Identity and Account Recovery Design

Secondary, higher ed, professional | Runbook | 45-75 minutes

Before class: This is an instructor preparation runbook. Assemble the fictional scenarios, messages, or data it specifies before use; it does not provision a lab or include a ready-made dataset.

Lab ID: IAM-RECOVERY-01 Outcome: Evaluate identity lifecycle and recovery controls for a fictional service. Environment: Diagram and scenario; optional approved test tenant. Time: 45-75 minutes.

Scenario Elements

- Account proofing
- Provisioning and role assignment
- Password or passkey enrollment
- Multifactor or phishing-resistant authentication
- Registered device
- Recovery code
- Help-desk or support recovery
- Session revocation
- Access review
- Deprovisioning

Learner Tasks

1. Map the normal identity lifecycle.
2. Map two recovery paths.
3. Identify abuse cases for support, device loss, and recovery codes.
4. Recommend proofing, notification, rate limiting, logging, review, and session controls.
5. Address accessibility and continuity.
6. Explain residual risk.

Instructor Verification

- No real account information is used.
- Recovery does not depend on one unverified channel.
- Learners distinguish authentication from authorization.
- Deprovisioning and active-session revocation are included.

Evidence

Lifecycle diagram, misuse-case table, control recommendations, and two-minute design briefing.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Runbook 2 - Identity and Account Recovery Design.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/identity-and-account-recovery-design/