Regulations Search

Proposed by: Ethan Santoro and Noah Barrall
Proposal Date: February 5 2024

Legal Authorities and Reasons to Comply

Cybersecurity regulations listed in both the Federal Aviation Administration, Transportation Security Administration, and the National Institute of Standards and Technologies must be complied with at all times in order for Starfall Airlines to remain functional as a business. There are many reasons Starfall must comply with these authorities. Examples of these include public safety, such as preventing physical harm and terrorism, as well as maintaining industry wide standards and a good reputation to the public. More importantly, data security, dealing with personal data and preventing unauthorized users from accessing the data tends to be the most important reason to comply with legal authorities. Failure to do so can result in fines and criminal charges.

Regulations In Use and How to Obtain Them

The regulation that applies to our current model is the National Institute of Standards and Technologies(NIST) Cyber Security Framework 800-53, found on the company's website. Instances of these standards are broken down into multiple sections, the first of which is Identify. This deals with Governance (ID. GV), Risk Assessment (ID. RA), and many more topics. The first of these principles dictates that policies and procedures used to manage all legal and operational requirements should be understood and that management is always informed of cybersecurity risks. The second example delves deeper into the previous section, confirming that our organization understands all cyber-related risks. Furthermore, the Protect segment enforces the protection of data, with Data Security (PR.DS) mandating that all information and records are managed with consistency in regards to our company’s risk management policy. While obtaining these controls is not something that needs to be done, they are to be taken into account and implemented properly.

Impact Regulation has on Cyber Defense

The NIST 800-53 sets the standard that asset vulnerabilities, threats, and business impacts are both identified and prioritized. Implementing intrusion detection and vulnerability management will help identify threats, minimizing potential damage. The regulation also sets high standards of protecting data both at rest, and in transit, causing the team to have to implement protocols with higher security levels. Additionally, measures must be taken that restrict unauthorized users from accessing important systems. Furthermore, monitoring is now required to ensure that policies and cybersecurity defense systems are always up to date.

How the Impacts Look Practically

In a practical manner, Starfall Airlines' cybersecurity team will be focusing mainly on network segmentation. Working on dividing networks into smaller segments that will limit the damage attackers are able to do, as well as keep critical systems safe. In the event that a system is accessed, we must develop and test a proper incident response procedure. Basic steps to start this plan include implementing Multi-Factor authentication, as well as assigning roles to personnel responsible for certain tasks. Another way this regulation can be practically implemented would be to keep track of and review access control of all users in the system monthly. Finally, a very important aspect of encryption and classifying data will be dealt with to reduce the risk of data breaches.

Why This Regulation is in Place

These regulations are in place in order to ensure the safety of all people operating in the business, whether it be employees or customers. Unfortunately, airplane accidents can happen quite often, and therefore it is our goal to take every possible measure to minimize and avoid any type of risk when it comes to aviation. To start, the security of all people should be at the forefront of our airline, and that starts protecting their personal information such as financial, personal, and professional data. If a data breach were to occur, customers would be hesitant to deal with our airline anymore, knowing that we allowed their data to be stolen. This regulation is set in place to protect both our company and our customers. While protecting the users of our services is our main concern, especially dealing with aircrafts and very sensitive systems, we also want to keep our company afloat to keep providing these services.

Penalties for Non-Compliance

Given that the 800-53 Cyber Security Framework is not legally required, it does not have any consequences, but the FAA and TSA do. The consequences for breaking these guidelines range from having pilot’s licenses revoked to imprisonment. Naturally, hefty fines can be handed out for failing to comply with these rules. On top of this, the reputation of our business would certainly decline if regulations were to not be followed, and therefore we enforce strict compliance at all times.