Risk Escalation Map

RISK MANAGEMENT | SD2 SUBMISSION

Process for reporting, managing, and mitigating algorithmic and security risks — CyberPlug DevSecOps Security AI

1. Severity Tier Definitions & Remediation SLAs

Tier	CVSS Range	Definition	Response SLA	Remediation SLA
CRITICAL	9.0 – 10.0	Actively exploitable; direct impact on payment, PII, or auth systems	< 4 hours	24 hrs or deployment block
HIGH	7.0 – 8.9	Significant exposure; likely to impact confidentiality or integrity	4 hours	72 hours
MEDIUM	4.0 – 6.9	Limited exploitability; requires remediation within sprint cycle	24 hours	14 days
LOW	0.1 – 3.9	Minimal direct risk; informational or low-impact misconfiguration	Best effort	30 days

2. Escalation Pathway — 6-Step Process

Step	Stage	Actions Taken	Responsible Party
1	Detection	Automated scan identifies vulnerability. CyberPlug Risk Rating (CRR) assigned. Finding logged in tamper-resistant audit trail.	CyberPlug Platform (automated)
2	Notification	In-platform alert and email sent to Asset Owner and Security Engineer. Deployment block applied for Critical findings.	CyberPlug Alerting Engine
3	Triage	Security Engineer reviews AI-generated finding summary and selects treatment: Remediate, Mitigate, Accept, or Transfer.	Security Engineer
4	Escalation (Critical/High)	If SLA is approaching or treatment is Accept/Transfer for Critical: automatic escalation to Compliance Officer and CISO.	CyberPlug + Compliance Officer
5	Remediation & Evidence	Fix applied; re-scan triggered; evidence attached to finding record (patch log, config change, test result).	Security Engineer + Asset Owner
6	Closure & Reporting	Finding closed in CyberPlug. Included in next compliance report. Exception documented if risk accepted.	Compliance Officer

3. Override Controls — Human-in-Command Functions

Function	Description	Authorised By	Logged In
STOP	Immediately halts all active scans and blocks new AI outputs. Used for systemic failure or rights violation.	CISO / AI Governance Lead	Human Interactions Log — Stop Event
PAUSE	Suspends AI recommendations for a specified asset or tenant while human review is conducted.	Compliance Officer, CISO	Human Interactions Log — Pause Event
DISREGARD	Marks a finding as disregarded with documented business justification. Preserved in audit trail.	Asset Owner, Security Engineer	Human Interactions Log — Disregard + justification

OVERRIDE	Replaces AI recommendation with human-determined action. Both AI recommendation and human rationale preserved.	Security Engineer, Asset Owner	Human Interactions Log — Override + rationale
REVERSE	Reverses a previously executed automated action. Dual authorisation required for Critical-tier reversals.	Asset Owner + Compliance Officer (dual auth)	Human Interactions Log — Reverse + dual sign-off

4. SD3 Checklist — Pending Items

Item	Status	Owner	Target Date
HR Integration — offboarding to RBAC deprovisioning sync	IN PROGRESS	HR Ops + Platform Eng.	May 30, 2026
HR Integration — contractor access review automation	PENDING	Security Eng.	June 15, 2026
Sustainability — carbon footprint baseline for scan compute	PENDING	Platform Ops	June 30, 2026
Sustainability — renewable energy usage reporting	PENDING	CTO Office	July 31, 2026
Sustainability — e-waste and hardware decommissioning policy	DRAFT	IT Operations	May 31, 2026