vSecureLabs

# 11 IAM Best Practices to Secure Your Enterprise

Enterprises, more than ever, are adopting IAM to provide …

… better control and access to users and employees.

But, simply integrating an IAM solution won't be enough to secure your enterprise.

You also need to enforce IAM best practices for providing verified access to confidential and sensitive corporate data.

Let's discuss these best practices in detail…

## List of IAM Best Practices:

Not surprisingly, external threat actors keep looking for prospects to streamline large-scale cyber-attacks.

The Covid situation has increased the likelihood of cyber attacks, as people are working remotely and accessing the enterprise data from across the globe.

By witnessing such an increase in cyber threats, security experts and business leaders had to re-evaluate their IAM best practices for 2022 and beyond.

Here is a list of such security best practices that enterprises can leverage.

## #1. Develop a Zero-Trust Approach to Security:

In the modern & complex IT infrastructure, it is always better to assume that no one is trustworthy, unless verified otherwise.

In the zero-trust framework, all users in or outside the enterprise should have to continuously validate them to maintain their access to the enterprise data or assets.

It helps the IAM system evaluate the risk level during each session.

Enabling a zero-trust framework in the IAM solution helps an enterprise to identify abnormal behaviors, breaches, or violations of any law.

## #2. Centralize the Security System:

Centralizing the IAM operations allow all functionalities and configurations to reside in one central environment.

A centralized security system will render better visibility to all the different security configurations.

In a hybrid scenario, maintaining a centralized system is a security best practice that allows managing accounts from one location.

It allows users to have access to both cloud & on-premise resources through a common digital identity.

## #3. Eliminate High-Risk Systems:

Another elegant approach to keeping your IAM in its most robust form is, to eliminate high-risk software and third-party integrations.

There are a lot of software and integrations that no longer support patches and updates by their vendors.

These end-of-life applications with no security updates might create security gaps in your IAM solution.

Again, applications like remote desktop sharing can also pose security threats as the protocols they use can record or gain access to other's systems.

So, it is always a good practice to avoid such risky systems.

**#4. Use Multi-Factor Authentication:**

Enabling a "must-have" multi-factor authentication is the first step in building a security layer for all user accounts.

It adds a layer of protection to the sign-in process.

The process adds an extra factor to ensure that the entity involved in the authentication is a legitimate person and not an attacker.

Even if an attacker compromises the login credentials, MFAs like OTPs and bio-metric verification will restrict them from gaining illegitimate access to the account.

**#5. Ensure Privileged Accounts Get Properly Managed:**

One of the IAM best practices is to lock down the root user for day-to-day usage.

Enterprises should follow the principle of least privilege, and if the privilege is given to the person, it should get properly managed.

Enterprises should also assign a minimum permission level for achieving any particular duty or role and maintain complete monitoring and logging of such roles.

## #6. Routine Review & Removal of Orphan Accounts:

Another good practice to keep IAM solutions secure is to perform periodic reviews of user accounts and their privileges.

Employees keep coming and going from every organization regularly.

For off-boarding employees, their accounts become orphans, and anyone can misuse them.

Hence, it is essential to do a periodic check on those orphaned accounts & delete them or withdraw their roles and privileges.

It increases security and minimizes the chances of attacks & breaches.

## #7. Enforce a Strong Password Policy:

Keeping weak passwords that are susceptible to brute force or credential stuffing is not an IAM best practice.

Having a strong password always acts as a firm pillar to construct an impactful IAM solution.

Passwords should be easy to remember and difficult to guess or crack.

For password creation, enterprises should follow the guidelines that are recommended by NIST, like…

- Password's length should be 8 to 64 characters long
- Special characters are a must
- Better to avoid sequential or repetitive characters between the password (e.g., 98765 or gggg)
- A good practice is to set up a password expiration policy

## #8. Establish Single Sign-on (SSO) Authentication:

Enterprises can establish a Single Sign-on (SSO) authentication mechanism for their apps and devices, so that employees or users can use the same access tokens to gain access to other required accounts.

It reduces the challenge of remembering passwords, and enterprises do not have to take heavy precautions to store the passwords securely.



## #9. Set Password Expiry Policy:

In the case of password-based authentication, it is a best practice if enterprises can set 45 days or 60 days password expiry policy.

Renewing the password after every two months or so helps to secure the employee accounts from identity theft, credential stuffing, and other such password compromise attacks.

## 2 BONUS Practices:

### #10. Automate Onboarding & Off-boarding:

Organizations should configure IAM where customers or users can self-serve or automate the onboarding and off-boarding processes.

The onboarding should start with a registration page that will drive the users to follow the registration page and activate their journey from there.

Through automated onboarding, anyone who joins the organization for the first time finds it mandatory to register before using any organization asset.

For off-boarding employees, such automation can help organizations to stay risk free as the orphan accounts get automatically dissolved, so that no one can misuse them.

## #11. Conduct Routine Audits:

Companies usually face the situation where they provide access to employees and this remains active, even when they do not require access anymore.

Others with malicious intension can gain access to those privileges or data and might conduct something malicious on behalf of their credentials.

Hence, it is a good practice to conduct a routine audit of the IAM and manually remove the accounts or privileges that are not necessary.

## Conclusion:

We hope this blog has given you a clear understanding of the various IAM Best Practices that enterprises should implement to leverage IAM solutions to their full potential.

Do you want to secure your enterprise against any cyber attacks (or) data breaches:
Speak with our expert right now

## ✓ Contact us:


- Address: 3831 McCoy Dr Unit 101, Aurora, IL 60504, United States
- Mobile: +1 630-741-4344
- Email: vinod.k@vsecurelabs.co
- Website: vsecurelabs.co