

This is a brand-new Article that was necessary as we are moving into a more technologically advanced world. Your Negotiating Team saw the need to have contractual protections for items like expectations of privacy and for use of SWA apps on your own personal device. This Article also establishes a subcommittee to ensure all the contractual provisions related to “the system” are met and the intent of negotiated language is followed.

ARTICLE 36

TECHNOLOGY SECURITY AND PROTECTIONS

1. Expectation of Privacy

Flight Attendants will have an expectation of privacy in their use of the Inflight Electronic Flight Bag (IEFB) for personal, non-work purposes in accordance with the terms in this Article and the Company’s Information Security Policy (ISP). The Company considers the IEFB to be a Company owned device for Flight Attendants to perform their jobs, but a Flight Attendant may choose to use it for personal purposes with the following protections:

- A. The Company will not track a Flight Attendant or the location of the IEFB device unless the Flight Attendant opts in to mapping capabilities. Flight Attendants may elect to set up “find my device” or geo-location capabilities on their device for their own personal use, but Southwest will not use those capabilities to track Flight Attendants or their devices.
- B. The Company will not review, access, collect, or use data related to a Flight Attendant’s non-work related data on, and personal use of the IEFB (including, the types of apps installed on the device, app inventory, electronic mail, personal data and content, PIN, GPS location, and statistical data such as the number and duration of phone calls, number of text messages, whether or not the device is roaming, and search history).
- C. Device logs will be visible to the Company during maintenance or repair of the IEFB but will not regularly be viewed or used for any other purpose.
- D. The Company will not remotely collect device logs via the Mobile Device Management (MDM) agent app (no website tracing, etc.).
- E. The Company will not remotely wipe a Flight Attendant’s personal data on the IEFB without first advising the Flight Attendant.

- F. Flight Attendants may choose to carry a second device. If a second device is confiscated by a government authority due to limitations on the number of devices a Flight Attendant can bring into a specific locale, the Flight Attendant may choose to turn over the Southwest IEFB device as the second device. The Company will be responsible for any fines associated with the second device and will not seek reimbursement from the Flight Attendant for such fines or the replacement cost of the confiscated device. Flight Attendant will not be subject to discipline or discharge for any fines or government confiscation of the IEFB.

2. **On-duty and business-related usage of IEFB**

Each Flight Attendant is provided a functioning IEFB, maintained by the Company, for work related duties and communication. Provisions of the Southwest Airlines Information Security Policy govern Flight Attendants using the IEFB for business purposes. Flight Attendants need to be aware that the Company has visibility to the following:

- A. Mobile Device Management (MDM) managed apps and the versions of those apps;
- B. Device Identifier (UDID), and the device serial number;
- C. Battery charge;
- D. iOS version;
- E. Type of iPad;
- F. Installed Southwest Airlines profiles and certificates; and
- G. TWU 556 will retain “Read Only” visibility to the MDM dashboard to maintain transparency.

3. **Southwest Mobile Applications on Personally Owned Devices.**

- A. Flight Attendants can download to or remove SWA Crew applications from their personally owned device(s) at their own discretion.

- B. The Company will not ask Flight Attendants to turnover or provide access to a personally owned device unless it is legally required.
 - C. If a Flight Attendant enables Location Services for a SWA Crew Application on a personally owned device, e.g the Airport Maps feature in CrewHub, the device location is not accessible to the Company.
 - D. Southwest Technology teams may access information on a personally owned device when it performs error logging and reviews application performance statistics to help diagnose issues with SWA Crew applications.
 - E. For technical support, Southwest may collect certain information such as IP address, operating system, browser version, and transaction logging when a personally owned device is connected to SWA systems.
 - F. Southwest Technology teams monitor usage analytics (which are de-identified) of the SWA Crew applications to introduce new functionality and improve user experience.
- 4. If the Company extends additional data privacy or information security protections to any other crew work groups related to workplace devices used by the Flight Attendants to perform duties, if applicable to the Flight Attendants, they will be offered to the Union, and if accepted by the Union, such protections will be incorporated into this Agreement.
 - 5. The Company's intent is to provide clarification to Flight Attendants that their personal data is safe and secure when using SWA Crew applications. A Flight Attendant's personally owned devices are just that - personally owned. Southwest respects a Flight Attendant's privacy and ability to choose what is installed on his or her device.

6. **JOINT TECHNOLOGY IMPLEMENTATION SUBCOMMITTEE**

The parties acknowledge that in certain parts of this Collective Bargaining Agreement there are planned technology tools and applications, some of which have yet to be developed. The parties will meet to ensure that the parameters for the technology tools and applications to be developed are consistent with the terms of the Collective Bargaining Agreement.

- A. In addition, within thirty (30) days of ratification, the Joint Technology Implementation Subcommittee "JTIS" will be created with the goal of providing feedback and guidance to ensure contractual provisions are met.

The JTIS will aid in the facilitation of the Company's implementation of technological systems (referred to as "the system") including, but not limited to messaging, notifications, reserve components and other electronic means designed to replace current phone communication methods.

- B. The Subcommittee will be comprised of a limited number of Members appointed by the Union and the Company. The Members attending a Subcommittee meeting may vary depending on the subject matter being addressed. The Union and the Company will continue to meet as needed.