Pragmatic GRC™

C-006
Identity Offboarding Protocol Guide

Cybersecurity Operations Resource | Version 1.0 | Practical Implementation Guide

Executive Summary

Timely identity offboarding is one of the highest-value cybersecurity controls for small and medium-sized businesses. This guide provides a standardized process for removing access when employees, contractors, or vendors separate from the organization or change roles.

Document Information

Field	Value
Resource ID	C-006
Resource Family	Cybersecurity Operations
Version	1.0
Related Chapters	4, 8
Related Resources	F-001, F-002, F-004, R-001, G-002

1. Purpose

Establish a repeatable process for securely removing or modifying user access whenever personnel leave the organization or change responsibilities.

2. Scope

Applies to employees, contractors, temporary staff, interns, consultants, managed service providers, and third-party users with access to organizational resources.

3. Triggering Events

Voluntary resignation, termination, retirement, contract expiration, role changes, transfers, extended leave, or security-related account suspension.

4. Identity Offboarding Workflow

HR or management notification → Verify separation date → Disable accounts → Revoke privileged access → Collect organizational assets → Remove MFA devices and tokens → Validate completion → Update documentation.

5. Access Removal Checklist

Disable network and cloud accounts; revoke VPN access; remove privileged accounts; disable email; revoke SaaS access; remove MFA registrations; collect badges, keys, laptops, mobile devices, and tokens.

6. Validation and Documentation

Document completion date, reviewer, exceptions, remaining dependencies, and evidence that all required access was removed.

7. Metrics

Track offboarding completion time, overdue offboarding actions, privileged account removals, and exceptions reported during Monthly GRC Heartbeat™ reviews.

8. Integration with Pragmatic GRC™

Update the Unified System Security Plan (F-002), Master Asset Register (F-001), Governance Roles (F-004), and Enterprise Risk Register (R-001) when offboarding reveals control weaknesses.

Recommended Offboarding Timeline

Time	Activity	Owner
Immediately	Disable privileged and remote access	IT/MSP
Same Day	Disable user accounts and email	IT/MSP
Same Day	Collect company assets	Manager
Within 24 Hours	Verify SaaS access removal	IT/MSP
Within 48 Hours	Update documentation and review completion	Governance Owner

Best Practices

- Automate offboarding where possible.
- Remove privileged access before standard user access.
- Coordinate HR, management, and IT activities.

- Maintain evidence of completed offboarding.
- Review offboarding metrics during the Monthly GRC Heartbeat™.

Revision History

Version	Date	Author	Description
1.0		Pragmatic GRC™	Initial publication