ATPCO Information Security Compliance

December 2023

Airline Tariff Publishing Company (ATPCO) is the foundation of modern airline retailing, enabling you to get the right offer to the right customer at the right time.

Owned by airlines, ATPCO blends reliable data and systems with innovative technology so we can create value for everyone.

Document Scope and Use

This document is designed to provide ATPCO customers with an overview of the implemented security controls which are designed to protect ATPCO customer and employee data from unauthorized access or compromise. We are continuously improving the protections that have been implemented and in keeping with that objective, the content of this document (including any related communications) is not intended to create a binding or contractual obligation between ATPCO and any parties, or to amend, alter or revise any existing agreements between the parties.

How To Contact Us

Should you have any questions about ATPCO Information Security Controls, please contact us via one of the following methods:

- **Message us:** **https://atpco.service-now.com/sp**
- **Phone:** **+1-703-661-7400**
- **Mail:** Airline Tariff Publishing Company
  Washington Dulles International Airport
  45005 Aviation Drive, Dulles, VA 20166

For information regarding ATPCO privacy controls, please refer to:
https://www.atpco.net/privacy

Table of Contents

Document Scope and Use 1

How To Contact Us 1

ATPCO Security and Risk Focus 4

ATPCO Information Security Controls 5

Information Security Policies 5

Human Resource Security 6

Security Awareness Training 6

Asset Management 6

Cloud Infrastructure Security 7

Network Infrastructure Security 7

Endpoint Security 8

Backups and Backup Strategy 8

Logging, Monitoring and Alerting 9

Change and Release Management 9

Configuration Management 10

Infrastructure / OS Patch Management 10

Software Development and Maintenance 10

Vulnerability Management 11

Penetration Testing 11

Physical Security 11

Identity Management and Access Controls 12

Incident Management 12

Data Breach Notification Procedures 12

Business Continuity 13

Disaster Recovery 13

Encryption and Key Management 13

PII Data Protection 14

Downloads 15

Compliance FAQs 16

ATPCO Security and Risk Focus

Since information and information resources are strategic assets vital to ATPCO's business, this requires that these resources be protected from unauthorized access or modification. ATPCO has been certified as meeting all the requirements for implementing and maintaining effective information security controls per:

- the Payment Card Industry Data Security Standard (PCI-DSS)
- the International Organization for Standardization ISO 27001 / ISO 27701 Information Security Standard
- the EU General Data Protection Regulations (GDPR)
- EU-U.S. PRIVACY SHIELD FRAMEWORK

In addition to industry standard information security certifications, ATPCO conducts its own security assessment and utilizes third-party risk assessment services to independently assess the security posture of its applications and services. If there are any significant changes to the ATPCO computing environment which could affect the security of customer data, we will notify affected parties via the standard ATPCO industry bulletin notification process. Any security deficiencies identified will be remediated by ATPCO in a reasonable time frame as conditions allow.

ATPCO will not permit nor authorize ad hoc audits by customers or customer representatives of our sites, facilities, systems, or security controls. Additionally, Customers / Vendors may not perform any security testing of ATPCO's application or services without prior written approval from ATPCO, which may be withheld.

ATPCO Information Security Controls

To protect the data that is entrusted to us, ATPCO utilizes a defense-in-depth approach to implement layers of security controls throughout our entire technology stack and all layers of business processes.

Information Security Policies

ATPCO has implemented a comprehensive set of information security policies which reflects the requirements and standards of ISO 27001 / ISO 27701, the Payment Card Industry Data Security Standard, and information security best practices. These policies are reviewed, approved, and updated at least annually.

Third party entities providing services to ATPCO must ensure their supplier contracts include responsibility for information security controls. Additionally, where applicable, third-party entities are required to provided evidence of security controls such as a security certification (e.g. PCI, ISO 27001, etc.)

Cloud Services and Hosted Services providers must provide evidence (e.g. ISO / IEC 27001 certification) which demonstrates that the service provider has proper controls in place to protect customer data.

Additionally, where Cloud or Hosted service providers store or process personally identifiable information (PII) on behalf of ATPCO, evidence of controls for protecting PII data in public cloud environments (e.g., ISO / IEC 27017 certification) must be provided.

Human Resource Security

All prospective employees undergo professional reference checks. Any candidate who will have access to credit-card data will be subject to an extensive third-party pre-employment background check. Additional background screening is conducted as necessary dependent on the position of the candidate, for example Directors and Officers.

Upon hire, employees are required to read, acknowledge, and agree to abide by the ATPCO Information Security policies.

ATPCO has a strict on-boarding/off-boarding process with an established workflow for account provisioning, for requesting access to systems and data, and for revoking access upon termination.

Security Awareness Training

ATPCO considers employees to be our first line of defense against cyber threats and we ensure that employees are well trained for their respective roles. All new hires must undergo security awareness training that covers general information security best practices. Additionally, more specialized security awareness training is provided on an ongoing (at least annual) basis, covering such topics as secure software development, common risk, threats, and handling sensitive information.

Asset Management

ATPCO is committed to the protection of its information assets and maintains an accurate asset inventory that is monitored and audited at least quarterly.

All new assets (software and/or hardware) are assigned a designated owner and recorded in the asset inventory to deployment. Additionally, hardware assets are labeled with an “ATPCO” asset tag.

Additions or removal of any registered asset requires documentation within the ATPCO ticketing system. Retired assets (for example, hard drives) are removed from inventory and securely wiped prior to disposal. In the case of sensitive data, the media is destroyed and verified via a certificate of destruction.

Cloud Infrastructure Security

ATPCO does not host any products, systems, or services within its corporate offices. ATPCO outsources hosting of its infrastructure to several leading cloud infrastructure providers:

- **Public Cloud**
  - guarantees between 99.95% and 100% service availability and ensures redundancy to all power, network, and environmental services.
  - resides in multiple local and international regions.
  - is fully certified and audited to verify compliance with physical, environmental, and infrastructure security protections.
  - has business continuity and disaster recovery plans which have been independently validated as part of SOC 2 Type 2 and ISO 27001 certifications.

- **Private Cloud**
  - operates as a monthly subscription model which provides fully managed hosting and guarantees 99.5% availability.
  - provides redundant infrastructure in the US East and Midwest
  - maintains an audited security program which is validated by the PCI-DIS Attestation of Compliance (AoC) and ISO 27001 Information Security Certification

Network Infrastructure Security

ATPCO employs state-of-the-art, layered firewalls to protect and control access to its internal resources. Encryption (SSL/TLS) is enabled for all credentialed access to ATPCO systems and applications. Network-level access and remote administrative access require two-factor authentication.

All confidential and sensitive data is transmitted via SSL/TLS/SSH. While at rest, confidential and sensitive data is either encrypted or protected by additional layers of access control which require approval for access.

Firewall rulesets are reviewed on an annual basis to help ensure that only necessary connections are configured and that configurations meet established configuration standards (such as PCI-DSS, CIS, etc.)

Endpoint Security

Where technically feasible, all ATPCO endpoints are configured with an Endpoint Detection and Response (EDR) solution which provides for real-time prevention, detection, investigation, and response to cybersecurity threats.

Endpoint Management
All endpoints are managed via the implemented Mobile Device Management (MDM) solution.
For security policy compliance, each device is configured with a list of profiles (device configuration, security, etc.).

Endpoint Operating System patching
All Operating System updates and version upgrades are applied via the implemented MDM solution. Endpoints must scan for and automatically install updates during the configured maintenance window. If an update is available through an update policy, the device downloads and installs the updates automatically.

Endpoint Compliance
Access to internal protected and sensitive resources is restricted to ATPCO managed and compliant devices. Employee-owned devices are only permitted access to selected non-sensitive data and systems via a secure web browser or smartphone app.

Backups and Backup Strategy

ATPCO databases are configured with automated backups for data protection and recovery.

For databases hosted on public cloud platforms, Production cluster backups are enabled both on primary and secondary regions to ensure backup data is available in case of a need for point-in-time recovery. Databases are backed up using native solutions on the hosting platform which provides daily snapshots and archive logs that are kept for at least 15 days for point-in-time recovery.

In the event of a disaster, a new database instance is configured with the pre-determined point-in-time recovery window for use by ATPCO applications.

For databases hosted on private cloud platforms, continuous replication of Production data is configured between our primary and secondary hosting facilities, providing for very low Recovery Point Objective (RTO) points of seconds to within a few minutes in the case of a Disaster Recovery (DR) event.

Production Database backups are taken once per day and follow a 14-day rotation schedule. For non-production data (i.e., development, test), backups take place once per week and follow a 14-day retention/rotation schedule.

Logging, Monitoring and Alerting

Logging is enabled via standard configuration of all network devices, hosts, and endpoints, and includes details such as Username / UserID, timestamp, system / application/ host being accessed, and the result of the access attempt (success for fail). Additionally, all end-user log-on activity is logged, and logs are maintained for at least 90 days.

The infrastructure is instrumented to alert operations control staff and administrators when anomalies occur, such as incident alerts, network attack or established error thresholds are exceeded.

Change and Release Management

The ATPCO Production Systems are critical enablers to provide the services that are the core of our business. As such**,** changes to ATPCO Production Systems are necessary to accommodate the introduction of new functionality and enhancement to existing functionality. ATPCO has implemented a formal Change and Release Management policy that requires management approval for all system configuration changes or application updates. The purpose of the Change and Release Management process is to manage changes to configurable items and software environments in a controlled and predictable manner to minimize the risk of adverse impacts to ATPCO business operations.

All changes to the Production environment require a request in the ticketing system that describes the requested change, identifies affected components, and includes a back out plan to restore systems and applications to their previous state in the event the changes results in a service disruption. All changes are scheduled on the weekly Forward Schedule of Releases (FSR) and are reviewed during the weekly Change Advisory Board (CAB) meeting.

Release Management evaluates entries on the FSR, evaluates risks and / or potential conflicts for items included on the FSR, and coordinates all scheduled releases via the weekly PROD Readiness Meeting.

Any Emergency Change which is required outside of the FSR / CAB process, must undergo an independent review process, and must be approved by the CTO or a Technology Director before implementation. Post implementation, Emergency Changes are required to go through a root cause analysis and review at the next scheduled CAB meeting.

.

Configuration Management

Server instances are tightly controlled from provisioning through deprovisioning, ensuring that deviations from configuration baselines are detected and remediated. All server type configurations are embedded in images and configuration files. Server-level configuration management is handled using these images and configuration scripts when the server is built. Changes to the configuration and standard images are managed through a controlled change management process. Each instance type includes its own hardened configuration, depending on the deployment of the instance.

Infrastructure / OS Patch Management

For servers and hosts, Patch Management is implemented using automated patch management tools.

Back-end services and servers are patched monthly for Critical and Security Patches, Update Definitions, and Update Roll-Ups. Critical Servers are in Availability Sets so one will always be available while the other is being patched.

For hosts on our Public Cloud Platform, Critical and Important Security patches are applied daily.

Additionally, all ATPCO system software is patched on a regular cycle. All critical system security patches/updates are installed within 30 days of release.

Software Development and Maintenance

All ATPCO systems are developed leveraging Agile methodology. In keeping with this strategy, ATPCO has implemented a Shared Accountability Model for Technology Governance and established a Shared Accountability Management Committee (SAMC). These two approaches:

- address foundational requirements for Software Development.
- establish agreed upon policies, standards and guidelines that are to be followed in development and operation of ATPCO software products.

Additionally, all ATPCO developers must undergo training for secure coding principles upon hire and annually thereafter. All software testing is conducted in a non-production environment and tests in non-production environments do not use live production data. If there is a justified need for testing with production-like data, the data is sanitized in a way to make it impossible to identify sensitive data.

Vulnerability Management

ATPCO performs regular (at least weekly) vulnerability scanning against all public Internet-facing hosts using automated vulnerability assessment tools. Internal hosts are continually assessed for vulnerabilities utilizing installed agents. Any identified vulnerabilities are remediated via established procedures.

If a critical security vulnerability is disclosed, but the vendor has not released a patch, a suitable available workaround will be devised, tested, and applied to mitigate any risk or threat in the interim period.

All production baseline builds are scanned for security vulnerabilities against a standard framework such as the OWASP Application Security Verification Standard using a static application vulnerability scanning tool.

Penetration Testing

ATPCO maintains an up-to-date threat model for all infrastructure platforms and data repositories. Penetrations Tests are conducted against network infrastructure components and business applications at least annually by independent third-party service providers as well as by ATPCO professional staff on an as needed basis (e.g. when there are significant infrastructure or application changes).

Following the third-party Penetration Test any critical vulnerabilities discovered will be promptly addressed or mitigated using the documented vulnerability management procedures.

Physical Security

Physical access to facilities is controlled by an electronic card key system. Access cards with photo identification are only issued to employees and long-term contractors. Access to the most secure environments is only granted to employees with elevated privileges. Access is also monitored and recorded via an electronic surveillance system.

Physical access rights are granted only based on authorized request and on business need.

All guests / visitors to ATPCO buildings and facilities must be registered in the visitor management system prior to their arrival. Registered guests must always wear visitor badges and be accompanied by a representative of ATPCO.

Identity Management and Access Controls

Each user (employee, contractor, or customer) is assigned a unique user ID for system access.

Password controls are enforced for complexity and account lockout via the security system on all platforms. Initial passwords are randomly generated and communicated securely to the authorized user. User accounts are revoked upon termination. Access to systems in controlled via a formal request process. Inactive accounts are regularly reviewed and deleted. System and session timeouts are employed for unattended systems.

Logical access to data is restricted by layered security controls, and all access is monitored/recorded and logged. Access lists are periodically reviewed for accuracy and consistency. Personnel are only granted access to systems and data based on their role and job responsibilities and this is strictly enforced by our systems security server with a default “deny all” rule.

Incident Management

ATPCO has implemented an Information Security Incident Response Plan to respond to any breach of ATPCO information security controls which could result in destruction, loss, alternation, disclosure, or unauthorized access to, ATPCO systems or data.

Upon detection, Incidents are categorized based upon the type of incident and prioritized to determine the response time objective. The response plan prioritizes limiting the scope of the incident and includes containment and remediation steps to restore normal business operations.

Data Breach Notification Procedures

In the event of a data breach, ATPCO has well-defined process for notifying affected individual and relevant authorities. Depending on the type of incident, a communication escalation plan is followed to determine notification requirements in the event of a data breach. Affected customers must be notified within 48 hours, advising them of the breach and the steps ATPCO is taking to contain the event and limit data loss or exposure. All external communication with customers must be approved by executive management and coordinated via the Marketing Communications team.

Business Continuity

ATPCO has established a Corporate Business Continuity Plan (and subordinate plans at the corporate, divisional, and location specific levels) which are designed to maintain and resume business processes during any event which disrupts business operations.

The plan defines and ranks in priority those data systems/resources and business processes that are critical to ATPCO ongoing operations and establishes procedures for the prompt resumption of business functions in case of disruption.

ATPCO Business Continuity plans are reviewed and tested / validated at least annually to ensure ongoing availability of business services and data for all customers, as well as to proactively minimize the impact of any security risk which would threaten service availability.

Disaster Recovery

The ATPCO computing environment consists of outsourced / cloud-hosted infrastructure supported by leading public and private cloud infrastructure providers.

For applications hosted by our private cloud service provider, our disaster recovery strategy includes live data replication to our secondary data center location with the ability to restore normal operations (RTO) within 8-hours with minimal data loss (RPO of 10 minutes or less).

Our secondary data center also provides full capacity to run the ATPCO normal production business transaction load so we can operate with no degradation of performance for our customers.

For applications hosted on our public cloud platform, ATPCO has standard procedures to failover to a secondary region in the event of a disaster. The secondary facility provides capacity to fully support these applications without any service degradation or reduced performance for our customers.

Encryption and Key Management

All sensitive interactions with ATPCO products, applications, and services (e.g. API calls, authenticated sessions, etc.) are encrypted in transit with TLS version 1.2, or 1.3 and 2,048 bit keys or better.

Encryption keys for both in transit and at rest encryption are securely managed by ATPCO.

Encryption keys and TLS certificates are rotated / renewed at least annually.

All encryption is implemented using NIST approved cryptographic modules. Ciphers for symmetric encryption include AES-256 and above with key lengths of at least 256 bits.
Asymmetric encryption is implemented with a minimum of 1024 key length.

PII Data Protection

ATPCO only collects essential Personally Identifiable Information (PII) which is required to provide business services to our customers and employees. Employees are prohibited from storing PII data on personal mobile devices. Only company issued devices with a digital security certificate are permitted to access the ATPCO secure data environment.

ATPCO has implemented a three-tier Data Classification system for handling data. This includes classification of Public, Sensitive, and Confidential data categories.

No proprietary and/or confidential documents are left on employee desks in plain sight.

Downloads

ATPCO Information Security and Compliance Standards (link to PDF version of this document)

PCI Attestation of Compliance

ISO 27001 Certification

ISO 27701 (PIMS) Certification

ATPCO Data Privacy Framework Certification

Compliance FAQs

1. **What information security standards does ATPCO comply with?**
   ATPCO complies with the Payment Card Industry Data Security Standard (PCI-DSS) as a Level 1 service provider, the International Organization for Standards ISO 27001 and ISO 27701 Information Security Standards, and the US Privacy Shield Framework.

2. **What Privacy standards does ATPCO comply with?**
   ATPCO complies with the EU General Data Protection Regulations (EU-GDPR) and ISO / IEC 27701 Data Privacy Framework.

3. **Where does ATPCO store and process its data?**
   ATPCO is headquartered in Virginia and uses cloud computing facilities based in US-based and international regions.

4. **Where does ATPCO operate, geographically? Where are ATPCO offices located?**
   ATPCO is headquartered in Virginia, USA. A list of global office locations is available here.

5. **How does ATPCO protect confidential data?**
   ATPCO uses approved and appropriate encryption technologies for confidential data at rest and in transit. In addition, ATPCO restricts access to confidential data on a strict need-to-access basis using Role Based Access Control (RBAC).

6. **Does ATPCO perform an annual penetration test? Can the report be made available?**
   Infrastructure, Application, and API Penetration Tests are conducted by a third party at least annually, or when significant changes are made to the underlying infrastructure. Executive level Penetration Testing reports can be provided upon request.

7. **What is the expected notification timeline in the potential case of an incident or data breach?**
   In the event of a data breach, ATPCO customers must be notified within 48 hours, including the steps ATPCO is taking to contain the breach and limit exposure.

8. **Does ATPCO have a Data Protection Officer?**
   ATPCO has a designated Data Protection Officer. Details can be provided on request.

9. **Does ATPCO follow secure software development practices?**
   ATPCO follows secure software design principles, including architecture and threat reviews, use of appropriate encryption technologies, static and dynamic code scanning, security testing and developer training based on the OWASP Top 10 Web Application Security Risks.