LERNER SOLUTIONS

# CHEATSHEET IT FOR NEW LOCATIONS

## 1 Process & Project Management

The most expansion failures are coordination failures, not technical ones. Clear ownership, disciplined handoffs, and tight change control matter more than tool choice once construction starts.

### The 4 Phase Process

Most IT delays come from treating technology as a punch-list item rather than a parallel workstream. These four phases are designed to run alongside construction — not after it. Every phase has decisions that must be locked before the next phase starts

**Design Set**
- Floorplan + scope review
- ISP research + order placed
- Equipment list finalized
- Network architecture designed
- Cabling plan created
- AV + access control scope se

**Construction Set**
- Final floorplan confirmed
- Cabling spec issued to GC
- Equipment staging ordered
- ISP install date confirmed
- Vendor schedules locked

**Pre-Install Coordination**
- Final floorplan confirmed
- Cabling spec issued to GC
- Equipment staging determined
- Procurement with lead times
- ISP install date confirmed
- Vendor schedules locked

**Field Installation**
- Final floorplan confirmed
- Cabling spec issued to GC
- Equipment staging ordered
- ISP install date confirmed
- Vendor schedules locked

### Project Management

IT success during expansion is less about technology choices and more about execution discipline. Most failures do not come from choosing the wrong hardware or platform; they come from unclear ownership, missed handoffs, and decisions drifting downstream into the field. Without tight coordination, IT decisions get made implicitly—by architects, GCs, or installers, often without full context, which leads to expensive rework.

- **Explicit Ownership:** Clearly define which stakeholders own design, procurement, configuration, and field validation to eliminate accountability gaps.
- **Scope Boundaries:** Document clear lines of responsibility between IT, Facilities, and external vendors to prevent "mid-build" surprises.
- **Field Trust but Verify:** Use trusted technicians for repeating work to ensure the "Lerner Standard" is maintained without constant oversight.

## Top 10 Things That Go Wrong

- ⚠️ IT is brought in after architectural drawings are already finalized.
- ⚠️ Key design decisions live in emails, tickets, or tribal knowledge.
- ⚠️ Device placement, mounting, power, & cable paths are solved in the field.
- ⚠️ Vendors design AV, security, access control, and specialty systems in isolation.
- ⚠️ ISP strategy is treated as procurement instead of a design dependency.
- ⚠️ Carrier lead times are ignored until the site is nearly ready to open.
- ⚠️ Hardware choices drift across sites, creating SKU and firmware variance.
- ⚠️ Rack, PoE, UPS, and switch capacity are undersized for future growth.
- ⚠️ Network segmentation differs across comparable sites.
- ⚠️ Sites open without formal validation of network, devices, and critical systems.

## 2 Design

IT design defines the big decisions that must be locked before construction and installation begin. Its job is to translate business context into a repeatable technical intent that can be executed consistently across sites.

### Technical Design Standards & Recommendations

| Parameter | Recommendation | Why it Matters | Allowable Exception |
|---|---|---|---|
| **Mounting Heights** | Explicitly specified per device and per location | Eliminates field guesswork and ensures brand aesthetic across 100+ sites. | ADA-specific requirements or landlord-mandated height restrictions. |
| **Closet Minimums** | 4' x 6' footprint; No shared storage with janitorial/wet utilities. | Prevents hardware overheating and accidental water/chemical damage. | Micro-sites using secure, ventilated wall-mount swing racks. |
| **Rack Orientation** | Side-mount or Center-room; 36" front clearance. | Ensures technicians can service cabling without dismantling the rack. | Shallow 2-post racks in space-constrained closets. |
| **Ceiling Mounts** | T-Bar clips for drop ceilings; Threaded rod for open-plenum. | Prevents "drifting" APs and cameras; ensures rigid alignment for AV. | Industrial warehouses requiring custom beam-clamp mounts. |
| **Termination** | Category 6; ANSI/TIA-568-C.2 B-Wiring standard. | Standardizes signal pair logic for remote cable testing and POE delivery. | Existing legacy cabling (must be tested/certified to pass). |
| **UPS Strategy** | Double-Conversion Online; Minimum 30-min runtime at 50% load. | Cleans "dirty" power and ensures transaction continuity during brownouts. | Temporary pop-ups using basic surge-protected power strips. |
| **Thermal Load** | Mandatory BTU/hr calculation; 24/7 dedicated cooling. | Prevents equipment throttling during off-hour HVAC setbacks. | Uncooled closets allowed only for passive gear. |
| **Conduit Diameter** | Explicitly specified on wire schedule & fill calculations | Ensures enough "pull-space" for future fiber or additional cabling. | 0.5" flex allowed for short "last-inch" drops to furniture. |

### 💡 The 15% Capacity Rule

Every rack and patch panel should be designed with 15% open capacity. This prepares for specialty tech (sensors, AI cameras, new POS) that will be added mid-lease; the cost of over-provisioning a rack today is 1/10th the cost of an uprade later.

### What Must Appear on Design Plans?

**Devices & Systems**
- Device type and role
- Device quantity per area
- Association to system class

**Device Placement & Mounts**
- Exact placement, not just schedule
- Mounting surface and orientation
- Mounting heights by device type

**Pathways & Cabling**
- Conduit routes and sizes
- Homerun vs consolidated cabling strategy
- Service loop expectations

**Power & Electrical**
- Circuit quantity and type per rack
- Protected vs unprotected loads
- PoE budget assumptions per switch
- UPS placement and supported equipment

**Ceiling & Mounting**
- Mounting heights by device type
- Ceiling condition (ACT, hard lid, open)
- Backing or bracing requirements
- Plenum vs non-plenum cabling assumptions

**Closes, Racks, & Layout**
- Exact rack location and orientation
- Front and rear service clearances
- RU allocation by system class
- Wall-mounted vs floor-mounted
- Door swing conflicts resolved

### Practical Tips & Advice

**Serviceability Zones** — Drawings must include a "Hatched Service Zone" (36" deep) in front of all racks. This provides a visual "No-Fly Zone" for other trades (plumbing, electrical) to prevent encroachment on the IT service path.

**MPOE Pathing** — Don't let the carrier "figure it out." Specify the exact 2" conduit path from the street to the MDF on the site plan; without this, carriers will take the path of least resistance, often creating "nightmare" cable runs through public spaces.

**BOH Drop Density** — Always double the data drops at the manager's station and staging areas. Underspecifying Back-of-House (BOH) leads to the "Spiderweb Effect"—unmanaged 5-port switches and power strips that become the highest source of failure.

**Growth Headroom** — Growth headroom must be explicitly reserved across core systems (rack space, switch capacity, PoE budget, AP density, and power) so expansion does not require redesign or field retrofits.

## 3 ISP Strategy

Design ISP connectivity for failure, not optimism. Default to dual-path internet where downtime matters, prioritize symmetric business-class circuits, and treat LTE/5G as failover—not primary. If the site can't survive an ISP outage, rethink the strategy

### Circuit Standards by Site Context

**Large Office / HQ**
- **Primary Circuit:** Dedicated Fiber (DIA)
- **Secondary Circuit:** Business Broadband Fiber

**Small Office**
- **Primary Circuit:** Business Broadband Fiber
- **Secondary Circuit:** LTE / 5G Failover

**Show Room**
- **Primary Circuit:** Business Broadband Fiber
- **Secondary Circuit:** LTE / 5G Failover

**Warehouse**
- **Primary Circuit:** Dedicated Fiber (DIA)
- **Secondary Circuit:** Business Broadband Fiber

**Retail Store**
- **Primary Circuit:** Business Broadband Fiber
- **Secondary Circuit:** LTE / 5G Failover

**Restaurant**
- **Primary Circuit:** Business Broadband Fiber
- **Secondary Circuit:** LTE / 5G Failover

### ISP Strategy Readiness Checklist

- ☐ **Physical Path Diversity**
  Confirm primary and secondary circuits enter the building through different conduits to prevent a single backhoe cut from taking down both links.
- ☐ **Static IP Allocation**
  Ensure the primary Fiber circuit includes a /29 or at least one static IP to maintain stable VPN tunnels and remote management reach-back.
- ☐ **Cellular Penetration**
  For sites relying on LTE/5G failover, verify signal strength inside the MDF; if signal is below -90dBm, consider alternative plan.
- ☐ **Contract Lead Times**
  Align fiber install dates with the "Power On" date; if the carrier quote exceeds 90 days, immediately trigger the cellular hardware as the "Day-1" temporary primary.

## 4 Network Engineering

Engineer the network for predictable failures and scale, not theoretical elegance. Standardize segmentation, routing, and QoS patterns so sites behave the same under load and during outages. If behavior differs by site, troubleshooting will fail.

### Network Engineering Patterns by Site Type

| Site Type | Hardware Redundancy | Network Segmentation | Security Policy |
|---|---|---|---|
| **Large Office** (HQ / Regional) | Redundancy in MDF and all IDFs. Redundant edge and critical switching, UPS for core gear, redundant MDF–IDF uplinks. | Function-based VLANs for Corp, Voice, Guest, Exec, Security, AV, and IoT. Designed to scale across floors and IDFs. | Strict isolation between segments. Guest is internet-only. Management access limited to IT admins with centralized logging. |
| **Warehouse / Industrial** | MDF doubled where downtime stops ops. IDFs may use single switches unless justified. Redundant edge only for critical sites. UPS for MDF/core. | Minimal VLANs (Corp, Scanners, OT, Security). OT (robotics/conveyors) and Scanners (WMS tools) are separated to ensure low-latency performance. | OT is logically isolated from Corp to prevent lateral movement. Scanners limited to required services. Guest access typically disabled. |
| **Showroom / Small Office** | No blanket redundancy. Single firewall, switch, and APs. Add redundancy only where revenue impact requires. UPS for edge/switching. | Simple segmentation on the firewall. Small number of VLANs separated by firewall (e.g., data, POS, AV, physical security, guest, infrastructure) | Block guests from everything but public internet. Employees lack access to POS and backend infrastructure. |
| **Retail / Restaurant** | | | Guests internet-only. Limited employee access to AV and surveillance. No employee access to POS or core infra. |

### Core Engineering Standards

These standards define the non-negotiable network behaviors every site must exhibit, regardless of size or location. They exist to constrain blast radius, prevent lateral movement, and ensure issues can be diagnosed and fixed remotely without site-specific knowledge.

**Layered Segmentation** — Separate Corp, Guest, Devices, AV, and Management into distinct segments to prevent cross-domain impact during outages or compromises

**Policy at the Edge** — Enforce access by role and segment at the boundary rather than relying on endpoint settings or user behavior

**Templatized Configs** — Require every site to inherit from a standard baseline; deviations must be justified and tracked to prevent drift

**Fail Closed** — Place unknown or misclassified devices into restricted segments by default rather than granting broad access due to misconfig

### Network Readiness Checklist

- ☐ **Segmentation Enforced**
  Verify device classes land in correct segments &cannot laterally traverse.
- ☐ **IP Overlap Prevention**
  Verify that the new site's IP range does not conflict with existing HQ or VPN-connected sites to prevent routing "black holes".
- ☐ **IP Space Allocation**
  Ensure network segments are sized for 2x the anticipated peak client count.
- ☐ **Wifi Validation Survey**
  Ensure that wifi signal is strong across all required locations.
- ☐ **Perform Failover Tests**
  Simulate ISP and power failures and confirm critical systems still operate.
- ☐ **Quality of Service (QoS) Verified**
  Stress test with bulk traffic to confirm voice and video remain stable.

### Wireless Engineering Defaults

- **SSIDs by Function:** Use dedicated SSIDs for Corporate, Guest, and Headless Devices (IoT) to ensure authentication methods and security policies match the specific usage.
- **Enterprise Authentication:** Mandate certificate-based or SSO-backed authentication for the Corporate SSID to eliminate shared credentials and improve auditability.
- **Minimum RSSI Enforcement:** Enforce strict signal thresholds to prevent "sticky clients"—where a device stays connected to a distant AP—which reduces roaming-related performance issues.
- **Plan for Stability:** Prefer lower channel widths to avoid WiFi interference and collisions.
- **Plan for Future:** Prefer using WiFi 7 capable WAPs

## 5 Systems & Hardware

Hardware decisions are context-dependent. The right hardware for a showroom, restaurant, warehouse, or office is different—but within each context, hardware should be standardized aggressively to preserve speed, supportability, and scale.

### Core Systems

Networking, power delivery, and physical infrastructure form the utility layer of each site and must be standardized aggressively to ensure durability, remote manageability, and consistent installs.

| Component | Large Office (HQ/Regional) | Warehouse / Industrial | Showroom / Small Office | Retail / Restaurant |
|---|---|---|---|---|
| **Firewall / Router** | Meraki MX95/105 | Meraki MX85/95 | Meraki MX67/68 | Meraki MX67C/MX67CW |
| **Switch** | Meraki C9300 | Meraki MS130/150 | Meraki MS130 | Meraki MS130 |
| **Access Points** | Meraki CW9176I | Meraki CW9176I/MR46E | Meraki MR46/CW9172I | Meraki MR46/CW9172I |
| **UPS / Power** | Eaton Cloud-Connected UPS (1500VA) | Eaton Cloud-Connected UPS (1500VA) | Eaton Cloud-Connected UPS (750/1000VA) | Eaton Cloud-Connected UPS (750/1000VA) |
| **Mgmt / Monitoring** | Cloud Dashboards | Cloud Dashboards | Cloud Dashboards | Cloud Dashboards |

### Integrated Systems

These systems fail disproportionately when treated as "facilities problems." The objective is to standardize platforms, power, and management so installs are repeatable and issues are diagnosable remotely.

| System | Large Office (HQ/Regional) | Warehouse / Industrial | Showroom / Small Office | Retail / Restaurant |
|---|---|---|---|---|
| **Cameras** | Verkada Dome (Indoor) / Bullet (Outdoor) | Verkada Bullet (High Retention/IK10 Rugged) | Verkada Dome (Standard) | Verkada Fisheye (360° Coverage) |
| **Access Control** | Verkada AC Controllers w/ HID Signo Readers | Verkada AC Series w/ Rugged Readers | Verkada AC Series (Cloud Managed) | Verkada AC Series (Mobile Credential Optimized) |
| **Meeting / AV** | Logi Rally Bar (Large) / Dual Displays | N/A (or Wall-Mount Tablet for Check-in) | Logi Rally Bar Mini (Huddle Rooms) | N/A (or Overhead Audio Interface) |
| **Signage** | Apple TV / BrightSign (Dual Screen) | BrightSign (High-Brightness Displays) | Apple TV (4K / MDM Managed) | Apple TV (Fixed Content Kiosk) |

### 💡 The 25% PoE Rule

Every switch should maintain at least 25% unused PoE capacity after accounting for APs, cameras, access control, and other powered devices. This preserves room for future devices and prevents expensive switch replacements when the site expands.

### Practical Tips & Advice

**SKU Discipline** — Standardize approved hardware models by site type so replacements, firmware, spares, and support procedures stay consistent across locations.

**Pre-Stage Hardware** — Configure, label, update, and test firewalls, switches, WAPs, cameras, controllers, and AV gear before shipping to the site.

**Accessories** — Validate mounts, brackets, injectors, power supplies, patch cables, SFPs, antennas, licenses, and adapters before install day.

**Firmware Alignment** — Keep core hardware on approved firmware versions so new sites do not introduce unstable releases or platform mismatches.

**Spares Strategy** — Maintain a standard spare kit for common failure points such as WAPs, switches, power supplies, SFPs, cameras, and access-control components.

**Asset Tagging** — Label every core device with site, location, role, MAC/serial, and management platform ID so support can identify hardware remotely.

### Security Controls by Site Type

| Site Type | Identity & Access | Network & Physical Protections |
|---|---|---|
| **Large Office** (HQ / Regional) | MFA-backed mobile credentials for employees; automated access reviews on role change; no shared or standing admin accounts | Full east-west controls; certificate-based Corp Wi-Fi; management and security systems isolated from user networks |
| **Warehouse / Industrial** | Primary identity model optimized for scanners and logistics accounts; ruggedized readers; vendor and admin access time-bound and audited | Hardened north-south controls; IoT/scanner devices restricted to VLANs; no direct Corp or management access |
| **Showroom / Small Office** | Cloud-managed scheduling for vendor access; guest identities isolated and non-persistent | Guest Wi-Fi client isolation; peer-to-peer blocked; AV/demo systems restricted to outbound-only access |
| **Retail / Restaurant** | Locked-down kiosk mode for POS; strong identity for managers only; no shared store credentials | PCI traffic isolated from non-payment systems; POS separated from Guest, Store, and Management; no shared routing |

## 6 Installation

The field installation phase is where design intent meets physical reality. The most common failure is treating install as "just plug it in" so that problems that should have been caught in staging get discovered on opening day.

### Go-Live Process & To-Do's

**Off-Site**
- Update firmware before shipping
- Apply site config templates
- Label hardware with site code
- Build shipping manifest
- Confirm site readiness with GC

**During Install**
- Verify power, conduit, MPOE on arrival
- Run and certify cabling first
- Rack, mount, and dress hardware
- Enroll network gear in dashboard
- Bring up ISP; validate failover
- Enroll APs, cameras, access control

**Go-Live**
- Run full validation checklist
- Test all VLANs
- Confirm camera recording active
- Verify POS connectivity
- Stress-test failover path
- Walk site; get sign-off

**Hand-Off**
- Deliver as-built network diagram
- Hand off site runbook
- Confirm alerts live
- Document credentials and assets
- Brief site ops on escalation path

### What's Most Likely to Go Wrong?

- **Explicit Ownership:** Installers make on-the-spot changes to mounting, placement, or cabling when drawings are incomplete or inconvenient, creating variance that is hard to unwind later.
- **Scope Boundaries:** Devices show up unconfigured, unlabeled, or mismatched to the drawings, slowing installs and increasing configuration errors under time pressure.
- **Field Trust but Verify:** IT work begins before power, ceilings, or finishes are ready, forcing rework and last-minute compromises to stay on schedule.
- **Field Trust but Verify:** Sites open without systematic testing of network, devices, and integrated systems, pushing avoidable issues into live operations.

## 7 Management

Opening day is the beginning of the operational relationship, not the end of the project. The sites that perform best long-term have defined support ownership, active monitoring, and a structured change process.

### Security Controls by Site Type

| Sensitivity Context | Observability Standard | Spares Strategy | Field Response Model |
|---|---|---|---|
| **Low Sensitivity**<br>• Pop-ups<br>• Small Offices | **Reactive:** Basic cloud-dashboard alerts and email notifications for offline status. | **Next-Day Shipping:** No on-site inventory; rely on vendor RMAs and standard shipping. | **Remote-First:** Troubleshooting is handled 100% centrally; no dedicated field dispatch. |
| **Medium Sensitivity**<br>• Showrooms<br>• Standard Retail | **Proactive:** Real-time dashboard monitoring with automated ticketing for critical failures. | **On-Site "Crash Kit":** Local storage of high-fail, low-cost items (cables, power bricks, peripherals). | **On-Ground Partner:** Tier 1 support dispatched via local partner with a 24-hour SLA. |
| **High Sensitivity**<br>• Volume Transactions<br>• Medical<br>• Specialty | **Predictive:** Heartbeat monitoring and "Visibility Tests" to diagnose issues before site awareness. | **Full Cold Spares:** On-site backup for mission-critical gear (Firewalls, Switches, POS terminals). | **Priority Field Engineering:** Dedicated internal or elite MSP response with a 4-hour on-site SLA. |

## Go-Live Checklist

- ☐ All ISP circuits are live and tested.
- ☐ Failover connectivity works by simulating a primary circuit outage.
- ☐ Network gear is online, healthy, and passing traffic.
- ☐ Required SSIDs are broadcasting on the correct segments.
- ☐ POS and payment systems process transactions successfully.
- ☐ Access control users, badges, doors, and schedules are enrolled and tested.
- ☐ Cameras are live, recording, and viewable remotely.
- ☐ Phones, voice, and any shared site lines can place and receive calls.
- ☐ Printers, scanners, receipt printers, and other operational devices work.
- ☐ Staff devices are imaged, enrolled, patched, and able to access required apps.
- ☐ Critical SaaS, VPN, file access, and line-of-business systems are reachable.
- ☐ Rack power, UPS status, and protected loads are healthy.
- ☐ Remote monitoring is active for circuits, network gear, UPS, and critical systems.
- ☐ Escalation path is documented for IT, ISP, POS, security, and vendor issues.
- ☐ On-site tech coverage is scheduled and contactable for opening-day support.