ATTENTION – URGENT ACTION REQUIRED!

Windows 7 - End of Life (EOL)
Windows Server 2008 R2 - End of Life

The IATA Common Use Working Group met in Athens in October 2018 and agreed that IATA recognized common use standards used for passenger processing will not be supported on systems using the Windows 7 operating system as of January 14, 2020.

BACKGROUND:
When Windows 7 was released on October 22, 2009, Microsoft made a commitment to provide 10 years of product support. Effective January 14, 2020, Microsoft will discontinue its Windows 7 Extended Support. Microsoft will no longer provide technical assistance and security updates which are critical to help protect your PC against security vulnerabilities.

Microsoft strongly recommends Windows 7 users to migrate to the latest operating system, Windows 10, before January 2020 to avoid a situation where airports and airlines no longer receive any Microsoft support. Refer to the link for Support for Windows 7 is ending for additional information.

Windows Server 2008 was released in February 2008, but effective January 14, 2020, Microsoft will discontinue Extended Support of this version. As such, servers should be migrated to Windows Server 2016 (Server 2012 as a minimum) to provide the longest support timeline and to be compatible with Windows 10 clients (Common Use Terminal Equipment systems - CUTE), CUPPS and CUSS kiosks). More information about Windows Server 2008 is available at Windows Server 2008 End of Support.

Additional key milestones causing the need to migrate from Windows 7 to Windows 10 are:

- **Hardware Incompatibility**
  Intel discontinued the availability of the 6th generation of Intel chips used in the manufacture of PCs compatible with Windows 7 or Windows 10. Without these chips, PC manufacturers have discontinued supplying PCs that are compatible with Windows 7, and only produce PCs that are Windows 10 capable. As such, PCs are **not available** for replacements or to add to installations operating on Windows 7.

- **Financial Fraud and Cybercrime**
  Data and credit card breaches, identity theft, and loss of privacy - these incidents have become everyday news. Victims are agencies, financial services companies as well as passengers, airports and airlines. Over the last couple of years there have been a number of examples across multiple industries, including the Air Transport Industry, of data breaches involving personal and payment data of hundreds of millions of people, each causing additional costs for the company, and reputational damage. A breach of personal data also can result in penalties as defined by the General Data Protection Regulation (GDPR).

- **Payment Card Industry Data Security Standard (PCI DSS)**

- PCI DSS requires the system environment be maintained on the highest level of security (please refer to PCI DSS Quick Reference Guide version 3.2.1), to protect systems against malware and other vulnerabilities. This of course can only be met when using supported software including the provision of patches for operating systems and other third-party applications.
- Ensuring that systems have current patches is especially important where payments are accepted at airports. More and more CUTE, CUSS and CUPPS devices, including Self Bag Drops (SBD) offer payment services to passengers for ancillary services, thus exposing systems to higher security risks when using a magnetic swipe reader (MSR). Information about payment security is available at Card Payment Acceptance at Common Use Positions at Airports.
- Airports and airlines are keen to remove the kiosk, SBDs and agent desks from PCI DSS scope with its strong regulations and requirements for security. While use of an unencrypted MSR does not prohibit PCI compliance, it does require extensive changes and controls by airlines and airports to ensure PCI DSS compliance

IMPACT:

- Use of Windows 7 beyond January 2020 can expose all parties (passengers, airlines and airports) to security vulnerabilities, exposing passengers to data and credit card breaches, identity theft, and loss of privacy, as well as fines and reputational damage for the airports and airlines where Windows 7 is used after January 14, 2020.
- Airlines and airports may not achieve compliance to PCI DSS Requirement 6.2 when Windows 7 security patches are not provided due to the EOL of Microsoft Extended Support.

➢ **Declining Number of Applications Supported on Windows 7**:
Over time, a significant number of third parties, such as application providers, airlines, and their DCS providers, may no longer develop nor support applications for Windows 7 environments.

➢ **New technologies for Air Transport Industry Require Current Operating Environments:**
Going forward, new technologies will require or operate at a higher reliability or compatibility when using an updated and current infrastructure.

RESULT – ACTION REQUIRED:

It is of paramount importance that all parties create and follow a plan to migrate systems from Windows 7 to Windows 10 to reduce risks and costs of security breaches as well as operational integrity, that can occur when Windows 7 and Windows Server 2008, and other third party applications, are EOL.

➢ **Airports:**
- Meet with your common use provider to agree on a migration plan, which may include new hardware, as part of your contractual obligations. Plan to migrate from:
  - Windows 7 to Windows 10 on all workstations and kiosks
  - Windows Server 2008 to Windows Server 2016 (Server 2012 as a minimum)
- Meet with the operating airlines to set dates. Verify the airlines' plans include the migration of their applications to Windows 10.

➢ **Airlines:**
- Ensure your applications, whether developed in-house or externally, are ready for deployment on Windows 10.
- Ensure the application has **no reliance on 16-bit process or executables**. Current available workstations are 64-bit, but also support 32-bit processes and executables.