RESOURCE CENTER

Identity and Access Management (IAM) best practices

Get the full interactive view at https://bitwarden.com/resources/identity-and-access-management-iam-best-practices/

bitwarden

Identity and Access Management, or IAM, helps organizations control who can access digital systems and information. It's a key part of keeping data safe — whether for a university, business, or any organization that manages personal or private information.

IAM protects user identities, manages permissions, and makes sure only the right people can access the right systems. This guide outlines best practices for building a strong IAM system, integrating it with other tools, and using it to improve security.

What is IAM?

IAM is a way to manage user accounts, passwords, and access permissions across an organization. It ensures that only authorized users can access sensitive systems, apps, or data. IAM tools also make it easier to manage large groups of users — like students, staff, or employees — without sacrificing security.

A secure IAM setup helps prevent unauthorized access, protects digital assets, and supports compliance with data protection laws.

Read more:

Easily integrate Single Sign-On security with flexible solutions

1. Start with a strong foundation

An effective IAM system begins with a clear structure. This means organizing user accounts, setting up basic security rules, and using tools like multi-factor authentication (MFA) to add extra protection.

Foundational steps:

- **Centralize directories:** Keep user accounts in one place to simplify management.
- **Set access rules:** Assign permissions based on role, like student, teacher, or admin.
- **Follow security frameworks:** Align with standards like GDPR or HIPAA to protect user data and meet legal requirements.

Tools like single sign-on (SSO) allow users to log in once and access everything they need — no need for multiple passwords.

2. Understand key IAM components

A full IAM system includes several tools that work together:

- **Identity management:** Add, remove, and update user accounts.
- **Access control:** Decide what each user can see or do.
- **Authentication:** Confirm a user's identity through passwords, MFA, or biometrics.
- **Provisioning and deprovisioning:** Automate account setup for onboarding and succession.
- **Single sign-on (SSO):** Let users log in once and access multiple systems securely.

Together, these features create a secure, easy-to-manage system for handling access.

3. Automate where you can

Automation reduces mistakes and saves time. When IAM systems connect to tools like HR platforms or student record systems, accounts can be created or removed automatically.

Integration tips:

- Connect IAM with **Active Directory** or similar systems to manage accounts from one place.

- Sync with **HR or student systems** to automate account setup and removal.
- Make sure IAM works with all **enterprise tools and apps**, including cloud services like AWS and Google Cloud.
- Enable **multi-factor authentication (MFA)** to meet new requirements from providers like Google.

Standardizing how users are added, updated, and removed improves both security and efficiency.

4. Use advanced IAM techniques

As threats become more sophisticated, IAM needs to go beyond the basics. Advanced strategies help detect and respond to risky behavior in real time.

Best practices:

- **Review access regularly:** Check who has access and remove anything outdated.
- **Audit permissions:** Use reporting tools to find excessive or unusual access.
- **Use adaptive authentication:** Adjust login requirements based on behavior (e.g., location or device).
- **Consider biometric options:** Features like facial recognition can add security while staying user-friendly.

These steps make it harder for unauthorized users to gain access — even if they have a password.

5. Ensure security and compliance

IAM helps protect data from breaches and supports compliance with laws like GDPR and HIPAA. It also makes it easier to generate reports, run audits, and prove that systems are secure.

Key benefits:

- Reduce the risk of unauthorized access.
- Monitor and log activity across systems.
- Demonstrate compliance to stakeholders and regulators.

Maintaining a strong IAM system shows that an organization takes data privacy seriously.

6. Use federation and single sign-on (SSO)

Identity federation allows users to log in across different systems — even from other organizations — using a shared identity. This is common in higher education or business partnerships.

Single Sign-On (SSO) reduces password fatigue by letting users log in once to access everything they need.

These tools make the user experience smoother while reducing the risk of password-related threats.

7. Monitor and improve

IAM systems should be monitored regularly to spot risks and improve over time. Many platforms include built-in tools like:

- **Activity logs** to track user behavior.
- **Automated alerts** for unusual activity.
- **Analytics** that identify patterns or trends.

Ongoing monitoring helps identify weaknesses, adapt to changes, and maintain trust.

Getting started with IAM

Secure IAM programs are built on a strong foundation, connected to the right tools, and supported by regular monitoring. IT and security teams play a key role in setting up and maintaining these systems, but everyone benefits — from students and employees to administrators and customers.

Strong identity practices reduce risk, improve user experience, and help organizations scale securely.

Bitwarden integrates with Identity Access Management systems through its support for single sign-on (SSO) solutions. By integrating with systems like Okta, Bitwarden provides a comprehensive IAM and SSO solution that centralizes access to SaaS applications and empowers individual employees. This integration helps reduce the number of login credentials employees need, thereby decreasing the potential surface area for cyberattacks and improving user experience and productivity.

Login with trusted devices (SSO) allows users to authenticate through their existing identity provider, leveraging protocols like SAML 2.0 or OpenID Connect. This integration provides flexibility for identity management and enhances security by allowing organizations to apply their existing SSO security controls to access password-based applications within the Bitwarden Vault. Additionally, Bitwarden supports directory integration through SCIM, which automatically provisions and revokes access to the Bitwarden vault, ensuring that changes in your directory are reflected in your Bitwarden organization.

Read more:

Bitwarden and Okta: Enhance security with plug and play integration

Start a free trial with Bitwarden

Strengthen your digital security with Bitwarden. Create a free account or start a 7-day trial of business plans to protect your team. Want to learn more? Join a live weekly demo and connect directly with the Bitwarden team.