SIRIUS STAR

BEST TECH • BRIGHT FUTURE

SIRIUS STAR ENTERPRISE TECHNOLOGIES

Your First 30 Days of Data Safety

A week-by-week plan for SMB manufacturers. No new hires required.

After 200+ Data Leakage Protection setups at industrial SMBs across Maharashtra and Gujarat, this is the exact 30-day plan we hand to every new client. Print it, pin it, work through it.

200+

DLP Setups

Completed at industrial SMBs across Maharashtra and Gujarat

30

Days to Baseline

From zero visibility to three working controls and a clean exit process

4

Weekly Phases

Discovery, controls, exit protocols, and DPDP-readiness handoff

WEEK ONE & TWO

Find out what you have, before you protect anything.

You cannot secure what you have not mapped. The first two weeks are entirely about building an honest picture of where customer data actually lives in your business — not where it is supposed to live.

Day 1–3: Device Inventory

Inventory every device that touches customer data. Laptops, desktops, the CCTV NVR, that one pen-drive. If it has data on it or passes data through it, it goes on the list.

Day 4–7: Data Location Audit

List every place customer data lives. Tally, Gmail, WhatsApp Web, the shared Google Drive, USB backups, the CA's laptop. Document it without judgement — accuracy matters more than appearances.

Day 8–10: Key-Person Interviews

Interview the 3 people who handle the most data. Where do they save it? Who do they share it with? These conversations will surface more risk than any automated scan.

Day 11–14: Build the Data Map

One spreadsheet. Three columns: **what / where / who has access.** This single document becomes the foundation of every control you build in the weeks that follow.

Output of Week 1–2: A data map that reflects reality, not policy. Most SMB manufacturers discover 3–5 storage locations they were not aware of. That is normal, and it is exactly the point.

WEEK THREE

Three controls that block 80 per cent of accidental leaks.

You do not need a ₹10 lakh DLP platform to stop most accidental leaks. These three controls are native to tools you already pay for, and every one of them can be live within a week.

1. Email Outbound Rule

Block sending of files larger than 5MB to non-domain recipients without manager approval. This is a native rule in both Microsoft 365 and Google Workspace — no additional licence required. Set it, test it, document it.

2. USB Block at OS Level

Group Policy on Windows. Approximately 10 minutes per machine. Free. This single control closes the most common physical exfiltration path in manufacturing environments — the pocket-sized pen-drive that leaves with an employee.

3. WhatsApp Web Policy

Disable on company laptops via browser policy. For phones: company-issued only, not personal. This is not about distrust — it is about ensuring customer data does not transit an unmanaged personal device with no audit trail.

Why these three first: Email, USB, and WhatsApp Web account for the overwhelming majority of unintentional data leaks in SMB manufacturing. Begin here, make them reliable, then layer additional controls on top.

WEEK FOUR

Exit protocols and the DPDP-readiness handoff.

The most overlooked risk in any SMB is not the current employee — it is the one who left six months ago and still has access. Week 4 closes that door and sets up the rhythm that keeps it closed.

Employee Offboarding Checklist

12 steps from access revocation to exit interview. Every leaver, no exception. This includes contractors, interns, and agency staff. The checklist is not optional — it is the control.

Vendor Data-Access Audit

Who has remote access to your systems? When was it last reviewed? Document every vendor, their access scope, and the date of last review. This is the item most commonly flagged in customer cybersecurity audits.

Quarterly Review Calendar

30 minutes every quarter with the leadership team. What changed? What broke? What is next. Schedule it now, before Day 30 arrives. A data safety programme without a review cadence is a document, not a practice.

AFTER 30 DAYS

Visibility, three working controls, and a clean exit process.

By Day 30 you have something most SMB manufacturers in your peer group do not: a documented picture of where your data lives, three enforced controls blocking the most common leak paths, and a formal process for when people leave. That is a meaningful baseline.

The next 30 days are about deepening — incident-response drills, the breach-notification one-pager required under DPDP, and employee training rollout. That is where Sirius Star comes in. We have run this programme at 200+ sites and we can run it at yours.

Free 1:1 30-min Data Risk Audit
Book a session and we will walk through your data map against the DPDP baseline — at no cost and no obligation.

siriusstar.in/audit | sudeep@siriusstar.in | +91-96996-05668