SECURE SCANNING CHECKLIST

Use this checklist with your team to assess the security, compliance, and efficiency of your document scanning workflows. Together, identify any gaps, confirm audit readiness, and ensure you're protecting sensitive data. A secure, streamlined process isn't just required—it's a competitive edge you can stand behind.

1. Physical Document Handling

☐ Secure intake protocols with logged chain of custody

☐ Minimal manual prep (no cutting, taping, or sorting required)

☐ On-site scanning options for sensitive or restricted files

2. Scanner Capabilities

☐ Multi-feed detection (ultrasonic sensors, thickness measurement)

☐ Automatic image validation (skew, clarity, completeness)

☐ Support for intermixed documents (size, thickness, condition)

☐ Encrypted output file generation (PDF, TIFF, etc.)

3. Software & Image Processing

☐ Real-time audit trails for all scan jobs

☐ Role-based access control and user authentication

☐ In-line OCR/ICR for secure and accurate data extraction

☐ Batch tracking with timestamps, operator ID, and exception handling

4. Compliance Readiness

☐ HIPAA safeguards for PHI

☐ GDPR compliance for PII handling

☐ FADGI 3-Star readiness (where applicable)

☐ Configurable retention and deletion policies

5. Operational Safeguards

☐ Secure workstation setup with controlled access

☐ Regular maintenance and scanner calibration

☐ Staff trained on compliance and data security protocols

☐ Contingency plans for hardware failure or scanning interruption

6. Post-Scan Handling

☐ Secure file transfer to DMS/ECM systems

☐ Document classification, indexing, and metadata tagging

☐ Physical document disposal or storage according to client policy

NOW WHAT?

You've checked all the boxes—now it's time to put that secure foundation to work. Use this list to validate your process, show value to clients, and prepare to scale. Security isn't just about compliance—it's a tool for growing your business with confidence and control.

1. Validate with a Trial Audit

Conduct an internal audit using a sample job to ensure everything works as expected.

Confirm audit trails are complete and accessible.

Review image quality and metadata tagging against client or regulatory standards.

2. Document Your Process

Write a standard operating procedure (SOP) detailing your secure scanning workflow.

Include access controls, file handling procedures, and exception resolution protocols.

3. Schedule a Client Walkthrough

Demonstrate your secure scanning workflow to key clients or stakeholders.

Highlight your compliance measures and audit-readiness as a value-added service.

4. Monitor and Optimize

Use your system's analytics to track throughput, error rates, and operator performance.

Set KPIs (e.g., average time per scan, rework rate, audit turnaround) and aim for continuous improvement.

5. Prepare for Scale

With a secure foundation in place, you can now:

Take on higher-volume or more sensitive jobs (e.g., legal, healthcare, elections).

Pursue certifications (e.g., SOC 2, ISO 27001) or contracts that require demonstrated compliance.

Offer secure scanning as a differentiated service in RFPs and marketing materials.

By following these steps, you're not just maintaining a secure scanning operation—you're setting a higher standard for compliance, efficiency, and client trust. Keep refining your process, track your results, and use your security posture as a differentiator in every conversation. You're ready to lead with confidence.

OPEX®