FIRST DUE TECHNOLOGY

GOOGLE WORKSPACE API SECURITY AUDIT CHECKLIST

A Practical Review Guide for School Districts

Google Workspace powers instruction, communication, and identity across your district. Third-party API integrations can retain broad access to Gmail, Drive, Calendar, Admin SDK, and directory data. Without periodic review, these connections may introduce unnecessary risk.

1. OAUTH APPLICATION REVIEW

- Export full list of connected OAuth applications.
- Identify apps with Gmail, Drive, or Admin SDK scopes.
- Identify unverified third-party applications.
- Document business purpose for each application.
- Remove unused or unknown applications.
- Restrict high-risk scopes.

2. DOMAIN-WIDE DELEGATION REVIEW (HIGH PRIORITY)

- Record service account ID and associated vendor.
- List approved scopes.
- Confirm contract status and approving administrator.
- Remove delegation for expired vendors.
- Reduce scopes where possible.

3. DEFAULT ACCESS CONTROLS

- Set default third-party app access to Restricted.
- Require admin approval for new OAuth apps.
- Limit high-risk scopes (Admin SDK, full Gmail access).
- Establish written vendor API access policy.

4. LOGGING & MONITORING

- Enable OAuth token activity logging.
- Enable Admin activity alerts.
- Configure alert for new domain-wide delegation.
- Configure alert for suspicious OAuth authorization.
- Schedule quarterly API review reminder.

5. VENDOR GOVERNANCE

- Document scope justification for each vendor.
- Tie access to contract term.
- Schedule annual review.
- Define removal process.
- Assign internal ownership.

EXECUTIVE SUMMARY TEMPLATE

After completing your review, summarize: • Total OAuth apps reviewed • Number removed • Delegations reduced • Policy changes implemented • Monitoring improvements enabled This documentation supports cyber insurance renewals, E-Rate readiness, and board-level reporting.