Last Revised: 4/1/2024

To: CEO, Starfall Airlines

From: Noah Barrall, Information Security

Subject: PL Family Implementation

The purpose of this document is to provide a detailed overview of the PL (Planning) control family's significance within Starfall Airline's vision and operational framework.

The overall risk of the system has been identified as High per the CIA triad:

- Confidentiality: **High**
- Integrity: **High**
- Availability: **Medium**

Following the NIST 800-53, we are proposing implementing the following controls into the system to maximize productivity and efficiency while planning:

- PL-2: System Security and Privacy Plans
- PL-4: Rules of Behavior
- PL-8: Security and Privacy Architectures
- PL-10: Baseline Selection
- PL-11: Baseline Tailoring

PL-2 deals with developing, distributing, reviewing, updating, and protecting security and privacy plans for our current system. We are proposing the following organizational assignments:

- Include policy development, risk assessment, data protection, privacy compliance, incident response planning, and other related activities that require system planning and coordination with:
    - Information Security Teams, CISO, Legal Team, Human Resources
- Distribute copies of the plans and communicate subsequent changes to the plans to:
    - Executive Management, Information Security Teams, Human Resources, All Department Heads
- If there have been no changes to the plans, review them quarterly. If the plans have been changed, review them upon revision, as well as quarterly.

PL-4 pertains to creating rules that describe individuals' responsibilities and expected behavior while using the current system. We plan to implement the following assignments:

- Review and update the rules of behavior annually.
- Require individuals who have acknowledged a previous version of the rules to read and re-acknowledge one time a year when the rules are revised or updated.

PL-8 is a major factor in our system as we will be implementing controls to protect the information of our organization and customers. This architecture will reflect our

enterprise architecture, as well as external systems and services. We will be implementing the following:

- Review and update the architecture twice a year to reflect changes in the enterprise architecture.
- Allocates access control (multi-factor authentication and role-based access), data security controls (encryption), and incident response procedures to airport terminals, data centers, and corporate offices.
- Require that our firewalls, intrusion detection systems, encryption technologies, and access control systems allocated to the airport terminals, data centers, aircraft systems, and corporate offices are obtained from different suppliers.

PL-10 is what we will use to select the base controls for our system. Implementing this control will allow us to select the correct controls for the protection of our system. The controls chosen will satisfy:

- Mandates imposed by law
- Executive orders
- Directives, regulations, policies, standards, and guidelines

These baselines represent a starting point for the protection of individuals privacy and information, with the selection of the controls being determined by the stakeholders.

PL-11 plays off PL-10. Upon selection of the baseline controls, PL-11 allows for tailoring of controls specific to organizational needs. This allows our organization to develop security and privacy plans that reflect our business functions. For example:

- AC-6, Least Privilege grants users the minimum access necessary to perform their job while ensuring integrity.
    - For the sake of Starfall, we can tailor this to allow for Role-Based Access Control, Access Reviews, and allow for Data Integrity Considerations.

Implementing the five previously listed controls will significantly enhance the security and privacy posture of Starfall Airlines, aligning with industry best practices and regulatory requirements. This comprehensive approach will safeguard sensitive information, protect our passengers and employees, and ultimately maintain the trust of our customers and stakeholders.

Signature: _____ Date Signed: _____