CompTIA ITF+ (FC0-U61) — One-Page Study Guide

A) Exam Snapshot

Exam: FC0-U61 (CompTIA ITF+)
Max questions: 75
Time limit: 60 minutes
Question types: Multiple choice
Passing score: 650 (scaled score; 900 max)
Renewal: [VERIFY: whether ITF+ is good-for-life/no CE renewal]

B) Domain Weights

Domain	Weight
1. IT Concepts & Terminology	17%
2. Infrastructure	22%
3. Applications & Software	18%
4. Software Development	12%
5. Database Fundamentals	11%
6. Security	20%

C) Core Workflow (How the exam thinks)

- Frame the scenario: goal, constraints, and what 'success' looks like.
- Identify the domain: hardware, operating system, networking, apps, databases, or security.
- Translate key terms: units, protocols, file types, and service models.
- Choose the best next step: low-risk checks before big changes.
- Validate: confirm connectivity, performance, permissions, and data accuracy.
- Document and communicate: symptoms, steps tried, results, and escalation notes.
- Apply safety and security basics: least privilege, backups, and malware hygiene.

D) High-Yield Concepts

- Data units: bit vs byte; KB/MB/GB; Mbps vs MBps.
- Numbering basics: binary and hexadecimal; ASCII vs Unicode; file extensions.
- Hardware roles: CPU, RAM, storage, motherboard, power, peripherals.
- Device types: desktop, laptop, mobile, and IoT; virtualization and cloud basics.
- Networking: IP vs MAC; what DNS and DHCP do; wired vs wireless tradeoffs.
- Operating systems: purpose, processes/services, drivers, patches and updates.
- Applications: local vs web vs SaaS; licensing types (open-source vs commercial).
- Troubleshooting method: identify, theory, test, plan, verify, document.
- Software development: logic, variables, loops; compiled vs interpreted.
- Databases: tables, records, fields; primary vs foreign keys; basic queries.
- Security: confidentiality/integrity/availability; authN vs authZ; phishing and malware basics.

E) Common Traps

- Treating Mbps and MBps as interchangeable (speed vs file size).
- Confusing RAM (temporary) with storage (persistent).
- Mixing IP address (logical) with MAC address (physical).
- Skipping the simplest cause first (power, cable, mute, airplane mode).
- Confusing encryption (reversible with key) with hashing (one-way).
- Mixing authentication (who) with authorization (what access).
- Choosing 'reinstall/replace' before checking settings or compatibility.
- Overlooking safety steps (ESD handling, battery removal, proper disposal).

F) Cheat Sheet

- 8 bits = 1 byte; watch decimal vs binary prefixes. [VERIFY: expected unit conventions in questions]
- Identifiers: file path (local) vs URL (web) vs IP address (network).
- Cloud models: IaaS/PaaS/SaaS (who manages what).
- Networking quick map: DNS = name lookup; DHCP = address assignment; HTTPS = encrypted web.
- Backup types: full vs incremental vs differential (what changes each time).
- Security basics: longer passphrases and MFA concepts beat short complex strings.
- Database keys: primary key is unique; foreign key links tables.
- SDLC phases: requirements, design, development, testing, deployment, maintenance.
- Common artifacts: screenshot + error code, change note, ticket history, basic logs.
- RAID: redundancy vs performance. [VERIFY: RAID depth expected for ITF+]

G) Exam-Day Tactics

- First pass: aim for about 45 seconds per question; mark the rest for review.
- Read the last line first (what is being asked), then scan the scenario.
- Eliminate two wrong answers quickly; choose the best remaining option.
- Watch for absolutes (always/never) unless the question signals a strict rule.
- For troubleshooting, pick the least disruptive step that could confirm the cause.
- If two answers feel close, choose the one that matches the stated symptom.
- Use remaining time on flagged items; do not change answers without a clear reason.
- Check the clock at 30 and 45 minutes to keep pace. [VERIFY: on-screen timer behavior]

H) 30-Minute Final Review Plan

- 5 min: scan domain weights and re-read notes from the weakest domain.
- 7 min: units/numbering and basic networking (DNS, DHCP, IP vs MAC).
- 7 min: operating systems and apps (updates, drivers, cloud models, licensing).
- 5 min: databases and software development definitions (keys, queries, logic).
- 4 min: security essentials (CIA, authN/authZ, phishing, malware).
- 2 min: common traps and exam-day tactics; set a steady pace plan.