ATPCO Attestation of Information Security Controls

March 2018

Information and information resources are strategic assets vital to ATPCO's business, and 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) and the International Organization for Standardization ISO 27001 Information Security Standard. ATPCO will also meet the requirements for the EU General Data Protection Regulations in May 2018. The current ATPCO PCI-DSS and ISO 27001 certifications can be accessed here: http://www.atpco.net/compliance

ATPCO will not permit nor authorize ad hoc audits by customers or customer representatives of our sites, facilities, systems or security controls. ATPCO systems are audited by and independent assessor at least annually. 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.

Should you have questions about ATPCO Information Security controls, please contact us at:
Manager, Enterprise Security Services
Privacy and Compliance
Airline Tariff Publishing Company
45005 Aviation Drive, Dulles, VA 20166
Tel. 703-661-7889
Email: privacy@atpco.net

ATPCO Attestation of Information Security Controls

ATPCO Information Security Policies

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

Third party entities are required to adhere to relevant sections of the ATPCO Information Security Policies and 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 of ISO / IEC 27001 certification, which demonstrate 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), evidence of ISO / IEC 27017 certification must be provided which specifies standards for protecting PII data in public cloud services.

The ATPCO Information Security Policies classify specific system configuration as Confidential and therefore restricted from public disclosure. In lieu of disclosing security configuration details, this document provides a high-level overview of the implemented security controls across the following information security domains:

1. Asset management
2. Human Resources security
3. Communications and Operations Management
4. Physical Security
5. Access control
6. Information Systems Acquisition, Development, and Maintenance
7. Incident and Event Management
8. Business Continuity Management
9. Disaster Recovery
10. Data Protection

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

Washington Dulles International Airport
45005 Aviation Drive Dulles VA, 20166
T: +1-703-661-7400
www.atpco.net

Security Domain	Implemented Security Controls
1. Asset Management	ATPCO maintains an accurate asset inventory that is monitored and audited at least monthly. Data retention is strictly enforced via embedded operating system (OS) controls based on data classification and business owner declaration. 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.
2. Human Resources Security	All prospective employees undergo professional reference checks. Any prospective employee who will have access to credit-card data will be subject to pre-employment background checks. Additional background screening is conducted as necessary dependent on the position of the candidate, which include Directors and Officers. All employees are required to undergo annual security awareness training and are required to take a security awareness test which confirms their acknowledgment and agreement to abide by the ATPCO Information Security policies. ATPCO has a strict on-boarding/off-boarding process with an established workflow for requesting access to systems and data and for revoking access upon termination.

Washington Dulles International Airport
45005 Aviation Drive Dulles VA, 20166
T: +1-703-661-7400
www.atpco.net

3. Communications and Operations Management	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 application. Network-level access and remote administrative access requires two-factor authentication. Anti-virus software is deployed on all servers/hosts where applicable. Logging is enabled via standard configuration of all network devices and hosts, and includes details such as User name / 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 maintained for at least 90 days. ATPCO has an established Privacy Policy, which is accessible here: https://www.atpco.net/privacy-policy All confidential and sensitive data is transmitted via SSL/TLS. While at rest, confidential and sensitive data is either encrypted or protected by additional layers of access control which require approval for access. All production removable media that leaves the ATPCO facility is logged, tracked, and accounted for via authorized sign-offs at each point. ATPCO conducts monthly scans for rogue wireless devices. Systems back-ups and restoration is validated via regularly scheduled disaster recovery testing. A formal change control program is in place that requires management approval for all system configuration changes or application updates.

Washington Dulles International Airport
45005 Aviation Drive Dulles VA, 20166
T: +1-703-661-7400
www.atpco.net

4. Physical Security	Physical access to sensitive areas is controlled by an electronic card key system and only employees with elevated access are granted access to the most secure environments. Access is also monitored and recorded via an electronic surveillance system. ATPCO has implemented hardware environmental controls such as generators, UPS, and a fire suppression/control system.
5. Access Control	All ATPCO systems display a warning log-on banner upon first access to secured resources. Each user (employee or customer) is assigned a uniqe UserIUD 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. Physical access rights are granted only based on authorized request and on business need. 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” rule.

Washington Dulles International Airport
45005 Aviation Drive Dulles VA, 20166
T: +1-703-661-7400
www.atpco.net

6. Information Systems Acquisition, Development & Maintenance	All ATPCO system software is patched on a regular cycle; all critical system security patches/updates are installed within 30 days of release. ATPCO performs regular (at least weekly) vulnerability scanning against all public Internet-facing hosts, and any identified vulnerabilities are remediated via established procedures. Network and Application Penetrations Tests are conducted at least quarterly, or when there are significant network changes. All ATPCO systems are developed according to an established Systems Development Life Cycle (SDLC), which includes security controls for common security vulnerabilities. ATPCO developers must undergo training for secure coding principles upon hire and annually thereafter.
7. Information Security Incident Management	ATPCO has an established Computer Security Incident Response policy and associated Incident Response Procedures, both of which address any event that threatens to compromise any aspect of computer or network security. A formalized plan has been established detailing procedures for incident detection, assessment, notification, and recovery activities to mitigate computer security risks.
8. Business Continuity Management	ATPCO has developed a Business Continuity plan (Enterprise Availability Plan) that provides for the protection of ATPCO's data and resources against disruption. The plan defines and ranks in priority those data systems/resources and business processes that are critical to ATPCO ongoing operations, and formulates procedures for the prompt resumption of business functions in case of disruption.
9. Disaster Recovery	The ATPCO computing environment consists of geographically dispersed, co-located datacenter facilities which provide fault-tolerance and complete N+1 redundancy for system/ network failures. Our disaster recovery strategy includes data replication to our second 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.

Washington Dulles International Airport
45005 Aviation Drive Dulles VA, 20166
T: +1-703-661-7400
www.atpco.net

10. Data Protection	Employees are prohibited from storing unencrypted customer data on mobile devices. Only company issued devices with a digital security certificate are permitted to access the cardholder data environment. ATPCO has implemented a Data Classification system for handling Public, Sensitive, and Confidential data. Any storage device or removable media used for transport is logged, authorized by management, and tracked. No proprietary and/or confidential documents are left on employee desks in plain sight. All software testing is conducted in a non-production environment and tests in non-production environments do not use live production data. If there´s a justified need for testing with production-like data, the data is sanitized in a way to make it impossible to identify sensitive data.

Should you have any further questions or require additional information, please contact your ATPCO representative.

Washington Dulles International Airport
45005 Aviation Drive Dulles VA, 20166
T: +1-703-661-7400
www.atpco.net