Information Security Policy

Metadata

Review

Accountable Director	CTO
Policy Author	CTO
Date Approved	Sep 2017
Date Last Reviewed	Apr 2020
Date Of Next Review	Yearly, Apr 2021

Document History

Version	Date	Author	Description of Changes
1	Sep 2017	CTO	Initial Version
2	April 2020	CTO	Add Metadata

Table of Contents

1. Physical Security

1.1 Secure Areas

Physical security must begin with the building itself and an assessment of perimeter vulnerability must be conducted. A building must have appropriate control mechanisms in place for the classification of information and equipment that is stored within it.

These include the following:

- Alarms fitted and activated outside working hours
- Window and door locks
- Window bars on lower floor levels
- Access control mechanisms (key cards) fitted to all accessible doors
- CCTV cameras
- Staffed reception area
- Protection against damage - e.g. fire, flood, vandalism

Identification and access tools/passes (e.g. badges, keys, entry codes etc.) must only be held by persons authorised to access those areas and should not be loaned/provided to anyone else.

Where breaches do occur, or an employee leaves outside normal termination circumstances, all identification and access tools/passes (e.g. badges, keys etc.) should be recovered from the employee immediately.

1.2 Paper and Equipment Security

Paper based (or similar non-electronic) information must be assigned an owner and a classification. Appropriate information security controls must be put in place to protect it according to the provisions in the Asset Handling Procedure.

Paper in an open office must be protected by the controls for the building and via appropriate measures that could include, but are not restricted to, the following:

- Filing cabinets that are locked with the keys stored away from the cabinet
- Locked safes

All general computer equipment must be located in suitable physical locations that:

- Limit the risks from environmental hazards - e.g. heat, fire, smoke, water, dust and vibration
- Limit the risk of theft - e.g. if necessary items such as laptops should be physically attached to the desk
- Allow workstations handling sensitive data to be positioned so as to eliminate the risk of the data being seen by unauthorised people

1.3 Equipment Lifecycle Management

The CTO must ensure that all of PassFort's IT equipment is maintained in accordance with the manufacturer's instructions and any documented internal procedures to ensure it remains in effective working order.

The use of equipment off-site must be formally approved by the user's line manager.

Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed. If the equipment is to be passed onto another organization (e.g. returned under a leasing agreement) data removal must be achieved by using approved, appropriately secure software tools.

2. Access Security

This access control policy is designed to take account of the business and information security requirements of the organization and is subject to regular review to ensure that it remains appropriate.

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to PassFort systems.

2.1 Business Requirements of Access Control

Business requirements should be established as part of the requirements-gathering stage of new or significantly changed systems and services and should be incorporated in the resulting design.

Information security requirements should be clearly stated within the business requirements specification document and should take account of the organization's standards established in the document Principles for Engineering Secure Systems.

In addition to the specific requirements, a number of general principles will be used when designing access controls for PassFort systems and services.

These are:

- **Defence in Depth** – security should not depend upon any single control but be the sum of a number of complementary controls
- **Least Privilege** – the default approach taken should be to assume that access is not required, rather than to assume that it is
- **Need to Know** – access is only granted to the information required to perform a role, and no more
- **Need to Use** – Users will only be able to access physical and logical facilities required for their role

Adherence to these basic principles will help to keep systems secure by reducing vulnerabilities and therefore the number and severity of security incidents that occur.

As part of the selection of cloud service providers specifically, the following access-related considerations should be taken into account:

- User registration and de-registration functions provided

- Facilities for managing access rights to the cloud service
- To what extent access to cloud services, cloud service functions and cloud service customer data can be controlled on an as required basis
- Availability of multi-factor authentication for administrator accounts
- Procedures for the allocation of secret information such as passwords

Addressing these requirements as part of the selection process will ensure that the provisions of this policy can be met in the cloud as well as within on premise systems.

2.2 User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

2.2.1 User Registration and De-registration

A request for access to the organisation's network and computer systems must first be submitted to the CTO.

An initial strong password should be created on account setup and communicated to the user via secure means. The user must be required to change the password on first use of the account.

When an employee leaves the organisation under normal circumstances, their access to computer systems and data must be suspended at the close of business on the employee's last working day.

User accounts should be initially suspended or disabled only and not deleted. User account names should not be reused as this may cause confusion in the event of a later investigation.

2.2.2 User Access Provisioning

Each user must be allocated access rights and permissions to computer systems and data that are commensurate with the tasks they are expected to perform. In general this should be role-based i.e. a user account will be added to a group that has been created with the access permissions required by that job role.

Group roles should be maintained in line with business requirements and any changes to them should be formally authorised and controlled via the change management process.

2.2.3 Management of Privileged Access Rights

Privileged access rights such as those associated with administrator-level accounts must be identified for each system or network and tightly controlled. In general, technical users (such as IT support staff) should not make day to day use of user accounts with privileged access, rather a separate "admin" user account should be created and used only when the additional privileges are required. These accounts should be specific to an individual e.g. "John Smith Admin"; generic admin accounts should not be used as they provide insufficient identification of the user.

Access to admin level permissions should only be allocated to individuals whose roles require them and who have received sufficient training to understand the implications of their use.

The use of user accounts with privileged access in automated routines such as batch or interface jobs should be avoided where possible. Where this is unavoidable the password used should be protected and changed on a regular basis.

2.3 Review of User Access Rights

On a regular basis (at least annually) asset and system owners will be required to review who has access to their areas of responsibility and the level of access in place. This will be to identify:

- People who should not have access (e.g. leavers)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification e.g. generic or shared accounts
- Any other issues that do not comply with this policy

This review will be performed according to a formal procedure and any corrective actions identified and carried out.
A review of user accounts with privileged access will be carried out by the CTO on a quarterly basis to ensure that this policy is being complied with.

2.4 User Responsibilities

In order to exercise due care and try to ensure the security of its information, PassFort expends a significant amount of time and money in implementing effective controls to lessen risk and reduce vulnerabilities. However, much still depends upon the degree of care exercised by the users of networks and systems in their day to day roles. Many recent high profile security breaches have been largely caused by unauthorised access to user accounts resulting from passwords being stolen or guessed.

It is vital therefore that every user plays his or her part in protecting the access they have been granted and ensuring that their account is not used to harm the organisation.

In order to maximise the security of our information every user must:

- Use a strong password i.e. one which is in line with the rules set out in the password policy
- Never tell anyone their password or allow anyone else to use their account
- Not record the password in writing or electronically e.g. in a file or email
- Avoid using the same password for other user accounts, either personal or business-related
- Ensure that any PC or device they leave unattended connected to the network is locked or logged out
- Leave nothing on display that may contain access information such as login names and passwords

Failure to comply with these requirements may result in the organisation taking disciplinary action against the individual(s) concerned.

3. Network Security

This policy sets out PassFort's rules and standards for network protection and acts as a guide for those who create and maintain our IT infrastructure. Its intended audience is IT and information security management and support staff who will implement and maintain the organisation's defences.

As a cloud service provider (CSP), this policy also applies to the methods used to design and create the physical and virtual networks used to deliver service to our cloud customers.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to PassFort systems.

3.1 Network Security Design

The design of networks is a complicated process requiring a good knowledge of network principles and technology. Each design is likely to be different, based on a specific set of requirements that are established early on in the process. This policy does not attempt to specify how individual networks should be designed and built, but provides guidance for the standard building blocks that should be used.

3.1.1 Requirements

A network design should be based on a clear definition of requirements which should include the following security-related factors:

- The classification of the information to be carried across the network and accessed through it
- A risk assessment of the potential threats to the network, taking into account any inherent vulnerabilities
- The level of trust between the different components or organisations that will be connected
- The hours of availability and degree of resilience required from the network
- The geographical spread of the network
- The security controls in place at locations from which the network will be accessed
- Security capabilities of existing computers or devices that will used for access

Requirements should be documented and agreed before design work starts.

3.1.2 Defence in Depth

A “Defence in Depth” approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network. For example network firewalls should be supplemented by host-based software firewalls on servers and clients in order to provide several levels of firewall protection.

At key points in the network a “defence diversity” approach should also be taken so that vulnerabilities are minimised. For example this may involve using firewalls from different vendors in series so that if a vulnerability is exploited in one device, the other will not be subject to it. This may be extended to the use of more than one network virus scanner at the perimeter for the same reason.

3.1.3 Network Segregation

The principle should be adopted that a network should consist of a set of smaller networks segregated from each other based on either trust levels or organisational boundaries (or both).

For a large network this should be achieved using separate domains, particularly where separate organisations’ networks are being linked. An appropriate level of trust should be configured at the domain level and domain perimeters should be secured using a firewall where appropriate.

Within networks, Virtual Local Area Networks (VLANs) will be used to segregate organisational units.

In a cloud environment, it is important that requirements for segregating networks to achieve tenant isolation are defined and the cloud service provider’s ability to meet these requirements is verified.

Where PassFort is acting as a CSP, it is important to enforce segregation between the cloud service customer environment and our own internal network.

3.1.4 Perimeter Security

At all perimeters between the internal network and an external network (such as the Internet) effective measures should be put in place to ensure that only authorised network

traffic is permitted. This will usually consist of at least one Stateful Inspection firewall and for major links with the Internet an Application (or Application Gateway) firewall should be used.

3.1.5 Public Networks

Where information is to be transferred over a public network such as the Internet, strong encryption via SSL/TLS must be used to ensure the confidentiality of the data transmitted.

3.1.6 Wireless Networks

Wireless networks should be secured using WPA2 encryption. WEP and WPA should not be used.

Wireless networks should be treated as insecure even if WPA2 is used as the encryption method and a firewall installed between the wireless network and the main LAN.

A guest wireless network may be provided for visitors. This should also be secured using a firewall.

Wireless access point admin logon passwords should always be changed from the default.

3.1.7 Remote Access

Where there is a requirement for remote access to the internal network the following controls will be used:

- A Virtual Private Network (VPN) will be used providing session encryption using SSL/TLS
- Two factor authentication at the client where appropriate

Remote access should be granted on an “as required” basis rather than for all users by default.

3.1.8 Network Protocols

The protocol used on all networks will be TCP/IP. UDP will be used where appropriate but other OSI layer 4 network protocols should not be used.

Only protocols and ports required on a specific server should be enabled by default in order to reduce the attack surface.

4. Policy review and update process

4.1 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