AIRPORTS COUNCIL INTERNATIONAL

The voice of the world's airports

ACI ADVISORY BULLETIN

Airport Information Technology recommendations during COVID-19

Montreal, 30 March 2020 – As the world grapples with COVID-19, Airports Council International (ACI) World has gathered the following Information Technology (IT) practices which are being implemented by airports around the globe.

In response to the rapid decline in traffic as a result of widespread travel restrictions and the health and safety implications of the spread of COVID-19, airports have had to reduce onsite staff (including IT) to essential personnel only, adopting emergency HR measures, and increasing the deployment of collaborative tools.

This advisory provides recommendations to help with this transition.

Build a strong collaborative team

The Air Transport Industry is highly dynamic environment which incorporates many disciplines. For this reason, it is imperative, especially during the COVID-19 crisis, that airports work collaboratively with other key stakeholders to modify – or develop new – processes to maintain a safe environment.

Activating the Executive Crisis Management team is essential, and IT must be a part of this group as it plays a critical role to ensure operations, communications, and business can continue.

Taking a crisis team approach, incorporating clear communications, will also help to ensure business continuity planning, where the sharing of responsibility for essential functions among airport business units and employees, contractors, tenants, and federal agencies is clearly understood. Airports can make use of emerging and existing technologies to help facilitate all of these efforts.

In addition to the airport crisis management team, airports should establish an IT response team. This should be done even where the airport operator is only partially responsible for IT infrastructure. This multi-disciplinary team should comprise representatives from all entities providing services at the airport in order to validate IT business continuity plans, or to create one.

Once the team is formed, a schedule of frequent meetings should be established (once a week, for example) so that information about airport technology systems can be shared, goals and objectives discussed, and decommissioning/recommissioning plans considered. Meetings can take place virtually.

Working in collaboration, this team must identify the tasks to be accomplished during the management of the pandemic. In an aviation ecosystem context, a business continuity plan is only effective if it is known, understood, and applied by all.

Ensure effective and secure IT infrastructure for remote access

IT infrastructure is key to helping airports operate efficiently. It underpins all airport critical systems and services which are key to not only the airport staff, but also airlines and other organizations at the airport. It supports a smooth and hassle-free passenger journey and allows airports to communicate the latest information. In response to this pandemic, airports must ensure that their IT infrastructure is able to handle new demands, especially the provision of increased remote access for staff.

The most effective way to control the spread of COVID-19 is to limit physical contact so the introduction of telecommuting/teleworking wherever possible is an important element of any business continuity plan.

In this scenario, only limited number of employees would be available onsite to support the IT infrastructure, including maintaining servers, critical hardware, and software. The plan must, therefore, include a work from home procedure that provides instructions and information regarding remote access to all, or most, systems and tools. This procedure must be validated and approved by the airport executive management including, but not limited to, the Chief Executive, Human Resources, and Finance.

Safe and secure connectivity may be offered via Virtual Private Networks (VPN), and cloud-based solutions which require only simple internet connections. This method does not connect the remote worker to a specific computer in the office but rather to the airport network and programmes in general. It is imperative that the airport VPN service is patched and up-to-date, and that the proper security measures are in place.

Whether the airport provides a laptop, allows the employee to take home a desktop computer, or encourages use of home devices, specific programs and applications that are critical to conduct business should be identified and made accessible. IT should then put into place the proper login and secure connectivity access, and data-saving capabilities.

During this pandemic, it is important for managers to keep in touch with their teams and industry colleagues to keep everyone informed and to prevent isolation. In order to facilitate daily crisis or periodic team meetings, use any of effective web programmes such as, but not limited to, Webex, Microsoft Teams, Zoom, Yammer Groups, or Skype; all provide a way to for teams and personnel to stay connected and up to date.

Airports should also establish ongoing communications with their critical vendors using collaborative IT tools and be assured that they have their own effective contingency plans in place.

System shut down, back up, and restoration

In the event that some areas of the airport terminal (or entire terminals) need to be closed, the Business Continuity Plan should include clear procedures and protocols to shut down hardware and software programmes being used during normal operations. These systems may include passenger and baggage processing systems, building maintenance, docking systems, security check points, access control, and the like.

IT teams must be ready to decommission systems as required and ensure that all historical data has been saved (and application logic preserved), affected parties are appropriately notified, and maintenance of hardware and software is conducted in compliance with established regulation.

Some airports around the world are reducing operations in their terminals but keeping the systems “live” and hardware operating. This is another option to ensure the systems are in good order when it is time to restore them to normal operations.

During reduced operations, a number of airports are electing to do some system maintenance and upgrades that would normally have to be done during nighttime hours or when the terminal is not in use. These should be considered, especially if they do not require onsite personnel (software upgrades and remote diagnostics, for example).

Establish a common information sharing approach

During the COVID-19 pandemic, airports must work with health authorities to make the most up-to-date information available and accessible. In addition, the various stakeholders in the ecosystem must ensure that they provide the right information to passengers in the event of terminal (or airport) closures or restricted access to certain areas of the airport.

With much information on the web and social media, it is very important that the information shared among the community is accurate and consistent. This is not easy, but leveraging the airport’s social media teams - and software programs that monitor posts - can help.

Airports also need to ensure that the message is consistent across all communication channels, such as social media, the airport’s website, physical screens on site, signage, and recorded voice message.

Implement Cyber resilience for business continuity

Following many government mandates for people to work from home due to COVID-19, airports are faced with additional cyber security risks, and data breach challenges. For this reason, addressing cyber security for not only the airport systems but those of

airlines, tenants and possibly passengers who might be using the airport infrastructure, must be included in the Business Continuity Plan.

It is imperative to have and update cybersecurity policies and procedures. These should be made available and apply to not only the IT and cybersecurity personnel, but the workforce in general.

Phishing campaigns that use messages purporting to be from the World Health Organization (WHO) and governmental representatives have been widely observed. In some cases, legitimate documents and information are being used. Once a link is clicked or the file is opened in such messages, a macro is triggered that installs malware into the system without the victim being aware that they have been infected.

In response to several scammers trying to take advantage of COVID-19 fears, all staff are recommended to be careful more than ever with what they download. There are many legitimate websites with accurate coronavirus information including the World Health Organization the Center for Disease Control and Prevention, ICAO, and, of course, national and local public health authorities.

Good cybersecurity hygiene practices should be communicated to all staff, such as making sure that the sender is who they say they are, using alternate ways of communication or reporting suspicious emails to the IT/cybersecurity team.

Some cybersecurity best practices to follow are:

- **Policy**: review current policies to make sure there are established guidelines for remote work and remote access to airport systems.

- **Communication**: management should be familiar with applicable security guidelines, plans and polices and ensure that the correct information and channels of communications are being used throughout the organization to disperse as well as receive information.

- **Training**: employees should be trained on cybersecurity issues related to working remotely. This should focus on the risks, threats and vulnerabilities of remote working, the impact on themselves and the airports and the actions required to mitigate them (phishing, social engineering, and the like).

- **Secure Networks**: secure networks should be established so devices and connections only use them. This could include using dedicated VPN and ensuring that they are up to date with the latest updates, as well as securing home WIFI routers, devices and connections.

- **Information**: revisit and limit access to protected information remotely to only personnel that absolutely require them. Remind employees of the type of information that they need to safeguard. This often includes confidential information such as access credentials, financial information, employee

information, customer information and any other information deemed sensitive. While storing or transferring such information from remote devices, data should be encrypted and sent via secure connections.

- **Detect, Response and Recovery**: attacks are threats that have been realized, whether they have been successfully averted by countermeasures or not. Those that have been averted should be noted so that trends can be identified. Successful attacks that have not been averted require immediate response. After the organization has recovered, additional countermeasures should be put in place to ensure that the uncovered vulnerability is addressed.

It is critical that cybersecurity is not only seen as an information technology concern, but rather a strategic risk that can quickly become a critical operational, safety, financial or reputational issue.

ACI therefore advocates for a management systems approach to cyber security, with buy-in and engagement from senior management, with good cybersecurity practices reflected throughout the organization

Deploy Innovative technologies and solutions for self and autonomous operations

During this global disruption airports have been forced to reconsider their normal business and operational processes, including how to use technology. For this reason, airports are considering what adjustments can be made for the post-COVID-19 environment.

Health screening is likely to become the new normal. Many different solutions are being deployed, and further work is required to determine the most efficient and effective best practices. This may also be the time to consider solutions for truly autonomous, hands-free passenger self-processing throughout the journey.

This advisory bulletin is intended to provide ACI airports members with a set of important key actions for addressing IT concerns during this pandemic crisis. Today, airports are focused on business continuity, but they will soon be considering how to manage the business impact in preparation to accelerate the growth. These key topics will be covered in later advisory bulletins.

Ends

1. Airports Council International (ACI), the trade association of the world's airports, was founded in 1991 with the objective of fostering cooperation among its member airports and other partners in world aviation, including the International Civil Aviation Organization, the International Air Transport Association and the Civil Air Navigation Services Organization. In representing the best interests of airports during key phases of policy development, ACI makes a significant contribution toward ensuring a global air transport system that is safe, secure, customer-centric and environmentally sustainable. As of January 2020, ACI serves 668 members, operating 1979 airports in 176 countries.