YACHTBYTE

Official resource

Server, NAS, and Backup Ownership Register

SLUG	server-nas-and-backup-ownership-register
SUMMARY	Printable register for yacht onboard servers, NAS units, virtual machines, file shares, media storage, monitoring systems, backup jobs, restore owners, and restore-test evidence.
RESOURCE TYPE	Template
RESOURCE AREA	Connectivity, IT & cyber
INTENDED AUDIENCE	ETOs, AV/IT crew, IT providers, captains, yacht managers
ESTIMATED USE MINUTES	25
DOCUMENT LABEL	Download PDF
PDF	server-nas-and-backup-ownership-register-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

System identity

- [ ] Device or service name recorded.
- [ ] Role recorded: file server, NAS, VM host, backup target, media storage, monitoring server or archive.
- [ ] Manufacturer, model and serial number recorded where applicable.
- [ ] Physical location, rack and power source recorded.
- [ ] Management IP address and VLAN recorded.
- [ ] Admin access method and credential vault location recorded.
- [ ] Local console or emergency access method recorded.
- [ ] Responsible onboard owner recorded.
- [ ] Responsible shore/vendor owner recorded where applicable.

Data and service role

- [ ] Data types recorded: owner office, crew admin, technical records, AV/media, CCTV exports, monitoring logs or backups.
- [ ] Business or operational criticality recorded.
- [ ] Main users or departments recorded.
- [ ] Sensitive folders or restricted shares identified.
- [ ] Cloud sync or replication relationship recorded.
- [ ] Local services or VMs depending on the system identified.
- [ ] Whether this is primary data, backup data, archive data or replicated data recorded.
- [ ] Whether personal, owner, guest or crew data is stored on the system recorded.

Backup record

- [ ] Backup source recorded.
- [ ] Backup destination recorded.
- [ ] Backup frequency recorded.
- [ ] Retention period recorded.
- [ ] Encryption status recorded.
- [ ] Offsite or cloud copy recorded where used.
- [ ] Backup alert destination recorded.
- [ ] Last successful backup date recorded.
- [ ] Snapshot schedule recorded separately from backup schedule.
- [ ] Replication jobs recorded separately from backup jobs.
- [ ] Backup failure notification route tested.
- [ ] Encryption key or recovery key location recorded.

Restore ownership

- [ ] Restore owner named.
- [ ] Vendor or support contact recorded.
- [ ] Restore priority recorded.
- [ ] Last restore test date recorded.
- [ ] Restore test result recorded.
- [ ] Known restore limitation recorded.
- [ ] Required credentials, licences or media noted.
- [ ] Expected recovery time recorded.
- [ ] Expected data-loss window recorded.
- [ ] Restore location recorded: original system, spare hardware, temporary VM, cloud or vendor environment.
- [ ] Captain or management continuity priority confirmed where needed.

Lifecycle and risk

- [ ] Firmware or software version recorded.
- [ ] Warranty or support status recorded.
- [ ] Spare drive or spare hardware location recorded.
- [ ] UPS connection and shutdown behaviour checked.
- [ ] End-of-life or capacity risk recorded.
- [ ] Open corrective actions assigned.
- [ ] Storage capacity and growth risk reviewed.
- [ ] Unsupported operating system or application dependency identified.
- [ ] Old vendor accounts or unused admin accounts removed.
- [ ] Handover note stored outside the system being documented.

Closeout evidence

- [ ] Screenshot or export of storage health captured.
- [ ] Screenshot or export of backup-job status captured.
- [ ] Restore-test evidence stored in the technical records.
- [ ] Network map or IP plan updated where needed.
- [ ] Access permissions reviewed after crew or vendor changes.
- [ ] Next review date assigned.