SOC 2 Mini Readiness Checklist

Tailored for Small SaaS Startups by Impact Risk Advisors

1. Scoping

- [ ] Identify customer data you store/process/transmit
- [ ] List in-scope systems (MS 365, Google Workspace, VPN, antivirus, backups)
- [ ] Identify vendors and service providers
- [ ] Decide: SOC 2 Type I (point in time) or Type II (operating over time)
- [ ] Document business-critical services and who uses them

2. Policies & Required Documents

- [ ] Information Security Policy (includes Acceptable Use, BYOD, Encryption, etc.)
- [ ] Access Control Policy
- [ ] Risk Management Policy
- [ ] Vendor Risk Management Policy
- [ ] Incident Response Plan
- [ ] Business Continuity / Disaster Recovery Plan
- [ ] Data Retention & Disposal Policy
- [ ] Change Management / SDLC Policy (if you develop software)
- [ ] Employee Handbook

3. Security Controls

- [ ] Enforce MFA (Microsoft 365, Google Workspace, VPN, etc.)
- [ ] Use Password Manager (e.g., Dashlane, 1Password)
- [ ] Install Antivirus / EDR on all devices
- [ ] Use a VPN for secure remote access
- [ ] Ensure Data Encryption (at rest and in transit - document how cloud vendors handle this)
- [ ] Establish Backup process (native or third-party)
- [ ] Create and follow an Employee Offboarding Checklist

4. Documentation & Evidence

- [ ] Version-controlled policy set with owner, approver, and review dates

- [ ] System log reviews (e.g., admin audit logs in Google/Microsoft)
- [ ] Spreadsheet or tracker for vendor reviews
- [ ] Risk register (even a simple one)
- [ ] Logs or screenshots showing MFA enforcement
- [ ] Results from incident response and DR tests
- [ ] Documented change logs or approvals (even in GitHub, Jira, or Notion)

5. Ongoing Compliance Activities

- [ ] Monthly: Review logs or security events (admin portals, antivirus)
- [ ] Monthly/Quarterly: Review access lists and remove unused accounts
- [ ] Annually: Risk assessment, Policy reviews, DR testing, Phishing test or training, Employee handbook acknowledgement

6. Security Awareness & Physical Security

- [ ] Provide basic security training (can be free or informal)
- [ ] Conduct phishing awareness - use free simulations if possible
- [ ] If physical office exists: restrict access, secure devices, use visitor policy or sign-in