Acceptable Use Policy

Document Control

Document Title:	Acceptable Use Policy
Version:	2.0
Version Date:	June 6, 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	April 13, 2020	TJ McCauley	Approved
1.0	June 21, 2021	TJ McCauley	Annual Review & Approval
2.0	June 6, 2022	TJ McCauley	Added MFA requirement to 3.1 Annual review & Approval

References

Standard / Guideline	Control Area(s)
ISO 27001:2013 ISO 27018:2014	A.5.1.1 Policies for information security A.8.1.3 Acceptable use of assets

Table of Contents

1. Purpose

The purpose of the Accommodations Plus International (API) Acceptable Use Policy is to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the use of information assets.
- To establish prudent and acceptable practices regarding the use of API information assets.
- To educate individuals in their responsibilities for the acceptable use of API information assets and overall adherence to the company's policies, procedures, and security requirements.

2. Scope

This policy applies equally to all individuals granted access to any API information asset.

3. Policy

3.1 General Use

- API employees are only to access information and systems to which they are authorized.
- API employees must not divulge any remote access information (e.g., VPN server identification, etc.).
- API employees must not share their API account(s), passwords, Personal Identification Numbers (PINs), security tokens/fobs (.e. smartcard), digital certificates, identification badges or similar identification and authentication information, or devices.
- API employees must not make or use unauthorized copies of copyrighted software.
- API employees must not purposely use API's information systems to engage in activity that may harass, threaten, or abuse others.
- API employees may not engage in willful or malicious activity that degrades information system performance, deprives an authorized API user of their access to a API information asset, allows unauthorized access to resources, or circumvents API computer security measures.
- API employees must not purposely use API information assets to access third party non-public systems or obtain third party proprietary information without the express permission of such third party.
- API employees must not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system without API management's explicit consent (e.g. password cracking programs, packet sniffers, port scanners, etc.).

- API employees should not install non-approved software on information assets.
- API employees must not intentionally access, create, store, or transmit material which API may deem to be offensive, indecent, or obscene. Such material includes but is not limited to:
    - Racist information
    - Pornography
    - Sexually harassing content
- API employees may only access API information assets with systems that are equipped with active, licensed, and up-to-date security software whose definitions are updated at least daily when connected to the company's network.
- API employees may only access API information assets with systems that are equipped with a mutli-factor authentication client.API employees must not engage in acts using API information assets against the aims and purposes of API as specified in rules, regulations, and procedures.
- API employees shall only use management approved Operating Systems on any company issued laptops and devices.
- Disabling or altering security software installed and configured on API information assets is prohibited (i.e. anti-virus software, disk encryption, personal firewalls, etc.).
- Individuals must report any weaknesses in API's computer security, applications, any incidents of possible misuse or violation of this agreement to the API IT Security: SecurityTeam@API.com.

3.2 Incidental Use

As a convenience to the API user community, incidental use of information assets is permitted. The following restrictions apply:

- Incidental personal use of electronic mail, Internet access, fax machines, printers, copiers, and so on, is restricted to API authorized users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to API.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- Storage of personal email messages, voice messages, files, and documents within API information assets must be nominal.
- All data, both professional and personal, located on company assets is owned by API, and management reserves the right to access any information on corporate assets at any time in accordance with this policy. Use of API's assets is implicit acceptance of this policy.

3.3 Email Access and Use

- Auto-forwarding electronic messages to email addresses external to the API domain is prohibited.
- Individual mailbox delegation is prohibited, with the exception of calendars, related functions, or situations which have received explicit management approval.
- API information assets may not be used to send or receive API Confidential Information, PHI or PII to a party unless:
    - Such party is under a signed non-disclosure agreement (or non-disclosure provisions in the commercial agreement) with API.
    - The Confidential Information is authorized for the purposes of the transaction with that party.
- Confidential Information sent via email must always employ strong encryption.
- Employee email accounts must not be used to send or respond to spam email messages.
- API provided email must not:
    - Involve solicitation to external parties.
    - Have the potential to harm the reputation of API.
    - Forward chain emails.
    - Contain or promote anti-social or unethical behavior.
    - Violate local, state, federal, international laws, or regulations or knowingly encourage others to do the same.

3.4 Internet Access and Use

- The Internet (including file sharing and sending services) must not be used to communicate API Confidential Information, PHI, or PII unless:
    - The confidentiality and integrity of the information is ensured and the identity of the recipient is established pursuant to a signed non-disclosure agreement (or non-disclosure provisions in the commercial agreement) with API.
    - The Confidential Information is authorized for the purposes of the transaction contemplated with the recipient.
- Users are required to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software or materials viewed, used, or obtained via API networking or computing resources.
- Using API networking and computing resources to make or attempt unauthorized entry to any network or computer accessible via the Internet is prohibited.

3.5 Blogging and Social Media

- API employees may not blog or share any corporate information on social media that is not already publicly available.

- API employees shall not engage in any blogging or social media communications that may harm or tarnish the image, reputation, or disparage API and any of its employees in any way.
- If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly, or implicitly, represent themselves as an employee, or representative of API.

3.6 Privacy

- Electronic files created, sent, received, or stored on information assets owned, leased, administered, or otherwise under the custody and control of API are not private and may be accessed by authorized API legal counsel, management, or authorized security personnel at any time, under the direction of API management, without knowledge of the user or owner.
- Systems Administrators, Engineers, Security Team, and other API personnel may have privileges that extend beyond those granted to standard business users. Personnel with extended privileges may not access files or other information that are not specifically required to carry out the tasks reasonably attributed to their role or responsibility.
- All API employees must exercise due care and due diligence to safeguard the privacy and security of all information entrusted to API by all entities.