

Risk Assessment and Vulnerability Management Policy

Purpose

Your Organization cannot eliminate risk, but it can identify, prioritize, and manage it deliberately. This policy defines how Your Organization performs information security risk assessments, and how it discovers, prioritizes, and remediates technical vulnerabilities across its systems on a defined, auditable cadence.

Scope

This policy applies to all Your Organization information systems, applications, and infrastructure that store, process, or transmit company or customer data, and to the risk assessment and vulnerability management processes that cover them.

Risk assessment

- Your Organization conducts a formal information security risk assessment at least annually, and following material changes to its technology footprint, business model, or threat landscape.
- The risk assessment identifies threats and vulnerabilities to Your Organization systems and data, evaluates likelihood and impact, and produces a prioritized risk register with owners and treatment decisions (mitigate, accept, transfer, avoid).
- Risk assessment results inform the security roadmap, budget prioritization, and the policy review cycle across Your Organization's security program.
- Significant identified risks are reported to executive leadership, with residual risk explicitly accepted, mitigated, or escalated — not left undocumented.

Vulnerability scanning

- Your Organization performs automated vulnerability scanning of externally facing systems and internal production infrastructure on a recurring schedule (at minimum monthly for external-facing systems, and following significant infrastructure changes).
- Web applications and APIs handling Confidential or Restricted data undergo periodic application-layer security testing (e.g., DAST/SAST tooling, or third-party penetration testing) at least annually.
- New systems are scanned before being placed into production where feasible, and are added to the recurring scanning scope upon go-live.

Vulnerability prioritization

Identified vulnerabilities are triaged and prioritized using a risk-based approach that considers severity (e.g., CVSS score), exploitability, whether the affected system is internet-facing, and the sensitivity of data it handles — not solely the vendor-assigned severity rating.

Remediation timelines

Your Organization targets the following remediation windows from the time a vulnerability is confirmed, measured from discovery:

Severity	Internet-facing systems	Internal systems
Critical	7 days	15 days
High	15 days	30 days
Medium	30 days	90 days
Low	Best effort, tracked	Best effort, tracked

Vulnerabilities that cannot be remediated within the target window require a documented exception, compensating control, and re-assessment date, approved by Information Security.

Penetration testing

Your Organization commissions independent penetration testing of its production environment at least annually, or following a significant architecture change. Findings are tracked to remediation using the same prioritization and timelines as scan-identified vulnerabilities.

Third-party and supply chain risk

Vulnerability exposure introduced through vendors, open-source dependencies, and supply chain components is assessed as part of the Vendor Risk Management Policy and, for software dependencies, through software composition analysis tooling integrated into the development pipeline.

Tracking and reporting

All identified vulnerabilities and risk register items are tracked to closure in an Your Organization-approved system, with status visible to Information Security leadership. Remediation metrics (mean time to remediate, overdue items by severity) are reported to leadership on a recurring cadence.

Roles and responsibilities

- **Information Security.** Owns the risk assessment methodology, vulnerability scanning program, and remediation tracking.
- **Engineering and IT Operations.** Remediate vulnerabilities in systems they own within target timelines.
- **Executive Leadership.** Reviews significant risk register items and approves risk acceptance decisions above a defined threshold.

Review cadence

This policy is reviewed annually by Information Security, or sooner following a significant vulnerability event or a change in remediation SLA expectations from a customer or regulator.

Effective date: [the date this policy takes effect]