FreshFlow FMCG

Global IT Support Operations Manual

Confidentiality: Internal Use Only

Document Control Number: IT-OPS-AIT-2026-V1

Last Updated: 19 January 2026 (Australia/Melbourne)

This manual consolidates the Global IT Standard Operating Procedures (IT-OPS-2026-V3) and the AIT Support Chatbot handover into an operationally complete, enterprise-grade runbook.

Owner	Global IT Operations
Primary Audience	Service Desk (L1), Infrastructure Specialists (L2), Global Engineering (L3)
Related Documents	IT-OPS-2026-V3 (SOP), Project Handover: AIT Support Chatbot
Change Control	All changes require approval under the IT Change Management Policy

Revision History

Version	Date	Author/Team	Summary of Changes
V1.0	2026-01-19	IT Operations	Initial consolidated manual (SOP + AIT Support Dashboard operations).

Table of Contents

In Word: References > Table of Contents > Insert/Update Table to generate the TOC automatically from headings.

1. Purpose and Scope

This manual defines the end-to-end operating model for FreshFlow IT Support across office users, warehouse operations, and corporate systems. It standardizes intake channels, prioritization, triage, escalation, resolution, documentation, and service reporting. It also provides an operations guide for the AIT Support Dashboard (a Retrieval-Augmented Generation IT support assistant) including knowledge lifecycle management and human-in-the-loop escalation via Microsoft Teams.

In scope

- End-user support for corporate office and warehouse operations (devices, connectivity, collaboration tools).
- Warehouse hardware and automation support (RF scanners, label printers, forklift terminals).
- Business application support entry point (SAP S/4HANA and related printing).
- Security, onboarding/offboarding, and phishing response processes.
- AIT Support Dashboard operations (RAG knowledge ingestion, escalation logic, controls, and monitoring).

Out of scope

- Engineering design for core SAP modules (handled by Global Engineering except for defined L1/L2 runbook actions).
- Non-standard local software development outside approved toolchains and governance.
- Unapproved AI tools and any processing of PII or customer pricing data in non-approved platforms.

2. Operating Model and Roles

FreshFlow uses a three-tier support model with clear escalation criteria and defined responsibilities.

2.1 Support Tiers

Tier	Role	Typical Scope	Examples
L1	Service Desk	Standard diagnostics and common fixes	Password resets, printer jams, basic software installation
L2	Infrastructure Specialist	Complex incidents, infra diagnostics, warehouse hardware, AI tool configuration	Network outage triage, server alerts, complex hardware, AIT escalation
L3	Global Engineering	Core platform and major incidents	SAP core failures, cyberattacks, data center outages

2.2 RACI (High-level)

Activity	End User	L1	L2	L3
Incident intake and initial details	R	A	C	C
Standard troubleshooting	C	A/R	C	C
Infrastructure and complex hardware resolution	C	C	A/R	C
SAP core remediation / hotfix	C	C	C	A/R
Security incident response	C	C	A/R	A/R
Knowledge base updates (AIT)	C	C	A/R	C

Legend: R = Responsible, A = Accountable, C = Consulted.

3. Support Channels and Hours

FreshFlow provides multiple channels. Users should start with self-service (AIT) unless the issue is safety-critical or requires immediate escalation.

3.1 Primary Channels

- AIT Support Dashboard (chat-based support with knowledge retrieval).
- Self-Service Portal for password resets and standard access requests.
- Microsoft Teams video support to the L2 on-call queue (authorized use cases only).
- Ticketing system (including High-Priority ticketing outside video support hours).

3.2 Hours of Operation (Video Support)

- Monday to Friday, 08:00 to 18:00 (AEST).
- Outside business hours: users must log a High-Priority ticket; on-call response follows the priority and severity policy.

4. Incident Management: Priorities, SLAs, and Communication

This section defines how incidents are prioritized and how response and resolution targets are managed. Where the SOP specifies exact timelines (e.g., SAP admin unlock), those values are mandatory. For areas not specified in the SOP, FreshFlow applies operational defaults that can be tailored per business unit.

4.1 Priority Matrix

Priority	Business Impact	Examples	Target Response	Target Restore/Workaround
P1	Safety risk or major outage	Smoke/fire from equipment, warehouse unable to ship, network outage	15 minutes	1 hour
P2	High impact to critical users or processes	SAP printing blocked, Wi-Fi authentication failures for multiple users	30 minutes	4 hours
P3	Moderate impact, workaround available	Teams device issues, OneDrive sync errors	4 business hours	2 business days
P4	Service request / low impact	Software install request, how-to guidance	1 business day	5 business days

4.2 Mandatory SLA: SAP Admin Unlock

SAP password lockout occurs after three failed attempts. Users should self-unlock via Fiori Launchpad. If admin unlock is required, the ticket subject must be "SAP UNLOCK - [Username]" and the SLA is 15 minutes.

4.3 Communications Standard

- P1/P2 incidents require user impact statement, next update time, and mitigation steps in the ticket within 15 minutes of classification.
- Major incidents should be announced in the relevant Teams channel (or incident channel) with an incident ID and owner.
- Post-incident, publish a brief RCA summary for P1 and recurring P2 incidents, including preventive actions and knowledge updates.

5. Network Infrastructure and Connectivity

This section operationalizes the network SOP and provides triage checklists for common connectivity issues. Sensitive details such as passwords must not be distributed; use the approved password vault or secured documentation store.

5.1 Wireless Networks (Wi-Fi)

- Corporate Office SSID: FreshFlow_Office_Secure (WPA3 Enterprise, domain login required).
- Warehouse Operations SSID: FreshFlow_WH_Ops (target devices include Zebra TC52 scanners and forklift terminals).
- Guest SSID: FreshFlow_Guest (captive portal, bandwidth capped at 5 Mbps).
- Passwords for protected SSIDs are [REDACTED] and must be accessed through the password vault.
- Known dead zone: Aisle 4 in Zone C (Cold Storage) due to thick insulation; operators should move to the loading dock to sync if connection fails.

Office Wi-Fi triage - "No Internet"

1. Confirm whether the device has internet access on an alternative network (e.g., mobile hotspot).
2. Forget the SSID and rejoin using AD credentials (firstname.lastname).
3. If multiple users are impacted simultaneously, treat as a potential authentication/AP service degradation and escalate to L2.

Warehouse Wi-Fi triage - intermittent sync failures

4. Confirm the user location; if in Zone C Aisle 4, move to loading dock and retest sync.
5. Confirm the device type (TC52, forklift terminal) and whether MDM policies have recently changed.
6. If multiple devices fail simultaneously, escalate to L2 for WLAN controller/AP investigation.

5.2 VPN and Remote Access

- Client: Cisco AnyConnect Secure Mobility Client v4.10.
- Gateway: vpn.freshflow.com (Asia-Pacific).
- MFA: Microsoft Authenticator approval required for all connections.
- Common error: inability to verify the IP forwarding table; often a home router/IPv6 conflict. Disable IPv6 on the user adapter or test via mobile hotspot.

VPN triage checklist

- Capture the exact error text and timestamp of the MFA prompt/approval.
- Validate AnyConnect version and confirm the correct gateway region.
- Test alternate network path (mobile hotspot) to isolate home router policy issues.
- If reproducible across multiple users in the same region, escalate to L2 for gateway and MFA telemetry review.

6. Warehouse Hardware and Automation

Warehouse devices are managed assets. All incidents must record asset ID, location (site/zone/aisle), and whether multiple devices are affected (possible MDM profile change or network issue).

6.1 Handheld RF Scanners (Zebra TC52 / Honeywell Dolphin)

- Device management: enrolled in Microsoft Intune MDM.
- Issue: scanner not decoding barcodes. Steps: clean scanner window, verify symbologies Code 128 and EAN-13 in the DataWedge profile, then perform a cold boot (remove battery for 15 seconds).
- Battery policy: batteries below 80% health must be recycled. Spare batteries are stored in the charging cradle at the supervisor desk.

6.2 Industrial Label Printers (Zebra ZT411 / ZT610)

- Status lights: solid green = ready; flashing red = media out or ribbon out; solid red = printhead open or major error.
- Misaligned prints / label skipping: calibrate by holding PAUSE + CANCEL for 2 seconds; the printer feeds blank labels to measure the gap.
- Network IP: typically static (10.20.5.x). If offline, print configuration label to confirm the IP has not reset to DHCP (0.0.0.0).

6.3 Forklift Terminals (Honeywell Thor VM1)

- Power issue when ignition is off: check the ignition control wire and validate that it remains on for 15 minutes after key-off.
- Screen freeze: press Blue key + Reset to force reboot.

7. Workstation and Software Support

This section provides standardized fixes for common productivity tool issues and defines what data to capture before escalation.

7.1 Microsoft 365 and Teams

- Teams audio issue ("I cannot hear anyone"): Teams Settings > Devices. Ensure Custom Setup is not selected; switch to PC Mic and Speakers or the correct headset model.
- Always validate Windows audio device selection and confirm the issue in a Teams test call before closing.

7.2 OneDrive

- Red X on files: OneDrive icon > Settings > Pause syncing > wait 1 minute > Resume.
- If unresolved: run Groove.exe /clean (legacy) or unlink/relink the PC account.
- Capture: user UPN, OneDrive build version, and any error codes in the sync client logs when escalating.

8. SAP S/4HANA Entry Runbooks

L1/L2 support focuses on access unlocks, printing dependencies, and capturing correct evidence for escalation. Core SAP issues are escalated to Global Engineering.

8.1 Account Lockouts and Unlock

- Lockout occurs after three failed attempts.
- Self-unlock: Fiori Launchpad > Forgot Password.
- Admin unlock: create a ticket with subject "SAP UNLOCK - [Username]"; SLA is 15 minutes.

8.2 Invoice Printing - Output Device Unavailable

- If SAP shows "Output Device Unavailable", check whether the local SAP Sprint service is running on print server AU-PRT-01.
- Capture: output device name, time of failure, affected transaction, and whether the print server is reachable from the user network segment.

9. AI and Automation Policy

This section operationalizes the AI policy to ensure productivity benefits while maintaining security and compliance.

9.1 Approved AI Tools

- FreshBot (Gemini-powered internal chatbot) for HR queries and IT FAQs.
- Coding assistants: GitHub Copilot or Gemini Code Assist (development team only).
- ChatGPT Enterprise may be used for summarizing Excel data. Users must not upload PII or customer pricing lists.

9.2 Automation Requests

- Departments requesting automation must submit a Process Optimization Request to the IT Efficiency Champion.
- Supported platforms include Power Automate, Python scripts, and Lovable.dev prototypes.

Operational control points

- No PII and no customer pricing lists in AI tools unless explicitly approved and covered by the enterprise agreement and data handling policy.
- For automation, define the process owner, data sources, access model, and rollback plan before implementation.
- All automations that touch finance, HR, or customer data require security review and change approval.

10. Security, Identity, Onboarding, and Offboarding

10.1 Onboarding (New Hire Setup)

- Lead time: 48 hours required from request submission to start date.
- Hardware allocation: warehouse staff receive rugged tablet + locker key; office staff receive Dell Latitude 5440 + dual monitors.
- Account creation is automated via the Workday-to-AD connector.
- Initial password follows the pattern Welcome + YYYY + ! (example: Welcome2026!).

10.2 Offboarding (Leaver Process)

- When HR notifies of termination, the Active Directory account must be disabled within 15 minutes.
- IT must collect devices and wipe data using DBAN prior to reimaging for the next user.

10.3 Phishing and MFA

- Report suspicious emails to security-alert@freshflow.com.
- Zero Trust: never approve an MFA request you did not initiate.

11. Escalation and Live Virtual Support (Human-in-the-loop)

11.1 Escalation Matrix

- L1: password resets, printer jams, basic software installation.
- L2: network outages, server alerts, complex hardware failures, AI tool configuration.
- L3: SAP core failures, cyberattacks, data center outages.

11.2 Video Support Authorization

Video support is resource-intensive and is reserved for cases where real-time visual inspection improves MTTR or safety response.

Authorized use cases

- Hardware failure visible via camera (smoke from printer, broken screen).
- Complex wiring issues requiring visual confirmation of a port panel or cabling.
- The AIT Support Dashboard fails to provide a solution after three attempts.

Unauthorized use cases

- Password resets (use the self-service portal).
- Simple software requests that can be handled through standard request fulfillment.

11.3 How to Connect (Microsoft Teams)

- When the AIT Support Dashboard cannot resolve the issue, it surfaces a red "Connect to Specialist (Video)" button.
- Clicking the button initiates a Teams call to the on-call L2 queue.
- Hours: Mon-Fri 08:00 to 18:00 (AEST). After hours, log a high-priority ticket.

- User preparation: have the camera ready to show error messages or hardware damage.

12. AIT Support Dashboard Operations Manual

The AIT Support Dashboard is a Retrieval-Augmented Generation (RAG) IT support system designed to answer questions using approved internal documents and to escalate to human support via Teams when required.

12.1 Technology Stack (as implemented)

- Frontend: Streamlit.
- LLM: Gemini 2.5 Flash.
- Embeddings: models/embedding-001.
- Vector database: FAISS with local persistence under vectorstore/faiss_index.
- Key libraries: LangChain, PyPDFLoader, pytz (AEST time checks).

12.2 Knowledge Base Lifecycle

- Admin mode allows authorized operators to upload PDF/TXT documents for indexing.
- Documents are chunked, embedded, and stored in FAISS; the index auto-loads on app startup to provide persistence across sessions.
- Knowledge updates require change control: approval, release note, snapshot backup, and a tested rollback path.

12.3 Escalation Logic (as implemented)

- Immediate escalation: if user mentions safety or hardware damage keywords (smoke, fire, broken screen, broken hardware), the dashboard shows the video support button immediately.
- Three-fail policy: if the assistant outputs a failure response (e.g., "I do not know" or "not in manual") three consecutive times, the video support button is offered.
- Business hours gate: video support is offered only during Mon-Fri 08:00 to 18:00 AEST; outside these hours the UI provides a high-priority ticket option instead.
- Password reset routing: password reset requests are redirected to the self-service portal and bypass live support.

12.4 Operational Requirements (enterprise hardening)

- Authentication and RBAC: the current admin checkbox is a development shortcut and must be replaced with SSO-backed authentication and role-based access control before production.
- Secrets management: store API keys in an approved secret manager; .env files are permitted only for local development.
- Logging: implement structured logs for query metadata, retrieval hits, and escalation triggers; mask any PII that appears in user prompts.
- Monitoring: track failure rate, escalation rate, and top recurring questions to drive knowledge improvements.

- Backup and rollback: maintain versioned snapshots of the FAISS index; support rapid rollback if knowledge updates degrade answers.

12.5 Deployment and Environment Management

- Run command (current): streamlit run app.py.
- Separate environments: DEV (engineering), UAT (validation), PROD (operations).
- Configuration via environment variables: business hours, timezone, Teams queue target, self-service portal URL, and escalation keyword list.

13. Standard Runbooks (Quick Reference)

These runbooks follow a consistent pattern: intake, verification, remediation steps, escalation triggers, and closure criteria.

13.1 Office Wi-Fi - No Internet

- Verify: can the user browse via an alternative network.
- Action: forget and rejoin FreshFlow_Office_Secure using AD credentials (firstname.lastname).
- Escalate to L2 if: multiple users are impacted or the issue persists beyond 10 minutes.
- Close when: user can browse and Teams call works.

13.2 VPN - IP Forwarding Table Verification Failure

- Verify: AnyConnect v4.10, correct gateway (vpn.freshflow.com), MFA approval occurred.
- Action: disable IPv6 on the adapter or test via mobile hotspot.
- Escalate to L2 if: recurrent across multiple users/regions or not resolved after isolating local network.

13.3 RF Scanner - Not Decoding Barcodes

- Clean scanner window (microfiber cloth).
- Confirm Code 128 and EAN-13 enabled in DataWedge profile.
- Cold boot: remove battery 15 seconds, reinsert, power on.
- Escalate to L2 if: repeated failures across devices (possible profile/MDM issue).

13.4 Label Printer - Misalignment / Red Status Light

- Interpret light: flashing red = media/ribbon; solid red = printhead open/major error.
- Calibrate: hold PAUSE + CANCEL for 2 seconds.
- Verify IP not reset to DHCP (0.0.0.0); confirm static assignment.
- If smoke/odor or safety concern: escalate immediately and use video support.

13.5 Teams - Cannot Hear Anyone

- Teams Settings > Devices: ensure Custom Setup not selected.
- Select PC Mic and Speakers or the correct headset device.
- Validate via Teams test call before closing.

13.6 OneDrive - Red X on Files

- Pause syncing for 1 minute then resume.
- If unresolved: Groove.exe /clean or unlink/relink.

13.7 SAP - Unlock and Printing

- Unlock: user self-service via Fiori; otherwise ticket "SAP UNLOCK - [Username]" (15-minute SLA).
- Printing: if output device unavailable, validate SAP Sprint service on AU-PRT-01.

14. Quick checklist

Pre-Replacement User Checklist (Logistics Operations)

Stop and Escalate Immediately (Do Not Continue Troubleshooting)

- Smoke, fire, burning smell, overheating, melted cable/charger, sparking
- Swollen battery, visible liquid ingress, chemical exposure
- Cracked screen/glass with sharp edges, bent frame, exposed wiring
- Any condition that could affect forklift driving safety or operator control
  Note: The support model includes immediate escalation to a specialist (video) for hardware safety issues and switching to a high-priority ticket outside business hours.

14.1 Handheld RF Scanner (Zebra TC52 / Honeywell Dolphin) – Pre-Replacement Checklist

A. Location and environment checks (avoid “false hardware failures”)

- Step 1: Move to a different area and retry (especially outside cold storage).
- Step 2: If you are in Cold Storage Zone C Aisle 4, move toward the loading dock and re-test, as this area can have poor signal coverage and cause sync failures.
- Step 3: Check whether the same barcode scans on a different scanner. If yes, the problem is likely device-specific. If no, suspect barcode quality or label damage.

B. “Cannot scan / barcode not recognized”

- Step 1: Clean the scanner window/lens (dust, tape residue, condensation).
- Step 2: Confirm DataWedge symbologies are enabled (Code 128, EAN-13).
- Step 3: Cold reboot: remove battery for 15 seconds, reinsert, power on.

C. Power and battery

- Step 1: Swap to a known-good spare battery and retest.
- Step 2: If the battery health is below 80%, treat it as a battery replacement issue first (not a device replacement).

D. What to record before requesting replacement

- Asset tag/serial number, location (site, zone, aisle), time of incident
- Symptom category (scan failure, app crash, sync failure, power issue)
- Which steps you completed (Lens clean, DataWedge check, battery swap, cold reboot)
- Whether the issue reproduces on other barcodes or only one barcode

14.2 Industrial Label Printer (Zebra ZT411 / ZT610) – Pre-Replacement Checklist

A. Status light and consumables (first decision point)

- Step 1: Identify status light condition:
    - Solid Green: printer is ready; suspect label template, network, or job queue.
    - Flashing Red: media/ribbon issue; check label roll and ribbon supply.
    - Solid Red: head open or major fault; ensure cover/head latch is fully closed.

B. Label skipping / misalignment / gap detection

- Step 1: Run calibration: hold PAUSE + CANCEL for ~2 seconds (feeds 2–3 labels).
- Step 2: Re-seat labels/ribbon, confirm guides are aligned and media path is correct.

C. “Printer offline” / cannot print over network

- Step 1: Print the configuration label and

15. Knowledge Management and Continual Improvement

- Every resolved P1 and recurring P2 incident must result in a knowledge update (runbook step, FAQ, or known error article).
- AIT failure cases ("not in manual") should be reviewed weekly to determine whether content gaps or retrieval tuning is required.
- Track quality KPIs: top recurring questions, answer accuracy sampling, escalation rate, ticket deflection, and MTTR.

16. Appendices

Appendix A - Ticket Intake Template

- User name, department, location (office / warehouse zone).
- Asset ID / serial number (if applicable).
- Symptoms and exact error text (screenshots encouraged).
- Time of first occurrence and whether the issue is ongoing or intermittent.
- Impact assessment: single user vs multiple users; safety impact; shipment impact.
- Troubleshooting steps already attempted.

Appendix B - Safety-Critical Script

- If smoke/fire is reported: instruct the user to stop using the device immediately and follow site safety procedure.
- Initiate video escalation (during business hours) or log a P1 ticket (after hours).
- Capture location and ensure facilities/safety is notified per site policy.

Appendix C - Redaction and Data Handling

- Do not publish SSID passwords, API keys, or sensitive internal addresses in general documentation.
- Store secrets in the approved secret manager; reference them via IDs or placeholders in this manual.
- Do not upload PII or customer pricing lists to AI tools; use approved pathways only.