Halcyon Creative Studio

Security Audit Checklist

TPN-style readiness assessment

Owner: IT & Systems Lead
Cycle: Bi-annual full audit; monthly spot-checks on critical controls
Scope: Digital Security pillar (DS-1 through DS-8). Management Systems and Physical Security controls live in the studio's policy manual.
Outcome: Continuous TPN-aligned readiness; zero critical findings open more than 30 days

Philosophy

Studios that handle pre-release content for major productions are graded continuously, not just at audit time. The four control families below organize the digital-security checks most relevant to a studio handling pre-release content — mapped to the Digital Security pillar (DS-1 through DS-8) of the MPA Best Practices framework that TPN assessors review:

- **Network & Perimeter.** Can content leave the building unintentionally?
- **Endpoint & Device.** Is every machine touching content audit-ready?
- **Content Handling.** Is the file itself protected at rest and in motion?
- **User Access & Identity.** Can the studio prove who saw what, when?

Severity tiers (internal scoring overlay; TPN itself uses Required vs. Highly Recommended): critical (must remediate before approval), high (close within 30 days), medium (close within 90 days). Status: pass, partial (mitigation in flight), or fail.

Network & Perimeter

Firewall, segmentation, VPN, screening room

ID	Control	Severity	Status	Remediation
N-01	[DS-3.0] Studio LAN segmented from public Wi-Fi (separate VLAN)	Critical	Pass	—
N-02	[DS-1.2] All inbound RDP / SMB / FTP ports closed at firewall	Critical	Pass	—
N-03	[DS-1.10] Site-to-site VPN to remote contractors with cert-based auth	High	Pass	—
N-04	[DS-4.1] Wi-Fi WPA3-Enterprise (radius) — guest network isolated	High	Pass	—
N-05	[DS-1.6] Sophos XG firewall logs retained ≥90 days; alerts on outbound anomalies	Medium	Partial	Extend retention 30d → 90d
N-06	[DS-3.6] IDS/IPS signatures updated weekly; quarterly tabletop review	Medium	Pass	—
N-07	[PS-7.0] Dedicated review-screening room with hardline ethernet only	High	Pass	—

Endpoint & Device

MDM, EDR, encryption, DLP

ID	Control	Severity	Status	Remediation
E-01	[DS-6.9] All studio Macs enrolled in Mosyle MDM at imaging time	Critical	Pass	—
E-02	[DS-6.7] FileVault 2 disk encryption enforced; recovery key escrowed	Critical	Pass	—
E-03	[DS-6.0] Gatekeeper + XProtect on; unsigned app installs require admin	High	Pass	—
E-04	[DS-6.4] OS auto-update within 14 days of vendor release	High	Partial	2 machines on 14.5; weekend update
E-05	[DS-5.1] No external USB / Thunderbolt write to studio Macs (DLP profile)	Critical	Pass	—
E-06	[DS-8.3] Screensaver lock ≤5 min idle; password complexity enforced	Medium	Pass	—
E-07	[DS-3.0] Personal devices blocked from studio LAN — guest only	High	Pass	—
E-08	[DS-6.0] Endpoint detection & response (EDR) deployed on all assets	High	Fail	EDR upgrade in pilot — replacing Sophos AV with CrowdStrike Q4

Content Handling

NAS access, watermarking, vendor transfers

ID	Control	Severity	Status	Remediation
C-01	[DS-11.0] Pre-release content stored on encrypted EVO SNS NAS only, never local	Critical	Pass	—
C-02	[DS-7.7] NAS access scoped per project — least-privilege ACLs	Critical	Pass	—
C-03	[PS-3.0] Watermarking applied to every internal review export	High	Pass	—
C-04	[DS-5.1] Personal cloud sync (Dropbox/iCloud/Drive) blocked at MDM	Critical	Pass	—
C-05	[MS-6.2] Project archives retained 90 days post-delivery, then purged	Medium	Pass	—
C-06	[PS-11.0] Physical printouts shredded; review-room printers locked	High	Partial	Add lock-and-print PIN on shared printer
C-07	[DS-13.0] Vendor handoff via studio-approved transfer tool only (Aspera)	Critical	Pass	—

User Access & Identity

SSO, MFA, onboarding/offboarding, access reviews

ID	Control	Severity	Status	Remediation
U-01	[DS-8.2] Single-sign-on (SSO) for all studio apps; MFA required	Critical	Pass	—
U-02	[DS-8.2] Privileged access (admin) with hardware security key	Critical	Pass	—
U-03	[MS-11.0] Onboarding checklist run for every new hire / contractor	High	Pass	—
U-04	[MS-11.1] Offboarding revokes within 4 hours of termination	Critical	Pass	—
U-05	[DS-7.6] Quarterly access review — every user, every system	Medium	Partial	Q3 review overdue
U-06	[MS-4.3] Annual security awareness training; phishing simulation	Medium	Pass	—
U-07	[DS-7.2] No shared accounts; each session attributable to one user	High	Pass	—

Remediation plan

Open items by priority and target close-out date

Action	Owner	Severity	Target
Deploy CrowdStrike EDR across studio (E-08)	IT lead	High	60 days
Extend firewall log retention to 90 days (N-05)	IT lead	Medium	14 days
Schedule overdue Q3 access review (U-05)	Ops	Medium	7 days
Update 2 macOS endpoints from 14.5 → 15.x (E-04)	IT lead	Medium	14 days
Enable lock-and-print PIN on shared printer (C-06)	Ops	Low	30 days