

**Executive Policy**

**Advanced Exploitation Risk and Systemic Exposure Controls**

Version 1.0

Policy Owner \_\_\_\_\_  
Approved By Executive Leadership / Board Risk Committee

Effective Date \_\_\_\_\_

Next Review Date \_\_\_\_\_

Review Cadence Annual or upon material change

## 1. Definitions

Advanced exploitation: Use of sophisticated techniques (including zero-days) to achieve unauthorized access or impact, often without user interaction.

High-confidence exploitation: Exploitation demonstrably reliable for specific targets/builds/conditions based on repeatable testing and operational constraints.

Attack surface: The set of exposed interfaces through which an attacker can interact with a system.

Pre-auth exposure: Functionality reachable prior to user authentication.

Radio-exposed surface: Wireless and discovery protocols increasing pre-authentication reachability.

Insider facilitation: Non-malicious or malicious insider actions that increase exploitability.

Insider intent: Deliberate action to enable exploitation; not assumed as necessary by this policy.

## 2. Scope and Exclusions

This policy applies to enterprise systems, cloud services, managed endpoints, network devices, appliances, and embedded systems presenting pre-authentication, externally reachable, or radio-exposed attack surfaces. The policy does not attempt attribution or model classified capabilities.

## 3. Tier-1 System Definition

Tier-1 systems are systems whose compromise would result in material business impact, regulatory exposure, or safety risk, including internet-facing services, identity systems, regulated data platforms, and critical infrastructure.

## 4. Executive Policy Implications

Sophisticated exploitation can arise from complexity and exposure duration alone. Defensive posture must prioritize exposure reduction, accelerated remediation, lifecycle governance, and adversarial validation, independent of insider intent.

## 5. Required Actions

- Threat modeling and assumption governance
- Attack surface minimization (pre-auth and radios)
- Exposure-based patch and mitigation timelines
- Legacy and end-of-life platform deprecation
- Adversarial testing against blind spots
- Insider facilitation controls beyond malice
- Logging, retention, and executive reporting

## 6. Policy Exception Handling

Exceptions require documented risk acceptance, compensating controls, expiration dates, approval authority, and periodic review.

## 7. Enforcement and Compliance Monitoring

Compliance is mandatory and monitored through audits, adversarial testing, and executive reporting. Material non-compliance is escalated to executive leadership.

## Appendix A — Evidence Artifacts (Enhanced)

| Control Area         | Required Evidence     | Evidence Source     | Control Owner         | Retention |
|----------------------|-----------------------|---------------------|-----------------------|-----------|
| Threat Modeling      | Threat model + review | GRC / Docs          | CISO Office           | 2 years   |
| Assumptions          | Assumption Register   | GRC Tool            | Security Architecture | 2 years   |
| Exposure Inventory   | Service inventory     | CMDB / Scanners     | Platform Ops          | 1 year    |
| Radio Controls       | Baseline configs      | MDM                 | Endpoint Engineering  | 1 year    |
| Patch SLAs           | Patch metrics         | Vuln Mgmt / Tickets | IT Operations         | 1 year    |
| Patch Exceptions     | Risk acceptance       | GRC / Ticketing     | Risk Committee        | 2 years   |
| EOL Management       | Lifecycle tracking    | CMDB                | Asset Management      | 2 years   |
| Adversarial Testing  | Pen test reports      | Testing Vendors     | Security Testing      | 2 years   |
| Insider Facilitation | Training records      | LMS / HR            | HR & Security         | 2 years   |
| Logging & Retention  | Log configs           | SIEM                | SecOps                | ≥180 days |

## Appendix B — SOC 2 Crosswalk (Enhanced)

| Required Action               | SOC 2 Criteria | Control Nature     | Primary Evidence                   |
|-------------------------------|----------------|--------------------|------------------------------------|
| Threat Modeling               | CC3.2, CC3.4   | Design & Operating | Threat models, Assumption Register |
| Attack Surface Minimization   | CC6.1, CC6.6   | Operating          | Service inventories, baselines     |
| Patch & Mitigation SLAs       | CC7.1, CC7.2   | Operating          | Patch dashboards, tickets          |
| Legacy / EOL Deprecation      | CC8.1, CC8.2   | Design & Operating | EOL reports, decommission records  |
| Adversarial Testing           | CC7.3, CC5.3   | Operating          | Pen test reports                   |
| Insider Facilitation Controls | CC1.2, CC1.4   | Design & Operating | Training, policies                 |
| Logging & Exec Oversight      | CC5.3, CC7.3   | Operating          | SIEM configs, dashboards           |

## Appendix C — Cloud, Mobile, and Infrastructure Mapping

| Domain               | Cloud Evidence         | Mobile / Endpoint Evidence | Network / Infrastructure Evidence |
|----------------------|------------------------|----------------------------|-----------------------------------|
| Threat Modeling      | IAM/VPC models         | OS threat models           | Network segmentation models       |
| Exposure Control     | Security Groups / APIs | MDM baselines              | Firewall / ACL configs            |
| Patch & Mitigation   | Cloud patch SLAs       | OS compliance reports      | Firmware update logs              |
| Lifecycle Management | Runtime EOL tracking   | OS lifecycle inventory     | Device OS / firmware lifecycle    |
| Logging & Monitoring | CloudTrail logs        | Endpoint telemetry         | Network device logs               |

## Appendix D — Executive Compliance & Readiness Checklist

- Tier-1 systems are identified and documented
- Threat models include non-insider exploitation scenarios
- Assumption Register exists and is reviewed annually
- Pre-auth and radio-exposed services are inventoried
- Exposure-based patch SLAs are enforced
- EOL platforms are tracked and decommissioned
- Adversarial testing challenges exploitability assumptions
- Insider facilitation controls are documented
- Security logs retained  $\geq 180$  days
- Quarterly executive security reviews are conducted

## Revision History

| <b>Version</b> | <b>Date</b> | <b>Description</b>            | <b>Approved By</b>   |
|----------------|-------------|-------------------------------|----------------------|
| 1.0            | YYYY-MM-DD  | Initial institutional release | Board Risk Committee |

## Executive Approval and Attestation

| Role             | Name | Signature | Date |
|------------------|------|-----------|------|
| CEO              |      |           |      |
| CISO             |      |           |      |
| CIO              |      |           |      |
| General Counsel  |      |           |      |
| Board Risk Chair |      |           |      |