RESOLUTION #4

Affirming airport’s commitment to addressing the evolving cyber threats in aviation

The Thirty-third ACI World Annual General Assembly:

Recognizing that the aviation industry heavily relies on interconnected systems and advanced technologies to maintain efficient, safe and secure operations;

Understanding that these systems may be vulnerable to cyber threats that can jeopardize the safety and security of passengers and staff, with damaging economic consequences and potentially significant adverse impacts on public trust and brand image;

Noting that the aviation industry is experiencing a rise in cyber attacks that are becoming more complex and widespread often targeting sensitive and confidential customer information, and critical operating systems leading to unprecedented service disruptions;

Considering that one of the critical vulnerabilities for an organization is the lack of cyber awareness by employees and the absence of an overall organizational cybersecurity culture;

Emphasizing that the use of proactive risk-based approaches for cybersecurity are crucial means to safeguard critical infrastructure and systems, protect sensitive and confidential data, and ensure public trust in the industry;

Understanding that in order to effectively address the growing cybersecurity risks and threats in the aviation industry, it is essential that all stakeholders involved work together in a spirit of cooperation and coordination;

Recognizing the commitment made by airports through Resolution *1/2018 An effective approach to cyber security* and the current efforts undertaken by industry as a whole, and by airports specifically, to address existing vulnerabilities and mitigate potential risks;

Recognizing that ICAO has placed Cybersecurity and Information System Resilience in Aviation as one of its core priorities and has established a new Cybersecurity Panel, in which ACI World is represented;

Noting the existence of a multitude of global standards for cybersecurity and the ongoing development of an aviation specific regulatory framework for cybersecurity both on a global scale through ICAO, and in regional contexts; and

Recalling that ACI World has been diligently working with members and the Airport IT Standing Committee on establishing guidance materials for airports to support their cyber risk preparedness and resilience, and has been actively contributing to the ongoing work at ICAO;

Resolves **that the General Assembly:**

a) calls on member airports to pursue existing efforts to strengthen the awareness on cyber threats to the industry and on the creation of a strong cybersecurity culture within their organization;

b) urges airports and all airport stakeholders to evaluate their level of risk and exposure to cyber threats and identify the appropriate mitigation measures that are needed to effectively reduce the risk, including incorporation of cybersecurity incident response and recovery plans into their emergency response procedures and business continuity plans;

c) urges States, International Organizations and relevant institutions to leverage the existing international standards and frameworks on information security and cybersecurity[1] in the development of aviation cybersecurity frameworks, standards and guidelines;

d) calls upon States and industry stakeholders to implement the necessary measures to support the development of a skilled aviation cybersecurity workforce by ensuring appropriate levels of funding, adequate training and career development opportunities for professionals in this field;

e) requests that ACI World work closely with ICAO, ACI Regions and other relevant institutions and organizations on the development and implementation of the appropriate aviation regulatory frameworks, focused on the challenges of the aviation and airport industry, including on specific regional needs, with the main objective of enhancing the overall sector's cyber-resilience;

f) encourages ACI World to continue its efforts to raise awareness across the industry of the rapidly increasing significance of cybersecurity for airports through appropriate communication campaigns, capacity-building initiatives and promotion of best practices and lessons learned among airports and other key stakeholders; and

g) requests ACI World to evaluate and potentially implement an information-sharing and collaboration platform for member airports and stakeholders to work together in identifying, assessing, and mitigating cybersecurity threats through an appropriate cyber risk management process for airports.

END

[1] Frameworks such as ISO 27001, ISO 27002, ISO 27032, NIST