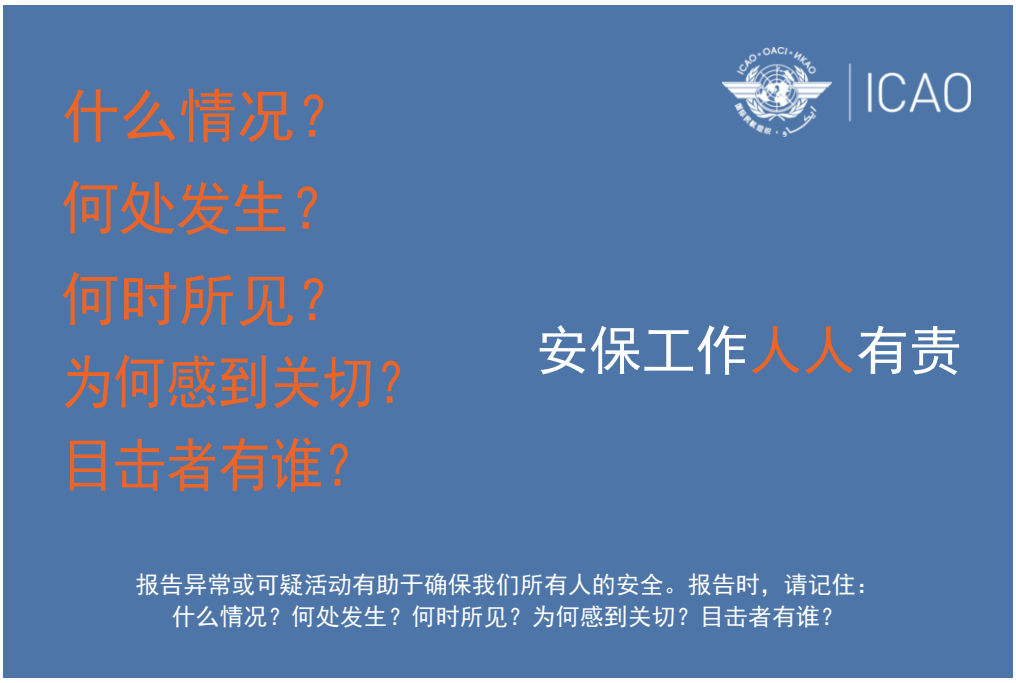
- 实际进出记录，主要关注时间和进入物理空间；
- 登录/注销记录，关注时间和用户匹配证明文件；
- 电子邮件应用程序日志；和
- 数据库应用程序日志。

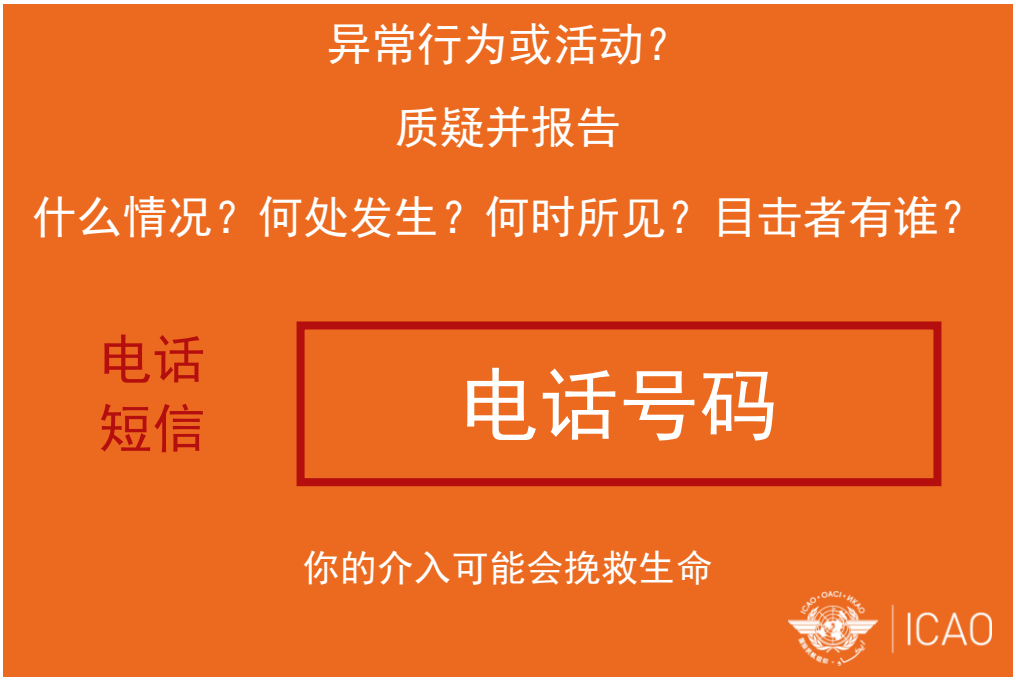
报告机制

报告可疑行为：报告机制应涉及整个组织的每个人，而不仅仅是直接参与安保的人。这些都很重要，因为雇员是机构的“眼睛”、“耳朵”和“声音”。

可以建立报告机制，以便雇员可以通过短信、电子邮件、电话、内部沟通渠道或通过亲自与某人交谈来安全地报告可疑行为或征候事件。安保报告应得到明确、有效和快速的响应。

匿名或秘密报告对于帮助减轻潜在的内部人员威胁和在组织中建立有效的安保文化非常有用。



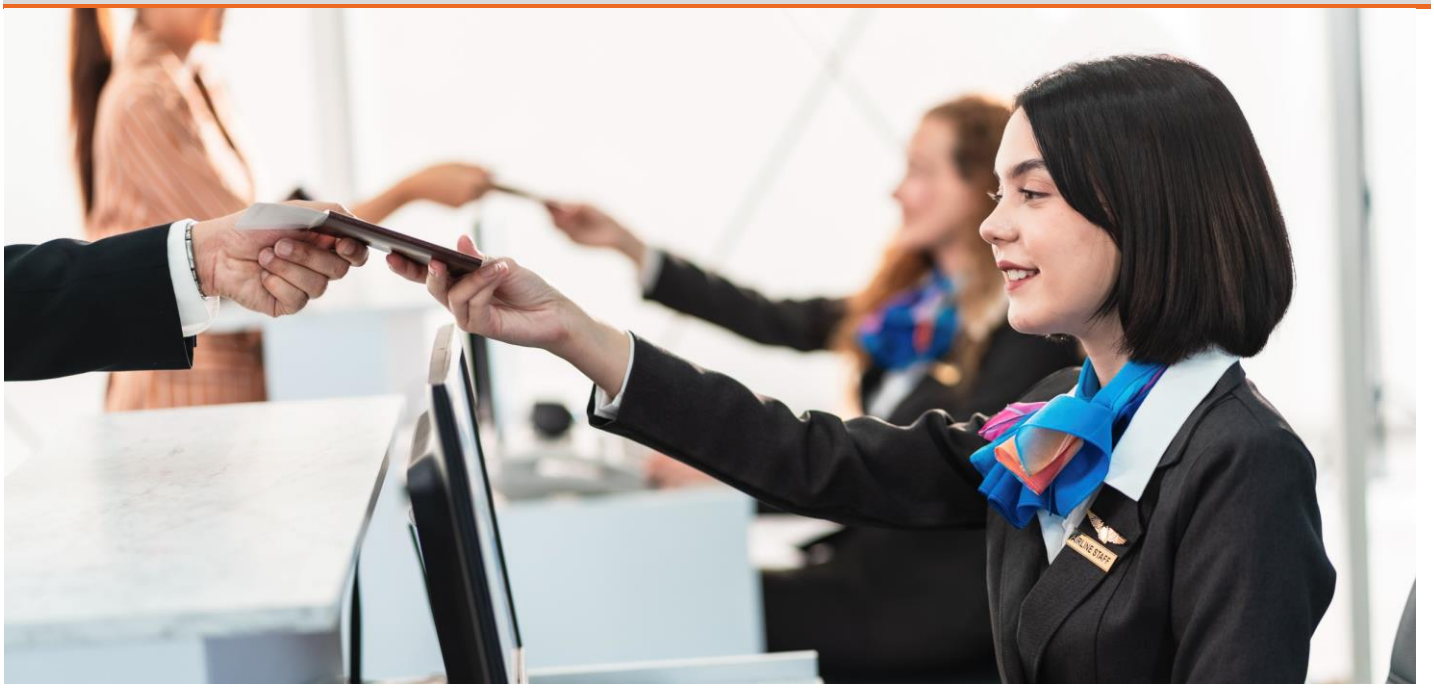


行为检测[4]

行为检测：有助于减轻内部人员威胁的一个有用工具是行为检测。它基于这样一个前提，即人们可能会表现出可疑或异常行为的迹象，并且这些迹象可以被接受过适当训练的人发现。

培训：让工作人员了解什么是可疑活动和异常行为，并了解如何对它们进行报告，这可能是一个有用的工具。

行为检测培训应面向广泛的人员，包括但不限于发放通行证、进行背景调查和检查的人。然而，作为一般安保意识培训的一部分，所有工作人员都可以从这类培训中受益。



安保文化[5]

强有力的和有效的安保文化：在整个航空部门建立积极的安保文化，对于减轻内部人员威胁和取得有效和稳健的安保结果至关重要。雇员：

- 通过定期掌握关于威胁和更广泛的安保问题的情况介绍，可以受到激励并了解到内部人员风险；
- 可以接受培训，从而可以识别和报告非正常的或可疑行为；和
- 可以成为有关易受攻击点及其解决方法的宝贵信息来源。

[4] 行为检测是采用有关行为特征识别的技术，包括但不限于异常行为在生理或手势方面的表现（言语表现和非言语表现），以查明具有实施非法干扰行为的潜在意图的人。

[5] 关于安保文化（包括国际民航组织安保文化资源）的更多信息，见国际民航组织安保文化网站：www.icao.int/Security/Security-Culture。

领导力和策略

强有力的领导力：至关重要的是，领导须了解他们在展示期待员工具有的积极安保行动和行为方面的作用。应鼓励雇员和管理层之间进行坦诚沟通，领导应了解员工的日常运行压力，以及这些压力可能产生的内部人员风险。

掌握安保风险原则、对安保政策采取自上而下的做法并在预期行为方面做出表率的行政长官（如高级经理）可能会在整个组织中促进更合规和更一致的做法，从而进一步帮助减轻内部人员威胁。

策略：建议采用（经领导层批准的）内部人员威胁减轻策略来帮助雇员了解如何识别和报告工作场所内的可疑行为。

策略还可包括针对内部人员的政策、指导原则和程序。这包括入职前以及雇员在机构整个任职期间采取的行动。应定期与所有主要利害攸关方一起定期审查该策略和相关政策。

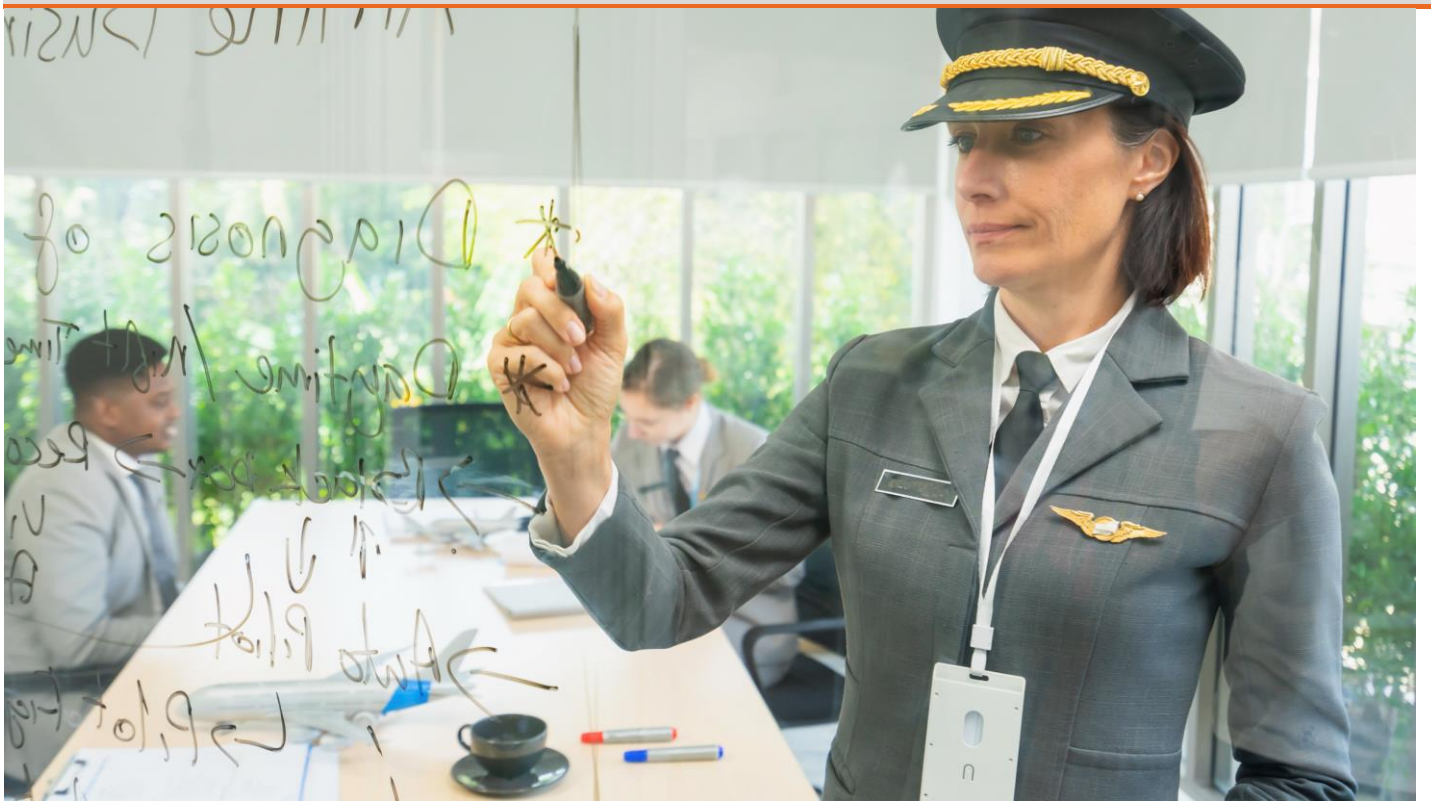
框架文件[6]、手册和指导材料可作为有用的额外工具。

[6] 例如：www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework

人的因素

人的行为能力和因素：各组织必须了解人的行为能力如何帮助减轻内部人员威胁。这包括认识到人的因素如何影响可能有意或无意利用其通行权限来制造非法干扰行为的个体。领导和高级管理层应：

- 了解人的各项能力，以及这些能力如何有助于减轻内部人员活动的风险；
- 了解人的局限性以及如何顾及这些局限性，以确保它们不影响行为能力；
- 使工作人员易于报告安保关切和可疑行为；
- 了解人的因素、安保文化和动机之间的联系；
- 确保人员可以获得需要的资源；
- 确保管理人员能够识别压力和疲劳的迹象，以便及时处理；和
- 避免在日常活动中出现满不在乎的情绪。

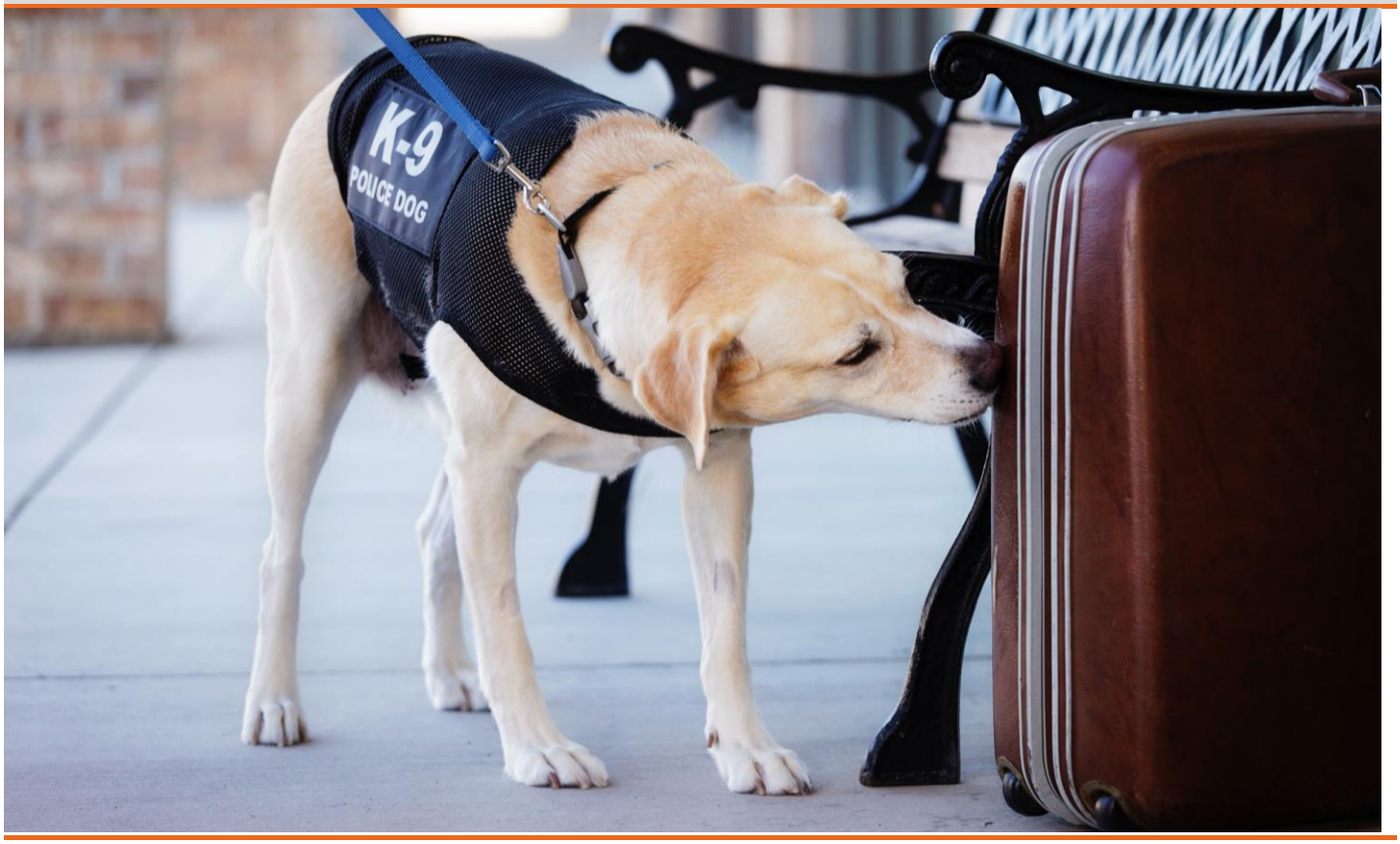


先进技术[7]

爆炸物痕量探测（ETD）：爆炸物痕量探测机器的使用强化标准的非旅客检查程序和/或整个安保限制区内采用的随机的和不可预测的安保对策，从而有助于减轻内部人员威胁。

[7] 先进技术的应用可通过在安保检查过程中提高探测标准和/或在机场环境中以随机和不可预测的方式应用时在安保基线的基础上加强安保，帮助减轻内部人员风险。

探爆犬（EDDs）：探爆犬团队可用于实现许多目的，例如：机场所有区域（陆侧、空侧、旅客区、非旅客区、行李区、货物区等）的安检，搜索安保限制区，并提供实施随机的和不可预测的安保措施的方法。



人工智能（AI）：训练有素的雇员使用基于人工智能的系统可以帮助识别趋势和非正常活动。例如，现代化的征候事件管理方案可以帮助识别征候事件，并将普通事件与迫在眉睫的威胁（如试图闯入受保护区域）区分开来。

—完—