Information Security Policy

22 June 2021

Metadata

Review

Accountable Director	CTO
Policy Author	CTO
Date Approved	Sep 2019
Date Last Reviewed	Jun 2021
Date of Next Review	Mar 2022

Document history

Version	Date	Author	Description
1	Sep 2019	CTO	Initial Version
2	Apr 2020	CTO	Add metadata
3	Jun 2021	CTO	Bring in line with Vanta.com's SOC2 recommendations. Split across multiple sub policies.

Contents

1 Overview 4

2 Purpose 5

3 Scope 6

4 Security Incident Reporting 7

5 Remote Access Policy 8

6 Acceptable Use Policy 9

6.1 Unacceptable Use 9

6.2 Email and Communication Activities 11

7 Additional Policies and Procedures Incorporated by Reference 12

7.1 Policy Compliance 13

8 Exceptions 14

9 Violations & Enforcement 15

10 Policy review and update process 16

10.1 When do we make changes? 16

1 Overview

This Information Security Policy is intended to protect PassFort's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfers, are the property of PassFort. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every PassFort employee or contractor who deals with information and/or information systems. It is the responsibility of every team member to read and understand this policy, and to conduct their activities accordingly.

2 Purpose

The purpose of this policy is to communicate our information security policies and outline the acceptable use and protection of PassFort's information and assets. These rules are in place to protect customers, employees, and PassFort. Inappropriate use exposes PassFort to risks including virus attacks, compromise of network systems and services, and legal and compliance issues.

The PassFort "Information Security Policy" is comprised of this policy and all PassFort policies referenced and/or linked within this document.

3 Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct PassFort business or interact with internal networks and business systems, whether owned or leased by PassFort, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at PassFort and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with PassFort policies and standards, and local laws and regulations.

This policy applies to employees, contractors, consultants, temporaries, and other workers at PassFort, including all personnel affiliated with third parties. This policy applies to all PassFort-controlled company and customer data as well as all equipment, systems, networks and software owned or leased by PassFort.

4 Security Incident Reporting

All users are required to report known or suspected security events or incidents, including policy violations and observed security weaknesses. Incidents should be reported immediately or as soon as possible by support@passfort.com.

In your email please describe the incident or observation along with any relevant details.

5 Remote Access Policy

Laptops and other computer resources that are used to access the PassFort network must conform to the security requirements outlined in PassFort's Information Security Policies and adhere to the following standards:

- To ensure mobile devices do not connect a compromised device to the company network, Antivirus policies require the use and enforcement of client-side antivirus software
- Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer.
- Users are prohibited from changing or disabling any organizational security controls such as personal firewalls, antivirus software on systems used to access PassFort resources
- Use of remote access software and/or services (e.g., VPN client) is allowable as long as it is provided by the company and configured for multifactor authentication (MFA)
- Unauthorized remote access technologies may not be used or installed on any PassFort system
- Users should use a VPN when transmitting confidential information on public Wi-Fi
- If you access from a public computer (e.g., business center, hotel, etc.), log out of session and don't save anything. Don't check "remember me, collect all printed materials and delete downloaded files (generally is discouraged)

6 Acceptable Use Policy

PassFort proprietary and customer information stored on electronic and computing devices whether owned or leased by PassFort, the employee or a third party, remains the sole property of PassFort for the purposes of this policy. Employees and contractors must ensure through legal or technical means that proprietary information is protected in accordance with the Data Management Policy. The use of Google Drive for business file storage is required for users of laptops or company issued devices. Storing important documents on the file share is how you "backup" your laptop.

You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of PassFort proprietary information. You may access, use or share PassFort proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use of company-provided devices.

For security and network maintenance purposes, authorized individuals within PassFort may monitor equipment, systems and network traffic at any time.

PassFort reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6.1 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Under no circumstances is an employee of PassFort authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing PassFort-owned resources. The list below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PassFort.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copy-

righted music, and the installation of any copyrighted software for which PassFort or the end user does not have an active license.

3. Accessing data, a server, or an account for any purpose other than conducting PassFort business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a PassFort computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
8. Making fraudulent offers of products, items, or services originating from any PassFort account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient, or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the PassFort engineering team is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the PassFort network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means.
17. Providing information about, or lists of: PassFort employees, contractors, partners, or cus-

tomers to parties outside PassFort without authorization.

6.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company and act accordingly.

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited email messages, including the sending of “junk mail”, or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or texting, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.
5. Creating or forwarding “chain letters”, “Ponzi”, or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within PassFort networks or other service providers on behalf of, or to advertise, any service hosted by PassFort or connected via PassFort’s network.

7 Additional Policies and Procedures Incorporated by Reference

Policy	Purpose
Access Control Policy	To limit access to information and information processing systems, networks, and facilities to authorized parties in accordance with business objectives.
Asset Management Policy	To identify organizational assets and define appropriate protection responsibilities.
Business Continuity & Disaster Recovery Plan	To prepare PassFort in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.
Cryptography Policy	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Device Policy	To ensure that devices are used appropriately within the organization
Data Management Policy	To ensure that information is classified and protected in accordance with its importance to the organization.
Human Resources Policy	To ensure that employees and contractors meet security requirements, understand their responsibilities, and are suitable for their roles.
Incident Response Plan	Policy and procedures for suspected or confirmed information security incidents.
Operations Security Policy	To ensure the correct and secure operation of information processing systems and facilities.

Policy	Purpose
Physical Security Policy	To prevent unauthorized physical access or damage to the organization's information and information processing facilities.
Risk Management Policy	To define the process for assessing and managing PassFort's information security risks in order to achieve the company's business and information security objectives.
Secure Development Policy	To ensure that information security is designed and implemented within the development lifecycle for applications and information systems.
Third-Party Management Policy	To ensure protection of the organization's data and assets that are shared with, accessible to, or managed by suppliers, including external parties or third-party organizations such as service providers, vendors, and customers, and to maintain an agreed level of information security and service delivery in line with supplier agreements.

7.1 Policy Compliance

PassFort will measure and verify compliance to this policy through various methods, including but not limited to, business tool reports, and both internal and external audits.

8 Exceptions

Requests for an exception to this Policy must be submitted to the CTO for approval.

9 Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

10 Policy review and update process

10.1 When do we make changes?

Broadly there are two categories of event which will trigger a review of this policy.

Standard triggers:

- We review this policy on an annual basis
- In response to changes in our business

Emergency triggers:

- In response to an incident – if we identify a major issue
- In response to regulatory change