PUEBLO CITY-COUNTY Library District

www.pueblolibrary.org

INFORMATION TECHNOLOGY

05.03.01.P1 Software Licensing and Management Procedures

Software Request and Intake

All software must be formally requested prior to acquisition or installation. Requests must be submitted using the PCCLD Software Vetting Checklist and Intake Form and must include business justification, intended use, user scope, data classification, and deployment type. No software may be installed, purchased, or subscribed to outside this process.

Vendor and Security Review

The IT Department is responsible for reviewing vendor background, software security posture, and known vulnerabilities. This includes evaluation of vendor reputation, patch practices, support lifecycle, and publicly disclosed security issues. Software presenting unacceptable security or privacy risk may be denied or require documented risk acceptance.

Licensing Review

The IT Department evaluates software licensing models and terms, including usage limitations, audit rights, renewal requirements, and financial exposure. Licenses with unclear terms or aggressive audit enforcement may be escalated for additional review.

CAB Review and Approval

All software requests and IT findings are reviewed by the Change Advisory Board (CAB). The CAB makes recommendations on approval, denial, conditional approval, or risk acceptance. Approved software may only be deployed by the IT Department.

Testing and Pilot (When Applicable)

For high-impact or high-risk software, the IT Department may require limited pilot deployment, security testing, or compatibility validation prior to full approval.

Inventory and Ongoing Management

The IT Department maintains a centralized inventory of approved software and licenses. License usage and compliance are monitored periodically. Software renewals, vendor changes, and emerging risks are reviewed as part of ongoing management.

Exceptions and Enforcement

Exceptions to these procedures must be documented and reviewed/approved by the CAB, the Director of IT or Executive Director (or designee). Unauthorized or unmanaged software is subject to removal. Failure to comply with these procedures may result in disciplinary action.