Script governance checklist

MSP checklist for signed script policy

MSP Script Governance Checklist

- Tenant signing policy documented and enforced
- All production scripts signed with approved certificates
- Approval workflow for script publish (four-eyes / dual-custody on by default in Settings → Security)
- Security audit logging enabled (Settings → Security)
- Export sample for assessor window (category + datetime filters)
- Separate storage of audit exports in GRC tool with retention policy
- Agent polling credentials rotated on compromise procedure
- IdP MFA enforced for all portal administrators
- Subprocessor list reviewed (/trust/subprocessors)
- Gaps documented in SSP (SIEM connector, immutability backlog)

Endpoint hardening (Windows)

- PowerShell ExecutionPolicy AllSigned at Machine scope (GPO or Intune)
- Code-signing CA / publisher certs deployed to endpoints (Trusted Publisher)
- Trustholm thumbprint allow-list matches deployed signing certificates
- Agent bootstrap (Bypass) documented separately from production AllSigned policy
- Pilot verification — unsigned local script blocked on endpoint
- Full runbook in portal: Guides → Require signed scripts on endpoints (GPO / Intune)

Trustholm trial: https://www.trustholm.com/trial

```
Sign in → Guides for operator runbooks (Intune/GPO, SSO, first-time usage).
```