民 用 航 空 中 的 网 络 安 保 文 化

由秘书长授权出版
2022 年 1 月
国际民用航空组织

1. 引言

本指导材料符合国际民航组织航空网络安保战略[1]以及网络安保行动计划[2]，网络安保行动计划的行动编号 CyAP7.1 建议界定并促进民用航空网络安保文化。

2. 范围

本指导材料旨在支持成员国和利害攸关方在其组织内设计和实施强大的网络安保文化。最终目标是支持民用航空安保以及抵御网络威胁和风险的能力。

3. 网络安保文化的定义、总体目标和益处

3.1 就本指南而言，对网络安保文化的通常理解是组织日常运行中固有的一套假设、态度、信念、行为、规范、看法和价值观，并在所有实体和人员与数字资产互动的行动和行为中加以反映。

3.2 正向的网络安保文化旨在使网络安保思维成为组织习惯、行为和流程的一部分，将其嵌入日常运行中，并反映在所有人员的行为和行为中。

3.3 建立起强大而有效的网络安保文化作为组织文化的组成部分，通过及早识别潜在的网络风险，能帮助组织提高整体绩效。

3.4 民用航空的网络安保文化奠基于该部门实施稳健的航空安全和安保文化方面的经验、努力和成功，并与其共享许多核心要素。网络安保文化的这种跨领域性质不仅会增强网络安保态势，还会在三个领域产生积极的溢出效应，以支持促进和加强正向的安全、安保和网络安保文化。

3.5 总之，网络安保文化使组织中的每个人，无论其角色如何，都能在数字环境中更好地发挥作用。设计和实施有效且稳健的网络安保文化的益处示例包括：

a) 提高组织的网络安保成熟度；
b) 所有人员对信息的适当处理；
c) 改进网络安保态势，支持组织在减轻网络风险方面的有效性和效率；
d) 提高所有人员对网络风险的认识，及其个人在识别和减轻这些风险方面所起的作用；和
e) 在应用组织网络安保流程和程序以及报告可疑网络活动等方面愿意进行个人监督报告，从而提高主动性、并更好地侦测网络风险。

3.6 本指南的以下部分说明了有效的组织航空网络安保文化核心要素。然而，尽管这些核心要素定义明确，但网络安保文化应该在每个组织内进行独特设计。应考虑不同方面，包括组织网络安保成熟度水平、现有文化和价值观，以及整体网络安保威胁格局。

3.7 强大和有效的民用航空网络安保文化核心要素是：

---

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
[2] 国际民航组织 2020/114 号国家级信件

a) 领导力；
b) 跨域链接；
c) 沟通；
d) 意识、培训和教育；
e) 报告系统；
f) 持续审查和改进；和
g) 正向的工作环境。

4. 领导力

4.1 有效的网络安保文化取决于组织中每个人的承诺，从高级管理层开始。高级管理层应在所有活动、战略、政策和组织目标中始终对网络安保文化做出充分承诺。

4.2 高级管理层应遵守网络安保政策，以身作则，成为组织主管和人员的榜样。他们还应该倡导将网络安保作为一种组织和个人价值，同时努力使他们的行为与这种价值保持一致。

4.3 在这方面，高级管理层应：

a) 努力增进他们的民用航空网络安保知识；
b) 始终遵守网络安保规则、流程和程序，并以身作则；
c) 明确将网络安保列为组织优先事项；
d) 将航空网络安保纳入组织的书面政策，成为公司管理计划不可分割的一部分；
e) 为网络安保文化的实施提供显明的支持；
f) 确保和支持所有人员的网络安保培训和能力建设；
g) 确保及时处理网络安保报告，并确保及时实施任何所需的纠正和预防措施；
h) 每当网络安保受到威胁时进行适当干预；和
i) 对组织网络安保态势、网络安保文化、以及为支持持续提高网络安保文化在整个组织的采用而分配的措施和资源等发展情况进行监测。

4.4 在高级管理层的领导下，组织的管理层还应根据其职责和管理范围，努力采取第 4.3 段中所载的行动，以便在整个组织内传播对网络安保文化的承诺。

5. 跨域链接

5.1. 考虑到每个组织存在众多的网络风险和漏洞，应该正式建立跨域链接。

5.2. 可以建立一个向高级管理层报告的多学科工作队，作为支持整个组织网络安保文化协调的一种手段。

5.3. 工作组的目标将包括以下内容：

a) 定期评估组织内网络安保文化的成熟度；
b) 查明网络安保文化实施方面的风险和机遇；
c) 弥合不同内部利害攸关方对网络安保文化的看法；和
d) 支持组织中开发和实施培养网络安保文化的相关跨领域活动。

6. 沟通

6.1. 在确保成功实施网络安保文化方面，沟通在内部和外部都发挥着至关重要的作用。这是达到预期意识水平的主要手段。

6.2. 为了使沟通有效，某些技能应被视为稳健的网络安保文化的一部分：

a) 积极倾听—观察语言和非语言信号的过程，以识别其他人的价值观和需求，并有助于改善团队沟通；
b) 根据不同的受众和情况调整沟通方式—了解他人如何沟通并定制信息以更好地向其传达；和
c) 沟通的清晰性—查明沟通的内容和方式。

6.3. 高级管理层应确保适当地向所有人员传达有关网络安保的内部政策和指南及其引入原因。稳健的内部沟通计划有助于所有人员接受和理解网络安保措施，并有助于促进组织中的网络安保文化。

6.4. 此外，内部沟通计划将极大地帮助：

a) 确保所有人员充分了解他们的职责、权利和组织中现有的报告机制；和
b) 推广组织数字行为准则，包括人员应始终遵守的流程、措施和控制。

7. 意识、培训和教育

7.1 意识、培训和教育是学习过程的关键领域，应该利用这些领域来建立强大的网络安保文化。意识为人们传授知识，培训教导技能，教育则在理论框架内提供知识和技能，从而将意识和培训结合起来。

7.2 所有与组织数字资产交互的民航人员，无论其角色或职能如何，均应参与网络安保意识、培训和教育方案，以确保他们具备有关航空网络安保风险、措施和目标的必要知识和技能。这些方案应在必要和可能的情况下根据受众而调整。

7.3 应为所有人员在聘用以及定期培训时提供网络安保意识方案。应根据组织中网络安保文化的成熟度确定意识方案复训的时间间隔，并且可根据该成熟度级别的发展情况重新审视。

7.4 建议至少真人亲身(在物理或虚拟教室环境中)提供一次网络安保意识课程。网络安保并不是所有人员都熟悉的题目，如果没有专业人士的指导，有时很难消化。因此，在课堂环境中与专业人士的互动有助于理解网络安保主题。这使得培训员能够以便于非技术人员理解的简化方式解释概念、流程、程序和控制，并说明增强组织网络安保态势的好处及其对人员整体生产力的积极影响。

7.5 在真人亲身提供的意识/培训初始课程之后，组织可以考虑使用电子学习方法(计算机管理学习)进行复训。此类决定应考虑组织中网络安保文化的发展情况，以及组织中为应对不断变化的网络安保风险环境而引入的网络安保流程、控制和程序的变化。

7.6 网络安保意识方案应由具备所需技术知识的专业人员提供。然而，技术意识方案面临的挑战之一是演示者缺乏软技能，而充分的沟通和“销售”技能则在吸引人员以及确保他们对网络安保文化的认可和支持方面大有帮助。因此，组织应确保意识方案领导者同样具备灌输人员行为改变以支持采用网络安保文化所需的技术知识以及软技能。

7.7 典型的网络安保意识方案应包括以下主题：

a) 意识方案的目的；
b) 组织中现有的沟通机制；
c) 对民用航空网络风险和潜在后果的总体概述(包括示例)；
d) 组织的网络安保控制、流程和程序；
e) 人为要素在保护组织免受网络风险方面的作用；
f) 在观察到同事的不合规行为时，人员相互提醒组织网络安保原则的重要性；
g) 概述可能针对人员的不同漏洞利用方法及其后果(包括示例)；
h) 如何识别可疑的网络活动；
i) 自满对组织的影响(包括示例)；
j) 网络卫生原则；
k) 妥善处理敏感数据和信息；和
l) 报告机制、如何使用以及后续机制。

7.8 还应定期开展网络安保意识宣传活动作为提醒，以加强人员的知识和技能。有多种工具可用于此目的，包括：

a) *纸质工具*—例如海报、小册子、宣传册等。此类媒体易于分发和消化。但是，这些是被动工具，需要经常更新(每次更新都要重新打印)；和
b) *在线工具*—例如电子邮件、时事通讯、屏幕保护程序上的消息、内联网、短视频、常见问题页面、电子学习(计算机管理学习)等。与纸质工具相比，这些工具的主要优势是能够与整个组织传达联系。它们在资源方面相对容易更新，并且生产成本较低。

8. 报告系统

8.1 内部网络安保报告系统的开发和实施是网络安保文化的基石。该系统使组织能够主动管理其网络风险，衡量组织网络安保态势的发展，识别和规划工作人员的意识和培训需求，并根据网络安保趋势的发展以及随着网络安保文化的成熟调整其内部流程、控制和措施。

8.2 网络安保报告系统从航空安全和航空安保报告系统中集结要素。因此涉及两个领域：第一个领域是报告不符合组织信息安保政策和流程的自身行动/错误，第二个领域是报告其他工作人员的可疑/错误行为。

8.3 在开发其网络安保报告机制时，鼓励组织借鉴开发和实施航空安全和航空安保全报告系统汲取的经验。

8.4 实施网络安保报告系统时应考虑以下要素：

a) 个人信息的保密性，即不收集和/或存储个人数据。收集个人数据时，仅应将其用于就所报告事件获得澄清和进一步信息、或向报告者提供反馈；
b) 为确保个人信息的保密性，应制定政策，清楚识别负责管理、维护、保证保密性、分析和跟踪收集信息的人员并向其追究问责；
c) 就如何使用报告系统向所有人员提供充分的培训；
d) 在网络安保报告中实施公正文化，并让所有人员充分了解公正文化如何运作，使其更自如地提供信息；和
e) 如适用，实施激励计划以便鼓励人员报告自己的错误以及他们观察到的任何可疑网络行为的。

公正文化

8.5 组织应鼓励其人员通过采用公正文化来报告网络安保事件。公正文化是在安全报告中实施的一个概念，对于促进网络安保文化具有重要价值。

8.6 在网络安保报告环境中，公正文化鼓励所有人员报告网络安保事件和错误。在这种环境中，每个人都明白，他们将根据自己的行为而不是行为的结果得到公平对待。在公正文化的环境中，所有人员都清楚地明白，对所有错误一律惩罚而不管其情况如何，这是不公平的，但同时他们也明白，一律免究不罚是不可接受的，因为一些行动可能是恶意犯行，或者可能是全然过失和/或漠不关心所致。因此，在设计公正文化时，重要的是在可接受和不可接受的行为之间划清界限。

8.7 公正文化不仅界定了人员对其组织的责任，也界定了管理层对人员的责任。这些职责应载入政策中，使组织的高级管理层应该：

a) 鼓励员工实践网络卫生，并承诺认可他们在支持组织管理网络风险方面所做的努力；
b) 承诺为所有人员提供适当的网络安保程序、意识、培训和教育，以支持他们履行职责；
c) 如果任何事件是由于缺乏应对某种网络风险的意识或及时性而引起的，则承担责任；和
d) 鼓励工作人员报告他们目睹的网络事件、危险、错误或任何可疑行为，而不必担心遭到报复。

质量控制

8.8 组织应实施旨在监测网络安保措施有效实施的质量控制方案。质量控制方案可以成为保持人员警觉和致力于网络安保文化原则的有效工具。通过展示管理层对网络安保目标和合规性的承诺，执行质量控制的频率和严格性可能对人员产生积极影响。

8.9 对现有报告机制的定期质量控制应作为质量控制方案的一部分进行。

9. 持续审查和改进

9.1 组织应制定绩效指标框架，以便评估现有措施对网络安保文化的影响，并查明理想的文化成果与实际文化成果之间存在的差距。

9.2 由于可能无法直接观察到网络安保文化的某些要素，因此可以使用一系列可能的指标来衡量网络安保文化的有效性。此类措施可能包括：

a) 报告事件的统计数据(与从组织日志中采掘得出的数据相比)，以衡量人员的网络安保绩效、他们的意识水平以及在促进网络安保报告方面取得的进展；
b) 复训的结果；
c) 模拟恶意攻击以测试人员响应的结果； 和
d) 问卷调查和访谈。

10. 正向的工作环境

10.1 总体正向的工作环境也可能极大地影响人员对网络安保文化的承诺并提高网络安保绩效。

10.2 正向的工作环境至少应包括：

a) 人员参与决策过程(例如改进网络安保意识培训方案的建议)；
b) 为人员分配足够的时间来完成适当的网络卫生培训；
c) 认可良好表现的机制(即激励和/或奖励方案)；
d) 就建议事项和网络安保报告向人员提供反馈；
e) 就网络安保事件设定明确、可实现和可衡量的目标，并定期向人员反馈组织在这方面的进展情况；
f) 提供必要的程序、意识、培训和工具，使人员能够履行职责；和
g) 为人员提供适当层级的自主权和责任。

— 完 —