Conditional Access Policy (CAP) Governance Standard

Prepared by: Ronnie Bailey, Senior IAM Engineer Lead

Date: July 30, 2025

# 1. Purpose

This document establishes the foundational governance standard for Conditional Access Policies (CAPs) within the organization. It reinforces the existing CAP framework, including the established sequential naming structure (e.g., CA028), while formalizing IAM’s role in reviewing, validating, and coordinating all new CAP activity. The purpose is to standardize intake, reduce policy conflicts, improve audit readiness, and shift the organization from reactive identity practices to proactive governance. This governance standard applies specifically to Conditional Access Policies managed in Microsoft Entra ID (formerly Azure AD). If Conditional Access enforcement expands into other environments (e.g., AWS IAM, Google Workspace, on-prem Active Directory), this plan may be revised to include platform-specific governance practices.

# 2. Background

Conditional Access Policies are currently created and maintained by multiple teams (e.g., MDS, SecOps, Cyber Defense) with limited centralized oversight. Although a sequential CA### numbering system exists (e.g., CA001 to CA999) and is actively used, inconsistencies in intake, testing, and documentation have introduced risk through overlapping policies, incomplete metadata, and audit gaps. This governance standard strengthens the existing framework by formalizing a consistent intake, review, and approval process, ensuring policies are intentional, documented, and traceable.

# 3. IAM Governance Role

IAM will own the governance process for CAPs, specifically to:

* - Serve as the central reviewing authority for all new CAP proposals.
* - Validate policies for logic, scope, naming alignment, and business justification.
* - Coordinate controlled testing in Report-Only mode with pilot users.
* - Provide approval prior to Change Review Board (CRB) submission.
* - Maintain documentation and lifecycle tracking for all CAPs.
* - Lead quarterly reviews to support cleanup and deprecation of stale or overlapping policies.
* - Ensure alignment with Zero Trust principles, least privilege access, and real-world threat prevention (e.g., tactics used by groups like Scatter Spider).
* - Identify and recommend opportunities for automation in CAP governance and reporting.

# 4. Standard CAP Workflow

1. Policy Drafting: Teams (MDS, SecOps, Cyber Defense) draft policies with required metadata and follow existing CA### naming structure.
2. Intake Submission: Proposals are submitted to IAM with business justification, target scope, and risk context.
3. IAM Review: IAM reviews logic, overlap risk, naming compliance, and intent.
4. Controlled Testing: Policies are deployed in Report-Only mode to a small pilot group; IAM monitors behavior and sign-in logs.
5. Production Approval: IAM provides sign-off and submits to CRB for production enforcement through the organization's standard change control process.
6. Lifecycle Oversight: IAM maintains documentation and conducts quarterly cleanup/review cycles.

# 5. Required Metadata

All submitted CAPs must include the following:

* - CA### policy ID aligned with existing numbering structure.
* - Full name and abbreviation reference (e.g., Conditional Access Policy (CAP)) on first mention.
* - Business justification for enforcement (e.g., regulatory, operational, threat mitigation).
* - Targeted users/groups (e.g., roles, geo, departments).
* - Targeted apps/resources.
* - Intended enforcement behavior (e.g., Block, Require MFA, Allow Hybrid Join Only).
* - Testing group and proposed go-live timeline.

# 6. Policy Exceptions

Any exception to standard CAP enforcement must be submitted with justification to IAM. IAM will coordinate with GRC, Risk, or the CRB for review. All exceptions must be documented, time-bound, and revalidated during quarterly reviews. Examples may include service accounts or edge use cases that cannot meet MFA or device requirements. Exception requests must follow a clear request/approval process with documented outcomes.

# 7. Roles and Responsibilities (RACI)

Defined below is the high-level RACI model for Conditional Access governance:

• Requesting Teams (MDS, SecOps, Cyber Defense): Responsible for drafting and initial testing.

• IAM Team: Accountable for review, approval, documentation, and lifecycle oversight.

• GRC/Risk: Consulted for compliance alignment and exception decisions.

• CRB: Final approval authority for production enforcement.

• Stakeholders: Informed of major CAP changes and quarterly outcomes.

# 8. Strategic Benefits

* - Formalizes governance without disrupting current CAP structure (e.g., CA### system).
* - Prevents conflicts and overlapping policy logic.
* - Supports audit readiness and regulatory alignment.
* - Improves response to emerging threats through clean, enforceable CAPs.
* - Positions IAM as a proactive, preventative function rather than a reactive one.
* - Encourages continuous improvement and lays groundwork for automation and Zero Trust initiatives.
* - Treats cleanup as a strategic, risk-reducing activity rather than an administrative task.

# 9. Next Steps

1. Share this governance standard with contributing teams for alignment.  
2. IAM to formalize intake and review procedures.  
3. Begin phased application of this standard to all new CAPs.  
4. Conduct inventory of existing policies for cleanup prioritization.  
5. Schedule first quarterly review with GRC and key stakeholders.