Compliance Policy

Document Control

Document Title:	Compliance Policy
Version:	1.0
Version Date:	June 23, 2022
Created By:	Pivot Point Security (PPS)
Approved By:	TJ McCauley
Document Owner:	Information Security Management Committee
Confidentiality Level:	Confidential

Revision History

Version	Date	Author	Comments
0.1	February 20. 2020	PPS	1st Draft for Review
1.0	May 26, 2020	TJ McCauley	Approved
1.0	June 23, 2021	TJ McCauley	Annual Review & Approval
1.0	June 23, 2022	TJ McCauley	Annual Review & Approval

References

Standard / Guideline	Control Area(s)
ISO 27001:2013 ISO 27018:2014	A.5.1.1 Policies for information security A.18.1 Compliance with legal and contractual requirements

Table of Contents

1. Purpose

The purpose of Accommodations Plus International's (API) Compliance Policy is to define the requirements and responsibilities to identify and comply with legal, regulatory, or contractual security obligations.

2. Scope

The Compliance Policy applies equally to all individuals required to comply with any legal or contractual requirements.

3. Compliance Goals

- Maintain a documented list of all relevant legal, regulatory, and contractual requirements applicable to the company.
- Ensure all relevant legal, regulatory, and contractual requirements are defined in the company's Master Service Agreement (MSA) or third-party agreement.
- Ensure all third-party agreements are reviewed by authorized and appropriate personnel. This may include external Counsel.
- Ensure all security requirements in all third-party agreements are vetted with the Director, Information Security, prior to signing.
- Ensure the Information Security Management Committee (ISMC) is aware of all security requirements that the Information Security Management System (ISMS) must meet to determine if adjustments or enhancements to any controls need to be made.
- Implement appropriate measures to ensure compliance with intellectual property rights and the use of proprietary software products.
- Ensure data protection and privacy as required in relevant legislation, regulations, and contractual clauses.
- Ensure cryptographic controls are documented and used in compliance with all relevant agreements, laws, and regulations.

4. Procedures

4.1 Identification of Applicable Legislation

- API's Counsel is responsible for identifying, assessing, and communicating the statutory and regulatory requirements applicable to API, its information, systems, and services.

4.2 Intellectual Property Rights

The following guidelines must be considered to protect any material that may be considered intellectual property:

- Software must only be acquired through known and reputable sources to ensure that copyright is not violated.
- IT should maintain appropriate asset registers and evidence of licenses, registration keys, manuals, etc.
- Licenses must be kept up-to-date.

4.3 Privacy and Protection of Personally Identifiable Information

- Local, state and international privacy regulations should be reviewed and followed where applicable to ensure data protection and privacy of Personally Identifiable Information (PII).
- API's Counsel is responsible for communicating these requirements to the ISMC to ensure that ISMS operations are compliant with applicable regulations.
- The ISMC may request assistance from Counsel or third-party consultants.
- The ISMC is charged with developing and implementing the Data Classification and Asset Management Policy and the Information Transfer Policy to protect and maintain all applicable information's privacy.

4.4 Prevention of Misuse of Information Processing Facilities

- API's Acceptable Use Policy should be followed while using any information system or accessing API's information.
- Any unauthorized activity identified by monitoring or other means must be reported to IT Security.

4.5 Regulation of Cryptographic Controls

- API's systems must not use cryptographic controls that violate US laws and regulations.
- API's systems must incorporate encryption to meet all regulations, statutes, and contractual obligations.

4.6 Implementation

- The ISMC is responsible for ensuring that this policy is applied to all personnel required to comply with any requirements affecting information systems or the ISMS.
- All API employees are responsible for following all requirements and reporting any instance of failure or weakness in compliance.