IDENTITY & ACCESS MANAGEMENT

Identity & Access Management (IAM) is a framework of business processes, policies, and technologies that facilitate the management of digital identities to ensure that users only gain access to data when they have the appropriate credentials.

THE RECOMMENDED BEST PRACTICES GUIDE FOR ADMINISTRATORS published by the Enduring Security Framework provides actional IAM recommendations to better secure systems from bad actors.

Environmental Hardening

- Take an inventory of all assets within the organization
- Know who has access to which assets
- Understand what security controls and gaps persist
- Develop a network traffic baseline that can be used to detect security anomalies in the network

Identity Federation/Single Sign-On

- Assess your organization's on-premises applications and your cloud providers ability to connect using single sign-on
- Determine if your single sign-on integration can collect user context during single sign-on logins including location, device, and behavior

Multi-Factor Authentication

- Determine the MFA solution best suited in your organization's operating environment
- Implement MFA as part of an enterprise SSO solution
- Maintain a robust inventory of the MFA authenticators
- Routinely test and patch your MFA infrastructure

IAM Auditing & Monitoring

- Establish baseline expectations of activity levels and monitor behavior for acceptable and suspicious activity
- Monitor activity between applications and systems and associated network traffic for changes in connectivity, level of activity, and types of data
- Monitor external traffic, including new interactions with previously unknown sites

LEARN MORE AT **NSA.GOV/ESF**