Cybersecurity Practices Cheatsheet

A quick reference guide to essential cybersecurity practices for protecting systems and networks. This cheat sheet covers key areas such as access control, data protection, incident response, and security awareness.

Core Security Principles

Fundamental Principles

Confidentiality: Ensuring data is accessible only to authorized individuals.

Integrity: Maintaining the accuracy and completeness of data.

Availability: Guaranteeing reliable access to data for authorized users.

Non-Repudiation: Ensuring actions can be traced back to the responsible party, preventing denial of actions.

Defense in Depth

Implementing multiple layers of security controls to protect assets. If one control fails, others are in place to prevent breaches. This includes physical, technical, and administrative controls.

Least Privilege

Granting users only the minimum level of access required to perform their job duties. This reduces the potential damage from insider threats or compromised accounts.

Access Control and Authentication

Authentication Methods

Passwords:	Using strong, unique passwords and implementing password policies (length, complexity, rotation).
Multi-Factor Authentication (MFA):	Requiring two or more verification factors (something you know, something you have, something you are) to access resources.
Biometrics:	Using unique biological traits (fingerprints, facial recognition) for authentication.
Certificates:	Using digital certificates for authentication and encryption.

Access Control Models

Role-Based Access Control (RBAC):	Assigning access permissions based on a user's role within the organization.
Mandatory Access Control (MAC):	Access control decisions are made by a central authority based on security labels assigned to both resources and users.
Discretionary Access Control (DAC):	Resource owners have the discretion to determine who can access their resources.

Data Protection

Encryption

Using encryption to protect data at rest and in transit. Symmetric encryption (e.g., AES) for data at rest, and asymmetric encryption (e.g., RSA) for secure communication.

Data at Rest: Encrypting data stored on hard drives, databases, and other storage media.

Data in Transit: Encrypting data transmitted over networks using protocols like TLS/SSL and VPNs.

Data Loss Prevention (DLP)

Implementing DLP tools to monitor and prevent sensitive data from leaving the organization. This includes monitoring email, web traffic, and file transfers.

Backup and Recovery

Regularly backing up critical data and systems to ensure business continuity in the event of a disaster or data loss. Testing the recovery process is crucial.

On-site Backups: Storing backups locally for quick recovery.

Off-site Backups: Storing backups in a separate location or cloud for disaster recovery.

Incident Response

Incident Response Lifecycle

Preparation: Establishing policies, procedures, and resources for incident response.

Detection and Analysis: Identifying and analyzing security incidents to determine their scope and impact.

Containment: Limiting the spread of the incident and isolating affected systems.

Eradication: Removing the cause of the incident and restoring systems to a secure state.

Recovery: Restoring systems and data to normal operation.

Lessons Learned: Reviewing the incident and identifying areas for improvement.

Reporting

Establishing clear reporting channels for security incidents. Reporting incidents to appropriate authorities and stakeholders.