YACHTBYTE

Official resource

Guest Wi-Fi Pre-Trip and Reset Checklist

SLUG	guest-wifi-pre-trip-and-reset-checklist
SUMMARY	Printable checklist for yacht guest Wi-Fi preparation, privacy checks, bandwidth controls, captive portal testing, trip monitoring, and post-trip reset.
RESOURCE TYPE	Checklist
RESOURCE AREA	Connectivity, IT & cyber
INTENDED AUDIENCE	ETOs, AV/IT crew, captains, interior managers, yacht managers
ESTIMATED USE MINUTES	15
DOCUMENT LABEL	Download PDF
PDF	guest-wifi-pre-trip-and-reset-checklist-v1-0.pdf
VERSION	1.0
PUBLICATION STATUS	Published resource archive
IMPORTANT NOTE	This resource is practical operational guidance. It does not replace the vessel SMS, flag or class requirements, manufacturer manuals, competent network/security advice, privacy advice, or the authority of the Captain and responsible technical officers onboard.

YachtByte Official Resource

Pre-trip access

- [ ] Guest SSID enabled and mapped to the correct guest VLAN.
- [ ] Guest password, voucher or portal access method confirmed.
- [ ] Old guest vouchers or temporary accounts removed.
- [ ] Shared password rotation reviewed.
- [ ] Contractor, event or yard SSIDs disabled if no longer needed.
- [ ] Support contact and escalation route confirmed.

Separation and privacy

- [ ] Client isolation tested from a real guest device.
- [ ] Guest device cannot reach firewall, switch or controller management.
- [ ] Guest device cannot reach owner, crew, AV/control, CCTV, bridge-adjacent or OT networks.
- [ ] Portal data collection reviewed.
- [ ] Guest logs and retention expectations reviewed.
- [ ] Screenshots or exports shared with vendors only when needed.

Performance readiness

- [ ] WAN links and failover state checked.
- [ ] Bandwidth profile or per-device limits applied.
- [ ] DHCP pool capacity checked for expected guest load.
- [ ] DNS/filtering policy tested.
- [ ] AP health and controller status checked.
- [ ] Coverage tested in priority guest spaces.
- [ ] Streaming, video call and messaging behaviour spot-checked.

During-trip monitoring

- [ ] Client count monitored.
- [ ] Top bandwidth consumers reviewed without unnecessary privacy intrusion.
- [ ] DHCP pool usage monitored.
- [ ] WAN latency or packet loss watched.
- [ ] Repeated disconnects or roaming complaints recorded.
- [ ] Guest complaints logged with location and time.

Post-trip reset

- [ ] Temporary vouchers removed.
- [ ] Shared guest password rotated where appropriate.
- [ ] Old device authorisations cleared.
- [ ] Stale DHCP or portal entries reviewed.
- [ ] Temporary bandwidth exceptions removed.
- [ ] Only necessary logs retained.
- [ ] Coverage or performance issues added to the fault list.
- [ ] Network records updated if SSID, VLAN, portal or bandwidth policy changed.