Green Hills University

IT Service Desk — Support Agent Guide (Operational Template)

Version: 1.1

Document date: November 27, 2025 (fictitious)

Table of Contents

1. Introduction

This document provides an expanded operational guide for the IT Support Agent at Green Hills University (GHU). It is intended as a practical reference for Level 1 support staff who handle common technical support tasks and initial triage. All procedures and examples are fictitious and intended to be adapted to each institution's specific tools, policies, and legal requirements.

2. Contact information and Service Levels (SLA)

Service Desk — Green Hills University Hours of operation: - Standard: Monday to Friday, 08:00 — 20:00. - Critical support (campus-wide network outages, core systems): 24/7 on-call rotation. Primary contact channels: - Email: itsupport@greenhills.edu (primary). - Phone: Campus line ext. 4200 (for urgent calls). - Self-service portal (tickets and password reset): https://servicedesk.greenhills.edu (fictitious). - Walk-in desk: Main Library Building, Level 1. Service Level Objectives (SLOs) — examples: - Critical: Acknowledge within 1 hour. Target resolution within 8 hours. - High: Acknowledge within 4 hours. Target resolution within 48 hours. - Medium: Acknowledge within 8 hours. Target resolution within 5 business days. - Low: Acknowledge within 24 hours. Target resolution within 10 business days. Note: Priorities should be adjusted based on academic calendar peaks (e.g., exam periods, registration windows).

3. Password reset and account management

Scope: - University user accounts including: students (@student.greenhills.edu), faculty (@faculty.greenhills.edu), administrative staff, and service accounts. Goals: - Restore legitimate user access quickly while protecting university systems and data. - Provide clear steps and documentation for identity verification and escalation. Standard procedure (step-by-step): 1) Identification and verification: - Students: verify student ID number and date of birth, or confirm secondary verified email on record. - Faculty/Staff: request staff ID or confirmation from department head via institutional email when necessary. - Remote verification: allow secure two-factor verification via an existing registered mobile number or authenticator app if configured. 2) Allowed support channels: - Self-service password reset portal (preferred) — user-initiated with multi-factor verification. - Ticket in Service Desk for manual resets (include justification and identity proof). - Telephone verification only when other channels are unavailable; require additional identity checks. 3) Password policy enforcement: - Minimum length: 12 characters. - Complexity: at least three character classes (uppercase, lowercase, digits, symbols). - Recommended change intervals: administrative accounts every 180 days; encourage students to update each semester. 4) Account lockout and reactivation: - Lockout after 5 failed attempts: automatic 15-minute temporary lock. - Suspicious activity (unusual login locations or patterns): immediate lock and escalate to Security Team. 5) Account lifecycle: - Student accounts suspended after 365 days of inactivity; retention policies defined by Registrar and IT. - Staff accounts deprovisioned within 7 business days after HR termination notice (unless otherwise requested). 6) Documentation: - Log every reset action in the ticket with time, agent name, and verification method. - Use pre-approved response templates for common scenarios.

4. Software installation and access provisioning

Scope: - Managed university devices (lab PCs, faculty laptops). - Requests for licensed software for specific users or research groups. - Access provisioning to internal systems (e.g., learning management system, research databases). Process overview: 1) Catalog and inventory: - Maintain a published Software Catalog with approved applications, versions, and licensing terms. - Include supported OS platforms and hardware requirements. 2) Request submission: - Users must open a ticket with: name, role (student/faculty/staff), software name, justification, and required license type. - For research projects, attach PI approval and project code when applicable. 3) Validation and approval: - IT Support Agent validates compatibility and availability of licenses. - Paid licenses routed to Procurement for approval and purchase order processing. - Open-source or free software still requires review for security and compatibility. 4) Installation methods: - Managed devices: use centralized deployment (MDM/Endpoint Manager, software distribution tools); installations occur in maintenance windows. - Personal devices: provide official installers and step-by-step guidance; do not install paid licensed software on personal devices without explicit agreement. 5) Access provisioning: - Roles and permissions managed via the central identity directory (Active Directory/LDAP). - Use group-based access control; requests that modify role memberships require manager or PI approval. 6) Patch management: - Coordinate monthly patch cycles; emergency patches outside cycle when critical vulnerabilities are discovered. 7) Licensing record-keeping: - Track license counts, expiration dates, and assigned users in the License Registry.

5. VPN and network troubleshooting

Services: - Remote access VPN: 'GHU-VPN' (based on OpenVPN/OpenConnect client). - Campus Wi-Fi: 'GHU-Secure' for authenticated users, 'GHU-Guest' for visitors (captive portal). Common scenarios and quick troubleshooting checklist: 1) User cannot authenticate to VPN: - Verify account status in directory. - Check password validity and MFA status. - Review VPN server logs for authentication errors. 2) VPN tunnel established but resources unreachable: - Confirm split-tunnel policy and route settings. - Check DNS resolution for internal hostnames. - Verify firewall rules on server side. 3) Intermittent disconnects or high latency: - Request traceroute and ping tests from user. - Check local ISP issues on user side. - Inspect VPN gateway and ISP peering for packet loss. 4) Wi-Fi connectivity troubles on campus: - Confirm SSID and certificate trust. - Verify DHCP lease and IP range availability. - Inspect access point health and recent configuration changes. 5) Guest access complaints: - Verify captive portal configuration and voucher/guest account status. 6) Escalation: - If problem affects multiple users or core infrastructure, escalate to Network Infrastructure Team and note ticket priority increase. Tools and logs to consult: - VPN gateway logs, RADIUS/AAA server logs, firewall policies, DHCP server, and access point management console.

6. Device setup and configuration

Scope: - University-owned laptops, lab workstations, classroom AV equipment, printers, and IoT devices managed by Facilities. Preparation checklist before handover: - Apply the official base image (Windows 11 Enterprise or Ubuntu LTS) including required drivers. - Enroll device in Mobile Device Management (MDM) for policy enforcement, remote wipe, and configuration. - Enable full-disk encryption (BitLocker for Windows, LUKS for Linux). - Install corporate antivirus and endpoint detection agents. - Preconfigure Wi-Fi profiles and VPN client. - Install mandatory accessibility tools where required. - Map network drives and connect to the central file share. - Register device in Asset Management with serial number, location, and assigned user. Post-deployment validation: - Perform a step-by-step checklist with the user: login test, network access, printing test, and peripheral checks (webcam, microphone). - Provide basic onboarding documentation and contact info. - Snapshot or create a golden image for lab deployments after final acceptance. Classroom and AV devices: - Include a quick reference card for instructors with steps to switch inputs, connect laptops, and report issues. - Ensure remote management agent is enabled for after-hours troubleshooting.

7. Licenses and IT policy questions

Responsibilities and best practices: - Maintain a centralized License Registry that tracks: software title, vendor, purchase date, license keys or entitlement, assigned users, and renewal dates. - Perform annual software audits to ensure compliance with vendor agreements. - Coordinate with Procurement and Legal for license negotiations and volume discounts. Sample policy responses (model answers agents can use): Q: How do I request a paid software license? A: Open a ticket with the justification and expected user count. IT will recommend the best licensing model and forward to Procurement for purchase approval. Q: I found unauthorised software on a university machine. What should I do? A: Isolate the device from the network if malware is suspected. Create a high-priority ticket, document actions, and notify Security Team.

Do not delete logs or files until Security instructs. Acceptable Use and Data Handling: - University IT resources must be used primarily for educational, research, and administrative purposes. - Sensitive data classification (e.g., student records, medical info) requires restricted access and encryption in transit and at rest. - Personal use is permitted within limits; mass storage of copyrighted material without license is prohibited. Renewals and budgetary considerations: - Plan renewals at least 90 days before expiration to avoid service interruption. - Maintain a multi-year license forecast and align with departmental budgets.

8. Escalation matrix and ticket templates

Escalation matrix (summary): - Level 1 — IT Support Agent (first contact): handle password resets, basic software installs, and simple troubleshooting. - Level 2 — Systems / Network Specialist: server issues, persistent VPN or performance problems. - Level 3 — Security Administrator: confirmed compromise, data breach, or malware incidents. - Level 4 — IT Director / Infrastructure Manager: vendor negotiations, major change approvals. Ticket template (use in Service Desk ticket body): Subject: [Priority] - [Service or System] - [User Full Name / Department] Description: 1) Steps taken by the user prior to the incident. 2) Exact error messages (attach screenshots). 3) Date and time of occurrence. 4) Device details (make, model, serial), OS and version. 5) Contact info and best time to reach the user. Attachments checklist: - Screenshot(s) of error. - Log files if available. - Approval documents for license requests.

9. Security considerations and incident response

Role of the IT Support Agent in security: - Detect and report suspicious activity promptly. - Preserve evidence: avoid changing system state if a potential breach is suspected. - Follow the Incident Response runbook and escalate to the Security Team. Basic incident steps for agents: 1) Contain: limit further access (isolate device from network). 2) Preserve: secure logs and note timestamps, user actions, and observed behavior. 3) Notify: open a security incident ticket and escalate to Security Administrator. 4) Remediate: follow Security Team instructions for cleanup, patching, or reimaging. Phishing and social engineering: - Agents should be trained to spot social engineering signals. Verification procedures must be consistently applied before making account changes. - Report phishing campaigns to Security and Communications for campus-wide alerts.

10. Training, communication and awareness

Ongoing education: - Quarterly training sessions for students and staff: topics include account safety, phishing awareness, safe use of university resources, and basic device hygiene. Communication channels: - Monthly newsletter: include security tips, maintenance windows, and known issues. - Pre-exam period reminders: advise students to update passwords and verify backups. Help resources: - Maintain a Knowledge Base with step-by-step guides, short video tutorials, and printable quick-reference cards. - Configure searchable FAQs in the Service Desk portal for common issues.

11. Frequently Asked Questions (FAQ) and annexes

FAQ (short): Q: I cannot receive the MFA code. What should I do? A: Check your mobile signal and authenticator app. If unavailable, follow the emergency verification steps and open a ticket. Q: Can I install software on a lab machine for a class project? A: Only if approved and deployed by IT. For short-term needs, request a temporary image snapshot for the lab. Annex A — Sample forms (templates): - Software License Request Form (fields: requester, software, justification, department approval). - Device Handover Checklist (fields: serial, OS version, installed software, user sign-off).

Appendix — Device Handover Checklist (example)

Field	Example / Notes

Device type	Laptop (Dell Latitude 5430)
Serial number (S/N)	ABC12345
OS / Version	Windows 11 Enterprise 22H2
Assigned to	Dr. Jane Smith, Physics Dept.
Encryption	BitLocker enabled
MDM enrollment	ValleMDM - enrolled
Installed mandatory software	Office Suite, Antivirus, VPN client
Handover date	2025-11-27
Agent name	IT Agent - Carlos M.

Document control and distribution

This manual is a living document and should be reviewed annually or when major infrastructure or policy changes occur. All IT Support Agents must acknowledge reading the document and complete required training modules. Copyright: Green Hills University — Internal Use (fictitious example).