SECURITY AND COMMUNICATION

# SAFEPASS®

SafePass is an expert in security
for people, buildings & assets.

## IT Security Guideline

## Protecting Systems Against

## Cyber Vulnerabilities

www.safepassglobal.com

SAFEPASS®

# TABLE OF CONTENTS

SAFEPASS®


## IT SECURITY: ALL FOR ONE

The leap to cloud-based systems can be a challenging undertaking for any company regardless of their size or experience. The advantages to switching to a cloud platform are numerous and security is the usual issue that comes to mind. Here, IT security is a cooperative effort that requires collaboration along the entire product supply chain, from the vendor to the end-user. IT security is not just a question of which tools or measures to use, or what to use them for (or against). It's about identifying potential risks and targets, understanding threats and taking informed measures to counter them. Cloud security isn't a one-size-fits-all solution that can protect all IT assets. The services deployed traditionally require more than one approach to security.

## WHO IS THIS GUIDE FOR?

This IT security guideline is addressed to anyone concerned with implementing and maintaining SafePass systems within IT environments. It provides advice, procedures and checklists to make devices, services and related network infrastructure as secure as possible. This includes server security basics, possible threats and scenarios, risk assessment, and installation guidelines.

# IT SECURITY GUIDELINES

Current advances in IT now provide an unprecedented level of usability and convenience. Consequently, due to such ease of use, a growing number of IoT devices have found their way into physical security systems. However, this spike in connected devices creates new vulnerabilities in existing infrastructure.

SafePass has a tradition of passion and commitment to security, both physically and digitally. We are acutely aware of what is at stake, as users depend on the reliability of our systems. Where digital security is concerned, we make every effort to ensure cyber security best practices are incorporated in the design, production and rigorous testing of every component.

### Basic Digital Security Goals for SafePass Systems

Setting up a digital line of defense against cyber-attacks involves the introduction of targeted safeguards and counter-measures to help prevent, minimize, detect, contain or defuse security threats to persons, physical property and other assets. While the goal is to guard against all threats, the secondary option is to reduce the amount of damage for those attacks which do filter through.

To adapt to changing technologies and attack strategies, a continued re-evaluation and management of implemented cyber security measures must be done (risk assessment, threat landscape mapping, identification of attack surfaces, etc.).

## ESSENTIAL COMPONENTS TO BE KEPT IN FOCUS INCLUDE:

### System Devices

Keeping devices physically safe. Enforcing firmware updates. Physical access to critical access ports (e.g. USB ports, ethernet ports, COM ports, etc.) must be restricted to reduce the risk of physical infiltration of malicious software.

### Internal Equipment

Keeping internal equipment such as servers physically and digitally inaccessible to unauthorized persons.

### Enforcing Software and Firmware Updates.

Physical access to critical access ports (e.g. USB ports, ethernet ports, COM ports, etc.) must be restricted to reduce the risk of physical infiltration of malicious software.

### Network Environment

Following network security best practices (authentication, encryption, firewalls, managed privileges, automatic lock-out, back-up management, etc.)

Restricting the exposure of devices and server components to local networks and the Internet

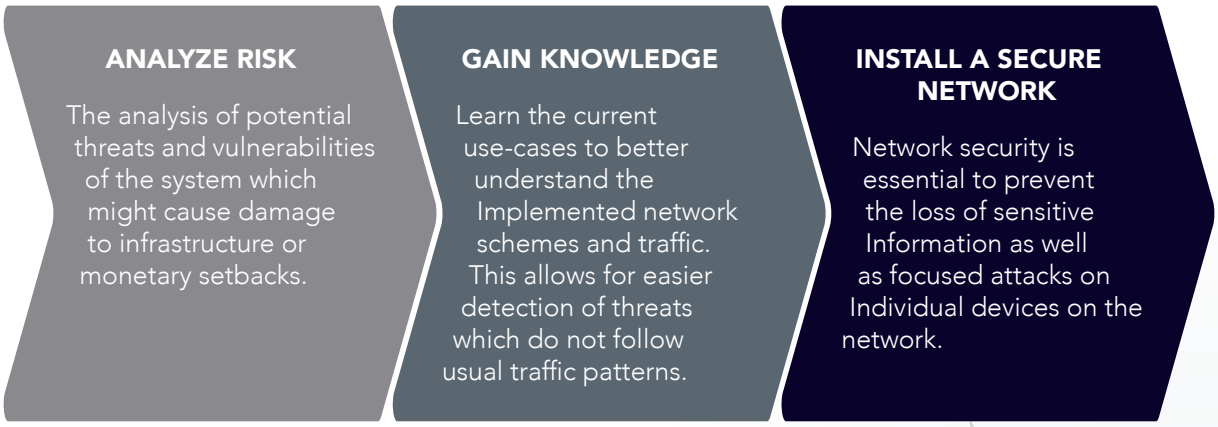
Protecting data and communication lines against external distractions (e.g. denial-of-service attacks)

## POSSIBLE THREATS AND SCENARIOS

Similar to physical security strategy, an IT Security strategy is crucial for starting with an implementation plan and the necessary steps for a secure system.


## SUGGESTED PROCEDURE

To follow a structured approach to secure IT infrastructure, we suggest the following to assist in securing the infrastructure used by the SafePass badging system. For detailed information about standards, procedures and checklist, please refer to the ISO27000 standard or the NIST cyber security Framework.




SAFEPASS®

# RISK ASSESSMENT

## Process of hazard identification, risk analysis and evaluation

We suggest taking a closer look at the following points when conducting a risk assessment.

- System requirements and objectives
- System or network architecture and infrastructure, such as a network diagram showing how assets are configured and interconnected
- Information available to the public or accessible from the organization's websites
- Physical assets, such as hardware, including these at the data center, network, and communication equipment and peripherals (laptops, desktops, smartphones).
- Operating systems (MAC OSX, Windows, Linux, etc.)
- Data repositories such as database management systems
- A listing of all applications Installed within the networked devices
- Network details, such as supported protocols in network and services offered
- Security systems in use, such as access control mechanisms, change control, antivirus, spam control in network monitoring
- Security companies deployed, such as firewalls in intrusion detection systems
- Processes, such as business processes, computer operation processes, network operation processes and application operation processes
- Identification and authentication mechanisms
- Government laws and regulations pertaining to minimum security control requirements
- Documented or internal policies, procedures and guidelines

For more information please visit **www.isaca.org** or the corresponding ISO standard for Risk Management in IT systems ISO 27005

# POSSIBLE THREATS

## TYPES OF ATTACKS

### Targeted Attack

Here, the attacker knows the exact system that must be Infiltrated. The focus in this case is on a goal (e.g., stealing specific data, spying on individuals or causing a disruption). Although they typically involve the same low-cost attack vectors and perpetration tools, targeted attacks involve a much higher level of dedication on the part of the attackers. In case of a failed attempt, the perpetrators are prepared to spend more effort on finding other attack surfaces and exploring more refined methods if their perceived benefit outweighs the resources expended to achieve it. The typical tools utilized for targeted attacks include things like social engineering (e.g., using persuasive e-mails or phone calls to trick employees into revealing passwords). If the attack is unsuccessful, the attacker will proceed to analyze the system to identify other vulnerabilities in the software, processes, firmware of connected devices, etc. and use his previous knowledge as a starting point for their next attempt.

### Opportunity Attack

Here, the perpetrators strike when they come across some vulnerability in a system (an open network or port, for example) and they hope to exploit It without much effort.

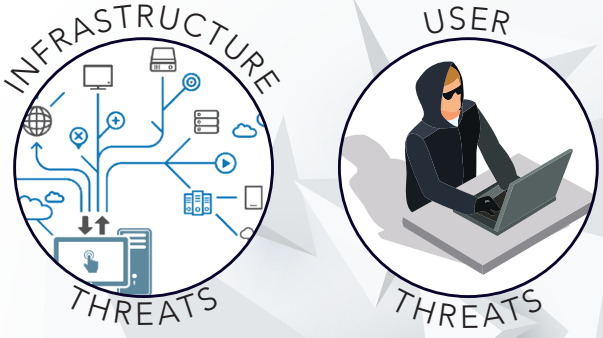
To find their potential targets, they use low-cost attack vectors such as mass phishing, scanning network domains for open ports, using software exploits, or trying common or known default passwords. Their method focuses on firing a broad shot at large numbers of potential targets rather than singling out an individual one. If an attempt fails, they will not bother to make further attempts but move on the next potential victim. Maintaining a standard level data protection policy is usually enough to diminish the risk of becoming the victim of an opportunity attack.

### Value and Cost of an attack

The value of an attack for a perpetrator depends on the pay-off (i.e., the gain or benefit relative to the cost/effort invested). From a data security point of view, the main goal is to apply a level of data protections that make the cost/benefit ratio of an attack as unattractive (unprofitable) for perpetrators as possible. The key to maintaining an adequate level of cyber security is to know which of the many possible threats are in fact plausible, given what is at stake. This knowledge is helpful when it comes to identifying the attack surfaces that are most likely to be exploited and therefore need to be addressed by (technical, organizational or other) security measures.

### Most Common Threats

There are different possibilities for the classification of IT security threats. The most common IT security threats related to SafePass systems are:




SAFEPASS®

# INFRASTRUCTURE OR NETWORK THREAT

In the aspect of a digital badging system, a network attack can be considered the most catastrophic.

On cloud-based systems, their network connectivity is the most likely protocol to be exploited. Today's network attackers ("hackers") have a wide range of refined tools and sophisticated strategies. Most commonly, they will sniff out data packets of an open network to gain knowledge of the traffic and then base their attacks on this data. In other cases, they will actively intercept, manipulate or corrupt the data, or disrupt the network and related infrastructures. Insufficiently protected systems are primary targets for attacks of this type. As an operator of a cloud-based system, having an appropriately high level of network security in place is of crucial importance to protect data integrity.

## EAVESDROPPING

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in the network to "listen in" or interpret (read) the traffic. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Once physical access has been attained to the network an exploit like thus Is difficult to perceive.

## DATA MODIFICATION

After an attacker has read the network data, the next logical step is to alter it. An attacker can modify the data in the transmission without the knowledge of the sender or receiver.

## IDENTITY SPOOFING

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsified. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate Intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete network data. The attacker can also conduct other types of attacks, as described in the following sections.

## PASSWORD-BASED ATTACKS

A common denominator of most operating system and network security plans is password-based access control. This means access rights to a computer and network resources are determined by who accesses It, that is, by the username and password. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

## DENIAL-OF-SERVICE ATTACK

Unlike a password-based attack, the denial-of-service attack prevents normal use of a computer or network by valid users. After gaining access to the network, the attacker can do any of the following:

- Refocus the attention of internal Information Systems staff so that they do not see the intrusion immediately, this allows the attacker to attack highly guarded points during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services thus disrupting everyday operations.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

## MAN-IN-THE-MIDDLE ATTACK

As the name indicates, a man-in-the-middle attack occurs when someone between the secure system and the person with whom the secure system is communicating is actively monitoring, capturing, and controlling the communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

## COMPROMISED-KEY ATTACK

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

## SNIFFER ATTACK

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be opened and read unless they are encrypted.

## APPLICATION-LAYER ATTACK

An application-layer attack targets application server by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of the application, system, or network.

# USER THREATS

User threats (commonly known as insider threats) are a cause of costly security breaches and are often very difficult to remediate. Especially, when the system is related to physical security of the building or asset, the possibility of a user threat should be considered as one major aspect of the whole security concept. There are several reasons why this is the case:

### Insider Threats Can Go Undetected For Years

The longer It takes to detect a breach or a leak, the more remediation costs go up.

Insider threats can be very tough to detect, which is why they are the most expensive to remediate.

### It Is Hard To Distinguish Harmful Actions From Regular Work

Therefore, insider threats are very hard to detect. When an employee is working with sensitive data, it is almost impossible to know whether they are doing something malicious or not.

### It Is Easy For Personnel To Cover Their Actions

While it's hard to detect malicious actions when they happen, it can be almost impossible to detect them post-attack. Tech-savvy personnel will know how to clean up after themselves by editing or deleting logs to conceal malicious action.

### It Is Hard To Prove Guilt

Even if malicious actions are detected, employees can simply claim that they made a mistake and get away with it. It is almost impossible to prove guilt in such cases. Unless If key-loggers and constant behavioral monitoring Is Implemented.

The following three factors must be taken into account:

#### Privileged Users

These are usually the most trusted users in a company, but they also have the most opportunities to misuse company data, both intentionally and unintentionally.

#### Third Parties

Remote employees, subcontractors, third-party vendors and partners all usually have access to the system. Since one knows nothing about the implemented security of their systems and often even about the very people accessing the data, one should treat them as a security risk.

#### Terminated Employees

Sometimes employees can access company data even after termination. (e.g. by retaining their access because nobody bothered to disable it.)

### Possible measures to overcome these threats:

Define processes and educate system users
Use the principle of least privilege for the users
Monitor user action related to both IT and physical security

# INSTALLATION GUIDELINES

BEST PRACTICE

The following points are a selection of best practices for installing an IoT network.

## Network Isolation

One way to establish a secure network is to implement a network isolation scheme. This ensures that critical network resources and components that require no direct interaction are separated into individual network segments (this is why 'network isolation' is also known as 'network segmentation').

In case of a successful attack, the breach (and therefore the attack value) will be limited to the compromised network segment, leaving the others unaffected. Unlike configurations where one successful attack may be enough to infiltrate an entire network, isolation has the advantage of limiting the potential dam age while multiplying the cost of an attack.

With the help of managed switches, network isolation may also be implemented on a virtual (VLAN) level. Segmentation can even be refined to the point where individual resources have their own cabling and network gear in place. The selection of a segmentation scheme to use depends on the required level of security, existing infrastructures and available budget.

PHYSICAL SECURITY AND NETWORK AUTHENTICATION

## Reference to Product Manuals

To do a proper planning and installation of a SafePass System, please review the corresponding product manuals related to the system. We suggest configuring all SafePass products according to the company's internal IT security regulations.

The product-related material is available via our website, **www.safepassglobal.com.**

# TERMINOLOGY

## KEY CYBERSECURITY TERMS

**Adware** - Any software application that displays advertising banners while the program is running. Adware often includes code that tracks a user's personal information and passes it on to third parties without the user's authorization or knowledge. Adware slows down a computer significantly. Over time, performance can be degraded To the point that one may have trouble working productively. See also Spyware and Malware.

**Authentication** - Confirming the correctness of the claimed identity of an individual user, machine, software component or any other entity.

**Authorization** - The approval, permission or empowerment for someone or something to do something with the implemented infrastructure.

**Backdoor** - Hidden software or hardware mechanism used to circumvent security controls.

**Backup** - File copies that are saved as protection against loss, damage or unavailability of the primary data. Saving methods include high-capacity tape, separate disk sub-systems or In the cloud . Off-site backup storage is ideal, sufficiently far away to reduce the risk of environmental disasters, which might destroy both the primary and the backup if kept nearby.

**Bandwidth** - The capacity of a communication channel to pass data such as text, images, video or sound through the channel in a given amount of time. Usually expressed in bits per second.

**Brute Force Attack** - An exhaustive password-cracking procedure that tries all possibilities, one by one. See also Dictionary Attack and Hybrid Attack.

**Blended Threat** - A computer network attack that seeks to maximize the severity of damage and speed of contagion by combining methods - for example, using characteristics of both viruses and worms. See also Electronic Infection.

**Clear Screen Policy** - A policy that directs all computer users to ensure that the contents of the screen are protected from prying eyes and opportunistic breaches of confidentially. Typically, the easiest means of compliance is to use a screen saver that engages either on request or after a specified short period of time. See also Shoulder Surfing.

**Digital Certificate** - The electronic equivalent of an ID card that establishes credentials when doing business or other transactions on the Web. It contains a name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

**Dictionary Attack** - A password-cracking attack that tries all of the phrases or words in a dictionary. See also Brute Force Attack and Hybrid Attack.

**Encryption** - A data security technique used to protect information from un authorized inspection or alteration. Information is encoded so that it appears as a meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.

**End User License Agreement (EULA)** - A contract between the customer and the software's vendor or developer. If the software's EULA is hard to understand or cannot be located, beware!

**Evil Twins** - A fake wireless Internet hot spot that looks like a legitimate service. When victims connect to the wireless network, a cyber-criminal can launch a spying attack on their transactions on the Internet, or just ask for credit card information as a standard pay-for-access deal. See also Man-in-the-Middle Attacks.

**Firewall** - A hardware or software link in a network that inspects all data packets coming and going from a computer, permitting only those that are authorized to reach the other side.

**Flooding** - An attack that attempts to cause a failure in the security of a computer by providing more input, such as a large volume of data requests, than it can properly process. See also Denial of Service Attack

**Hacker** - An individual who attempts to break into a computer without authorization.

**HTTPS**- When used in the first part of a URL (e.g., http://}, this term specifies the use of hypertext transfer protocol (HTTP) enhanced by a security mechanism such as Secure Socket Layer (SSL). HTTPS signifies that the site Is secure and can be trusted.

**Hybrid Attack** - Builds on other password-cracking attacks by adding numerals and symbols to dictionary words. See also Dictionary Attack and Brute Force Attack.

**Keystroke Logger** - A specific type of electronic infection that records victims' keystrokes and sends them to an attacker. This can be done with either hardware or software. See also Trojan Horse.

**Malware** - A generic term for a number of different types of malicious code. See also Adware and Spyware.

**Password** - A secret sequence of characters that is used as a means of authentication to confirm the identity in a computer program or online.

**Password Cracking** - Password cracking is the process of attempting to guess passwords, given the password file information. See also Brute Force Attacks, Dictionary Attacks and Hybrid Attacks.

**Password Sniffing** - Passive wire-tapping, usually on a local area network, to gain knowledge of passwords.

**Patch** - A patch is a small update released by a software manufacturer to fix bugs in existing programs. Computer's software programs and/or operating system may be configured to check automatically for patches, or the customer may need to periodically visit the manufacturers' websites to see if there have been any updates.

**Shoulder Surfing** - Looking over a person's shoulder to get confidential information. It is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine or type a password. Can also be done long-distance with the aid of binoculars or other vision-enhancing devices.. See also Clear Desk Policy and Clear Screen Policy.

**Spoofing** - Masquerading so that a trusted IP address is used instead of the true IP address. A technique used by hackers as a means of gaining access to a computer system.

**Spyware** - Software that uses an Internet connection to send personally identifiable information about a user to a collecting device on the Internet. It is often packaged with software that one download voluntarily, so that even if one removes the downloaded program later, the spyware may remain. See also Adware and Malware.

**SSL (Secure Socket Layer)** - An encryption system that protects the privacy of data exchanged by a website and the individual user. Used by websites whose URL's begin with https instead of http.

**Trojan Horse** - A computer program that appears to be beneficial or innocuous, but also has a hidden and potentially malicious function that evades security mechanisms. A "keystroke logger," which records victims' keystrokes and sends them to an attacker, or remote-controlled "zombie computers" are examples of the damage that can be done by Trojan horses. See also Electronic Infection.

**Virus** - A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting- i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. Often sent through email attachments. Also see Electronic Infection and Blended Threat.

**Fishing** - Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information . People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately-but in a fishing scam, they are urged to call the phone number provided rather than clicking on a link. See also Phishing.

**Vulnerability** - A flaw that allows someone to operate a computer system with authorization levels in excess of that which the system owner specifically granted.

**Worm** - Originally an acronym for "Write once, read many times," a type of electronic infection that can run independently, and can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. Once this malicious software is on a computer, it scans the network for another machine with a specific security vulnerability. When it finds one, it exploits the weakness to copy itself to the new machine, and then the worm starts replicating from there, as well. See also Electronic Infection and Blended Threat.

**Zombie Computer** - A remote-access Trojan horse which installs hidden code that allows a computer to be controlled remotely. Digital thieves then use robot networks of thousands of zombie computers to carry out attacks on other people and cover up their tracks.

## SECURE VISITOR MANAGEMENT SYSTEMS BY SAFEPASS

Can we imagine a system that millions of people rely on every day, where every interaction is critical? This is the world of SafePass! Innovative, simple, reliable solutions are our passion.

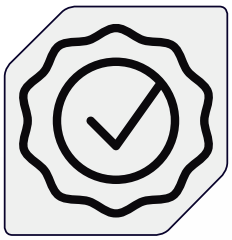
As a global market leader in Wi-Fi tracking software and digital badging hardware, we provide not just integrated solutions to third-party systems, we also provide products that open up new possibilities for visitor management. SafePass is the preferred choice for visitor management systems all over the world.

www.safepassglobal.com

Project consulting for tailored solutions

Long-term customer and supplier relationships

Short delivery times, even for large-scale systems



Superior SafePass quality means long product life cycles

## QUALITY TESTED. RELIABLE. WELL-DESIGNED.

SafePass products are developed by SafePass, Inc. in Houston, TX.

Our development and manufacturing processes are certified in accordance with EN ISO 9001:2015.

Technical details are provided for descriptive purposes only and do not constitute a legally binding guarantee of product properties.

**SafePass, Inc.**
2925 Richmond Avenue, Suite 1200
Houston, Tx 77098
(888) 559-0903 | info@safepassglobal.com
www.safepassglobal.com